TÉLÉCOMMUNICATIONS ET ÉCOUTES

ÉTUDE SUR LA CONFIDENTIALITÉ
DES
COMMUNICATIONS À DISTANCE

James

Communiquer : une nécessité vitale pour l'homme

Préface

Aux premiers âges du monde, la société ne comprend encore que des familles, et sur cette terre d'Asie, berceau de l'humanité, l'homme mène la vie pastorale et contemplative exempte de besoins.

Plus tard, comme l'a dit Victor Hugo, la famille devient la tribu, la tribu devient nation, et ainsi se constituent les royaumes, qui, peu à peu, se gênent, se froissent et se heurtent.

La guerre est née, et, avec elle, la nécessité de transmettre promptement au loin les ordres du commandement et les nouvelles importantes.

Cette nécessité donne naissance aux premiers courriers et ensuite à la télégraphie primitive qui n'est encore que « l'art des signaux ». Les étendards, les feux allumés sur les montagnes, tels furent les procédés rudimentaires mis en usage par les peuples de l'antiquité et que perfectionnèrent ensuite les Grecs, les Carthaginois et les Romains.

Nos ancêtres, les Gaulois et les Francs, usèrent également de ces mêmes procédés, et pendant la longue nuit féodale, on apercevait encore, au milieu des ténèbres, des feux allumés au sommet des forteresses qui étaient élevées sur tous les points de la patrie française menacée par les invasions des Normands et des Sarrasins.

Le danger passé, il n'est guère plus question de signaux par le feu, et cependant les chercheurs du moyen âge n'en poursuivirent pas moins la solution du problème si complexe de la transmission rapide de la pensée.

Pendant les quatorzième et quinzième siècles, les idées de sorcellerie, très en honneur dans la société française toujours à la poursuite du merveilleux, font dévier les recherches, qui plus tard se continuent sans succès dans des directions différentes jusqu'à la fin du dix-huitième siècle.

À ce moment, une lueur éblouissante s'élève du côté de l'occident et projette ses rayons bienfaisants sur l'Europe étonnée. C'est le génie de la Révolution française éclairant le monde ! Cette grande et sublime épopée se déroule au milieu d'effroyables tourmentes engendrées par la guerre civile et la guerre étrangère, et c'est pendant ces terribles convulsions que la télégraphie prend naissance.

Au plus fort de l'invasion, alors que nos places du Nord étaient au pouvoir de l'ennemi, que des forces écrasantes s'apprêtaient à démembrer la France, que la patrie était déclarée en danger, la Convention adopta avec enthousiasme la proposition de Claude Chappe, qui, au moyen du télégraphe aérien, lui offrait la possibilité d'avoir en quelques instants des nouvelles de nos armées.

Ainsi naquit la télégraphie aérienne, cette invention véritablement française, qui, après avoir eu la Révolution pour berceau, eut encore la double fortune d'être inaugurée par l'annonce d'une victoire, la reprise du Quesnoy sur les Autrichiens, et de terminer brillamment devant Sébastopol sa glorieuse carrière.

Militaire dans son principe, ou plutôt dans ses premières applications, la télégraphie conserva ce même caractère jusqu'à la chute du premier Empire, pour devenir ensuite, sous les deux Restaurations et pendant tout le règne de Louis-Philippe, un instrument politique, à l'usage exclusif de l'État.

Mais après un demi-siècle d'existence qui ne fut pas sans gloire, l'invention de Chappe, soumise, comme toutes les institutions humaines, à la loi inéluctable du progrès, dut disparaître à son tour, devant un agent nouveau, d'une puissance véritablement merveilleuse et incomparable : nous avons nommé l'électricité.

L'application de l'électricité à la télégraphie constitue l'une des plus surprenantes découvertes du dix-neuvième siècle. Cette nouvelle conquête de la science, dont l'Angleterre vient de fêter tout récemment le glorieux cinquantenaire, a été surtout remarquable par ses conséquences économiques.

La télégraphie électrique n'est plus, comme sa devancière, un instrument politique. Elle appartient à tous. Sa rapidité tient du prodige. Elle franchit les continents et les mers elles-mêmes, et son immense

réseau qui ne cesse de s'accroître, apparaît partout comme un symbole d'union et de fraternité parmi les hommes, comme une sorte d'élargissement de la patrie. Grande est sa mission ! Comme la poste, la télégraphie électrique a le rare privilège de n'être connue que par ses bienfaits. Le développement prodigieux qu'elle prend de jour en jour est là pour attester sa raison d'être et sa puissante vitalité.

Mais ce n'est pas tout encore.

L'électricité ne se borne plus à transporter instantanément la pensée d'une extrémité à l'autre de l'univers. Elle transmet aujourd'hui directement d'homme à homme les modulations de la musique et de la parole articulée.

Telles sont les merveilles réalisées pendant ce siècle par le génie humain, qui semble avoir pris pour devise : « *Escelsior ! Toujours plus haut !* »

Alexis Belloc

Paris, le 1er mai 1894 (*La télégraphie historique*, Deuxième édition)

Communiquer à distance

De tout temps, l'homme a éprouvé le besoin de communiquer, et même de « télécommuniquer », d'une part avec ses semblables, mais aussi avec les forces supranaturelles. Il a cherché aussi à s'affranchir de la distance séparant l'émetteur et le récepteur.

Parmi les mobiles les plus divers à ces besoins de communication, la diffusion d'une information en toute sécurité occupe une place prépondérante. Autrefois, les populations vivaient disséminées dans une nature peuplée d'animaux sauvages et de farouches guerriers. Il était dangereux de se déplacer et était nécessaire alors d'essayer de réduire les distances tout en préservant la confidentialité de l'information. Pour ce faire, l'homme a développé de nombreuses techniques dont ce sont inspirées nos télécommunications modernes.

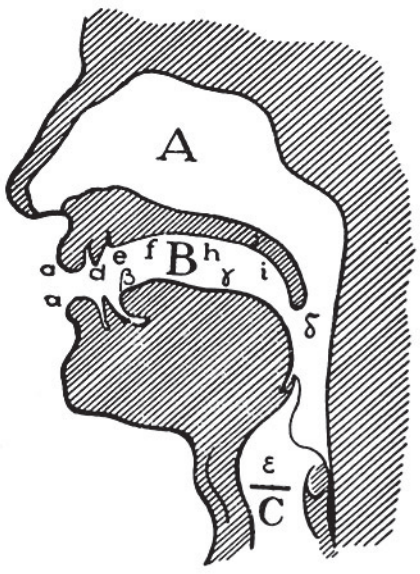
Nous nous limiterons dans ce chapitre à décrire les formes sonores de communication réservant les nombreuses formes visuelles au chapitre suivant. Nous nous appuierons sur des exemples concrets rencontrés dans des sociétés traditionnelles à travers le monde.

La voix

Le premier système de télécommunication est la voix humaine. Le message est clair puisqu'articulé et compris de toute la communauté linguistique dans une société donnée. En revanche sa portée physique est relativement faible, de quelques mètres à quelques centaines de mètres et fonction de l'environnement acoustique et de la forme de la phonation. De rares artifices permettent toutefois d'en accroître sa portée comme la disposition des mains en porte-voix afin de canaliser le son par devant, ou encore l'expression verbale ou chant en voix de tête.

L'appareil vocal et son fonctionnement[1]**.**

Pour la description de l'appareil vocal, nous nous bornons à une figure schématique, où A désigne la cavité nasale, B la cavité buccale, C le larynx, contenant la glotte ε entre les deux cordes vocales.



Dans la bouche il est essentiel de distinguer les lèvres α et a, la langue β — γ (β désignant la pointe et γ tout le reste), les dents supérieures d, le palais, comprenant une partie antérieure, osseuse et inerte f-h, et une partie postérieure, molle et mobile ou voile du palais i, enfin la luette δ.

Les lettres grecques désignent les organes actifs dans l'articulation, les lettres latines les parties passives.

La glotte ε, formée de deux muscles parallèles ou cordes vocales, s'ouvre par leur écartement ou se ferme par leur resserrement. La fermeture complète n'entre pour ainsi dire pas en ligne de compte ; quant à l'ouverture, elle est tantôt large, tantôt étroite. Dans le premier cas, l'air passant librement, les cordes vocales ne vibrent pas ; dans le second, le passage de l'air détermine des vibrations sonores. Il n'y a pas d'autre alternative dans l'émission normale des sons.

[1] La description un peu sommaire de Ferdinand de Saussure (linguiste suisse 1857-1913) a été complétée d'après le *Lehrbuch der Phonetik* de M. Jespersen, auquel nous avons aussi emprunté le principe d'après lequel les formules des phonèmes seront établies ci-dessous. Mais il s'agit là de questions de forme, de mise au point, et le lecteur se convaincra que ces changements n'altèrent nulle part la pensée de Ferdinand de Saussure..

La cavité nasale est un organe tout à fait immobile ; le passage de l'air peut être arrêté par le relèvement de la luette δ, rien de plus ; c'est une porte ouverte ou fermée.

Quant à la cavité buccale, elle offre un jeu possible très varié : on peut augmenter la longueur du canal par les lèvres, enfler ou desserrer les joues, rétrécir et même fermer la cavité par les mouvements infiniment divers des lèvres et de la langue.

Le rôle de ces mêmes organes comme producteurs du son est en raison directe de leur mobilité : même uniformité dans la fonction du larynx et de la cavité nasale, même diversité dans celle de la cavité buccale.

L'air chassé des poumons traverse d'abord la glotte, il y a production possible d'un son laryngé par rapprochement des cordes vocales. Mais ce n'est pas le jeu du larynx qui peut produire les variétés phonologiques permettant de distinguer et de classer les sons de la langue ; sous ce rapport, le son laryngé est uniforme. Perçu directement, tel qu'il est émis par la glotte, il nous apparaîtrait à peu près invariable dans sa qualité.

Le canal nasal sert uniquement de résonateur aux vibrations vocales qui le traversent ; il n'a donc pas non plus le rôle de producteur de son.

Au contraire, la cavité buccale cumule les fonctions de générateur de son et de résonateur. Si la glotte est largement ouverte, aucune vibration laryngienne ne se produit, et le son qu'on percevra n'est parti que de la cavité buccale (nous laissons au physicien le soin de décider si c'est un son ou simplement un bruit). Si au contraire le rapprochement des cordes vocales fait vibrer la glotte, la bouche intervient principalement comme modificateur du son laryngé.

Ainsi, dans la production du son, les facteurs qui peuvent entrer en jeu sont l'expiration, l'articulation buccale, la vibration du larynx et la résonance nasale.

Mais énumérer ces facteurs de production du son, ce n'est pas encore déterminer les éléments différentiels des phonèmes. Pour classer ces derniers, il importe bien moins de savoir en quoi ils consistent que ce qui les distingue les uns des autres. Or un facteur négatif peut avoir plus d'importance pour la classification qu'un facteur positif. Par exemple, l'expiration, élément positif, mais qui intervient dans tout acte phonatoire, n'a pas de valeur différenciatrice ; tandis que l'absence de résonance nasale, facteur négatif, servira, aussi bien que sa présence, à caractériser des phonèmes. L'essentiel est donc que deux des facteurs énumérés plus haut sont constants, nécessaires et suffisants pour la production du son :

- a) l'expiration,
- b) l'articulation buccale,

tandis que les deux autres peuvent manquer ou se surajouter aux premiers :

- c) la vibration du larynx,
- d) la résonance nasale.

D'autre part, nous savons déjà que a, c et d sont uniformes, tandis que b comporte des variétés infinies.

En outre, il faut se souvenir qu'un phonème est identifié quand on a déterminé l'acte phonatoire, et que réciproquement on aura déterminé toutes les espèces de phonèmes en identifiant tous les actes phonatoires. Or ceux-ci, comme le montre notre classification des facteurs en jeu dans la production du son, ne se trouvent différenciés que par les trois derniers. Il faudra donc établir pour chaque phonème : quelle est son articulation buccale, s'il comporte un son laryngé (~~) ou non ([ ]), s'il comporte une résonance nasale (….) ou non ([ ]). Quand l'un de ces trois éléments n'est pas déterminé, l'identification du son est incomplète ; mais dès qu'ils sont connus tous les trois, leurs combinaisons diverses déterminent toutes les espèces essentielles d'actes phonatoires.

On obtient ainsi le schéma des variations possibles :

	I	II	III	IV
a	Expiration	Expiration	Expiration	Expiration
b	Art. bucc.	Art. bucc.	Art. bucc.	Art. bucc.
c	[]	~~~	[]	~~~
d	[]	[]	.....	.....

La colonne I désigne les -sons sourds. II les sons sonores, III les sons sourds nasalisés, IV les sons sonores nasalisés.

Les sifflements

Les sifflements peuvent véhiculer soit un signal codé, connu de la communauté linguistique ou préalablement défini au sein d'un groupe d'individus, soit un véritable langage calqué sur le langage articulé. On rencontre deux types de sifflements : le sifflement émis directement par la bouche et celui utilisant des objets sonores.

Les sifflements émis par la bouche le sont directement par le jeu d'un positionnement dentolingual ou par l'utilisation des doigts. Ces formes de sifflements ont généralement une richesse communicative restreinte consistant à signaler une présence, héler ou initier une action selon un code connu ou préétabli par le groupe.

D'autres formes de sifflements utilisant des objets sonores véhiculent souvent de véritables langages. La plupart des peuples d'Afrique Noire utilisent des sifflets ou des flûtes à embouchure terminale possédant plusieurs trous permettant l'émission de sons de hauteurs différentes. De nombreux peuples de cette région du monde parlent des langues tonales, c'est-à-dire des langues dont le mode de compréhension tient compte de la hauteur relative des syllabes entre elles. Ainsi, un même mot prononcé à des hauteurs différentes ou avec des variations de hauteurs prendra plusieurs significations. L'utilisation des sifflets tient compte du rythme et de la hauteur tonale des syllabes. Ces sifflets sont le plus souvent utilisés par les chasseurs partis en brousse, les cultivateurs et éleveurs dispersés dans ce même milieu, ou encore par chacun pour encourager les lutteurs traditionnels.

Femmes Hmong

Chez les Hmong[2], population d'origine chinoise vivant principalement en Chine et dans une large partie de l'Asie du Sud-est, on utilise des feuilles rigides que l'on place entre les lèvres. Celles-ci émettent des sifflements extrêmement puissants permettant de communiquer entre les montagnes. La langue hmong est une langue tonale

[2] Les Hmong sont un peuple d'Asie originaire des régions montagneuses du sud de la Chine (spécialement la région du Guizhou) au nord du Viêt-Nam et du Laos. Ils sont aussi appelés les Miao, 苗(Miáo) ce qui signifie « riz cru » et désigne depuis longtemps des populations nomades peu intégrées. Les Hmong eux-mêmes emploient souvent la dénomination « montagnards ».

à huit tons. Ainsi, la hauteur des notes émises correspond-elle à ces hauteurs tonales. En dehors des messages courants, ces feuilles permettent de chanter des chansons d'amour et de courtiser l'âme sœur même éloignée de plusieurs centaines de mètres. Dans ce cas, le message est adressé à un interlocuteur unique sans confidentialité.

Les sifflets

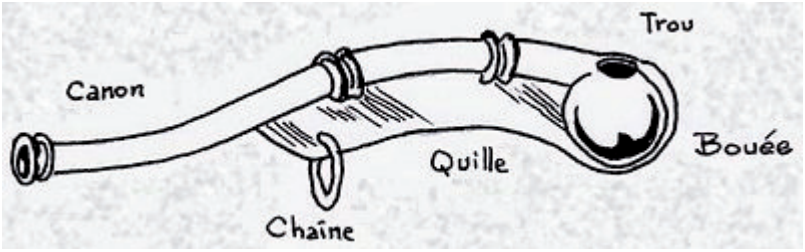
Le sifflet de Marine[3]

On sait que dans l'Antiquité, sur les galères romaines ou grecques, le rythme des coups de pelles était donné aux rameurs par un tambour, une flûte ou un sifflet.

Plus récemment au temps de la marine à voile, le seul moyen de transmettre les ordres à bord des navires était le coup de sifflet ou Boatswain's Call (« Appel du Maître d'équipage », officier chargé du gréement et des voiles). Il avait donc besoin de transmettre plus d'ordres que d'autres officiers et c'est pour cela qu'on appela son sifflet : Boatswain's Call.

Il fut utilisé en premier sur les navires anglais au XIII^{éme} siècle, au cours des croisades et fut connu sous le nom de « The Call » vers 1670, quand le Lord de l'Amirauté (Lord High Admiral of the Navy) porta un sifflet en or comme marque de son rang. Il fut alors connu sous le nom de « Whistle of Honour » (Sifflet d'honneur).

Par la suite chaque officier en porta un, mais en argent, et chacun le décora en le portant à l'aide d'un cordon tressé et ouvragé ou d'une belle chaîne. La Royal Navy très respectueuse des traditions, continua à perpétuer cette coutume qui se voulut une marque de respect envers le commandant ou des visiteurs de marque à bord ou encore pour mettre l'accent sur des ordres importants.



Chaque partie du sifflet est nommée d'un terme nautique : le canon, la quille, le trou, la bouée et la chaîne.

Ce mode de transmission des ordres était très performant à la mer, particulièrement au cours des tempêtes, où le niveau sonore y est tel que les ordres à la voix passent mal, et les marins étaient entraînés à répondre immédiatement au son du sifflet.

Le sifflet se tient entre le pouce et l'index, le pouce étant sur l'anneau de fixation de la chaîne. La bouée se plaçant dans la paume de la main, les autres doigts recouvrant le tout sans fermer hermétiquement de manière à ne pas boucher le trou de la bouée et à laisser sortir le son. On souffle dans le canon plus ou moins fort, tout en ouvrant les doigts de manière à obtenir le son désiré.

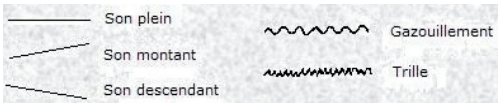
Ainsi, on peut considérer qu'il y a : 2 notes, haute ou basse et 3 tons :

— ton plein ;

— « gazouillement » série de coups de sifflet comme le cri d'un oiseau ;

— le trille (comme en musique, vibration de la langue).

[3] Texte et dessins de Jean-Philippe Chalaye, 12 mars 2004 - Référence : *Dictionnaire des commandements faits avec le sifflet, à bord des bâtiments de guerre.,* 2^{e} édition, 1819. Thomas-Marie Letourneur, capitaine de vaisseau.



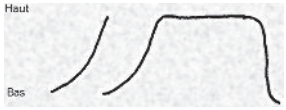
Les commandements au sifflet sont représentés symboliquement de la manière suivante :

Montée à bord ou départ du canot major

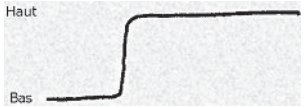
Continuer

Cesser le travail

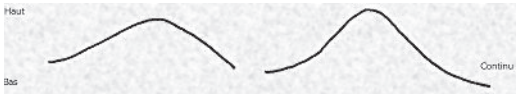
Appel des Maîtres d'équipage



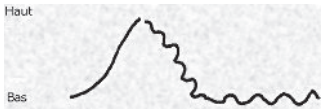
Navire en vue



A hisser les voiles, ou Souquer ferme



A la soupe

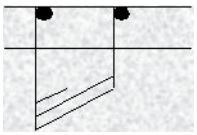


A laisser filer

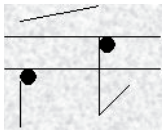
Cesser tout

Selon le Dictionnaire des commandements faits avec le sifflet, à bord des bâtiments de guerre, on peut obtenir quelques explications complémentaires. Une liste de signes élémentaires, décrits par des onomatopées telles que : i , it ou rui , rr , t , ti , tit, uit désignent les modulations que le gabier utilise sur son sifflet. En face de chacun de ces termes est représenté ce que l'on pourrait comparer à une portée de musique, mais ne comportant que 2 lignes ! (le son haut et le son bas) et sur lesquelles la note du sifflet en notation conventionnelle de musique est placée. On trouve des croches et des doubles croches liées par groupes et possédant également les signes musicaux que l'on rencontre dans une partition, comme : le trille, le silence, la note pointée, etc.

Exemples :



ui



rui

Les trompes et les conques

Presque partout à travers le monde sont utilisées les trompes ou les conques marines pour communiquer. Ces deux outils véhiculent, en fonction des populations, soit des messages codés soit des messages de type linguistique comme dans le cas des sifflets. Les trompes peuvent être en métal, en bois ou encore en corne d'animal. Nombre d'entre elles et leur utilisation ont une connotation guerrière, annonçant le départ ou le retour d'une lutte armée ou d'une vengeance.

Les différentes étapes d'une chasse aux chiens courants sont ponctuées d'appels à la voix et à la corne, qui sont des combinaisons de sons de même hauteur, mais de durée variable émis par des instruments à vent : les cornes ou cors.

Au moyen âge, le cor, commun aux pâtres, chasseurs et chevaliers (Cor du paladin Roland) est de corne, bronze ou ivoire[4]. À la Renaissance tout en s'enrichissant d'or et d'argent, il s'allonge et possède une enguichure[5]. Il existe aussi des cornuchets ou cornets qui sont de petites cornes, bien souvent nommées huchets[6].

Tirés à l'origine d'une corne animale naturellement creuse, ils possèdent dans leur pointe sectionnée un bec ou bouquin[7] avec ou sans anche. L'extrémité évasée constituée par la base de la corne, forme le pavillon. De nos jours ces instruments de dimensions variables, sont en corne ou en laiton, de forme généralement courbe et munis d'un bec à anche.

La Chanson de Roland

Marsile, roi Maure souhaitant épargner sa ville Saragosse de l'avancée de l'armée des Francs, convint d'un traité de paix avec Charlemagne par l'intermédiaire de Ganelon. Mais Ganelon corrompu et haineux envers Roland entraîna l'arrière-garde de vingt mille hommes dans un défilé où attendait une armée de Sarrasins.

Le chevalier Olivier, grand ami de Roland, signale une large troupe sarrasine approchant l'arrière-garde. Il demande à Roland qu'il sonne du cor pour avertir Charlemagne. Roland préfère mourir en guerrier que de se déshonorer à appeler à l'aide. Les hommes de Roland se battent contre une force cent fois supérieure à la leur. Lorsqu'il ne reste plus que soixante combattants, Roland fait sonner son olifant tellement fort qu'il se crève les tympans. Charlemagne pressentant le pire chevauche vers le lieu. Tous les chevaliers meurent, mais Roland et l'archevêque Turpin blessés arrivent à faire fuir l'armée maure avant de s'effondrer tous deux.

Roland a encore la force d'essayer de briser son épée Durandal contre un bloc de marbre ; sans succès : la lame reluit et flamboie sans s'ébrécher. Il s'allonge face à l'Espagne pour mourir et c'est alors que Saint-Michel, Saint-Gabriel et Chérubin l'emportent vers le paradis.

Avant que Charlemagne ne puisse rejoindre la bataille, l'assaillant a déjà fui. Charlemagne finit par défaire les forces restantes pour venger son champion avant de rentrer tristement à Aix-la-Chapelle. Là, il doit apprendre la triste nouvelle à la belle Aude, sœur d'Olivier et fiancée de Roland, qui meurt sur le coup à cette annonce.

La trompe de chasse est un instrument de musique français en cuivre. Issu des instruments de communication cynégétiques venant de la nuit des temps signalant par des sons lents ou courts, aigus ou graves, les différentes situations pendant la chasse. Ces instruments étaient faits de cornes d'animaux,

[4] Le cor en ivoire porte le nom d'oliphant ou olifant : du lat. *elephantus*, dans le sens d'ivoire ; c'est un petit cor que portaient les chevaliers (Roland sonna de l'olifant).

[5] Enguichure : système de suspension d'un cor de chasse (ou de chevalier par extension), cordons pour porter le cor de chasse.

[6] Huchets : petits cors de chasse qui figurent sur certains blasons à l'opposition des « grêliers » qui sont de grands cors de chasse faisant un tour sur eux-mêmes.

[7] Bouquin : de bouque ou bouche, c'est un bec avec ou sans anche ajusté à la pointe d'une corne creuse. « Cornet à bouquin » : petite corne ou trompe d'appel. On dit aussi par contraction « bouquin » pour désigner de petites trompes ou cors en métal.

de bois puis de cuivre. Les langages exploités par ces instruments s'appelaient les cornures. On chassait alors « À cor et à cris ».

On voit apparaître sous sa première forme à enroulement circulaire, la trompe musicale de Crétien (92 cm de diamètre), vers la seconde moitié du XVII[e] siècle. À ce moment, une écriture musicale plus élaborée devient nécessaire pour situer et discerner les animaux, les circonstances de chasse et éventuellement les lieux, en bref toutes les actions de chasse possibles.

Les conques marines sont quant à elles généralement réalisées avec un gros gastéropode (lambis, triton...) dont on a sectionné l'apex ou ouvert l'un des premiers tours de la spirale.

L'antsiva (appelé aussi *bankora* ou *angaroa*) est un instrument de musique malgache de la famille des aérophones, constituée d'une conque percée d'un unique trou latéral. On distingue l'*antsiva lahy* (mâle) plus aigu, de l'*antsiva vavy* (femelle) plus grave. Il est joué exclusivement par les hommes.

La conque, utilisée comme une trompette a servi à plusieurs buts dans l'histoire japonaise. Elle est nommée jinkai (陣貝), horagai (法螺貝), ou de plusieurs autres noms en japonais selon sa fonction.

La conque est associée surtout à son usage par les moines bouddhistes pour les buts religieux. Son usage est connu au moins depuis mille ans, et il a encore cours aujourd'hui pour quelques rituels, tel que la portion de l'*omizutori* (dessin d'eau) des rites Shuni-e au Todaiji dans Nara. Contrairement à la plupart des conques d'autres parties du monde qui ne produisent qu'une seule note, l'*hora* japonais ou *horagai* peut produire trois ou quatre notes différentes. Le processus pour transformer une coquille en instrument est gardé secret, mais il implique la mise en place d'un embout de bronze à la pointe de la coquille.

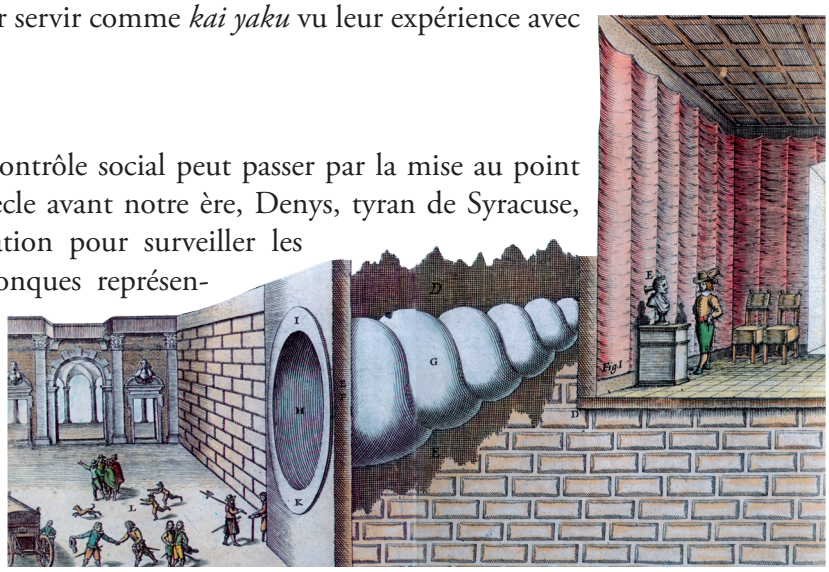
Moines guerriers ascétiques de la secte Shugendo, les *yamabushi* utiliseraient la conque pour signaler leur présence l'un à l'autre à travers les montagnes.

En temps de guerre, la conque, appelé *jinkai*, ou « coquille de la guerre », a été utilisée comme une trompette à signaux. Elle serait tenue dans un panier et utilisée dans cas différents pour signaler des troupes, pour attaquer, se retirer, ou modifier la stratégie.

Le trompettiste a été appelé *kai yaku* (貝役). Les *jinkai* avaient une fonction semblable aux tambours et aux cloches pour organiser des formations de troupes, mettre un rythme pour marcher, et fournir un accompagnement musical héroïque pour encourager les troupes. Beaucoup de *daimyo* (seigneurs féodaux) ont enrôlé des *yamabushi* pour servir comme *kai yaku* vu leur expérience avec l'instrument.

Un autre usage des conques :

Surveiller et punir : le désir de contrôle social peut passer par la mise au point de systèmes d'écoute. Dès le IV[e] siècle avant notre ère, Denys, tyran de Syracuse, aurait utilisé un mode d'amplification pour surveiller les conversations de ses sujets. Ces conques représentent des oreilles géantes, telles que l'ordre classique au XVII[e] siècle se les figurait. (Illustration extraite de « *Le Téléphone, Le monde à portée de voix* », A. Carré, Gallimard (1993) – gravure in « *Misurgia universalis* » Athanase Kirscher).



Les tambours

Les tambours sont probablement les outils de « télécommunication » les plus célèbres, mais aussi les plus méconnus quant à la spécificité de leur langage. On pourrait classer les tambours selon leur puissance sonore. Cette dernière est fonction de la taille de l'instrument – plus il est grand et plus sa « voix » porte – mais également de sa technologie. On distingue, parmi les « tambours-parleurs », deux types d'instruments :

les tambours à membrane(s) et *les tambours à fente(s)* appelés aussi « *tambours de bois* ».

Les premiers sont souvent des instruments mobiles – à l'instar de nos téléphones portables – utilisés en Afrique Occidentale par les griots que sont ces généalogistes, conteurs et journalistes de la tradition orale. À l'aide de ces tambours, ils délivrent deux types demessages : « pour information » ou « pour action ». Dans le premier cas, on veut annoncer au groupe des nouvelles telles : naissances, décès, arrivée d'un visiteur étranger, etc. Dans l'autre, on convoque tout ou une partie de la population pour des travaux d'utilité collective, un rassemblement, un départ à la guerre. Ces tambours sont frappés à mains nues ou à l'aide d'un ou deux bâtons. Il existe également de nombreuses formes de grands tambours fixes à membrane.

Les tambours à fente (ou de bois) sont, comme leur nom l'indique, en bois. Ils sont généralement faits d'un tronc d'arbre évidé à travers une fente pratiquée sur presque toute la longueur et sur quelques centimètres de large. Ils sont, compte tenu de leur grande taille et de leur poids, des instruments fixes posés au sol. Ils sont frappés avec des bâtons de bois par un ou plusieurs batteurs. Certains modèles sont en revanche, comme les tambours à membranes, portables. Les tambours à fente sont toujours utilisés traditionnellement en Afrique Noire mais ont disparu en Océanie, tout du moins dans leur contexte purement traditionnel.

Tambour à fente anthropomorphe. Nomvernaculaire : Mukoko.Ethnie : Pendé, Congo.

Les messages tambourinés

Le propre des tambours est de transmettre des messages de type linguistique dans un esprit identique à celui des sifflets. Pour être compréhensibles, les messages doivent comporter au moins deux sons de hauteurs distinctes.

Pour cela, plusieurs artifices sont utilisés : soit le tambour possède deux peaux dont chacune émet une note, soit il n'en possède qu'une. Avec ces derniers, on émet alors deux notes en adaptant la forme de la frappe. Une autre solution consiste en deux tambours de même facture, mais de hauteur différente,

placés côte à côte et frappés par un ou deux batteurs. Et dans le cas des tambours à fente les deux lèvres se trouvant de chaque côté de la fente émettent chacune un son de hauteur différente.

En Afrique, parmi les tambours à membranes, il en est un particulièrement sophistiqué communément appelé « tambour parleur » ou encore « tambour d'aisselle ». Il est cependant préférable de le désigner sous le terme de « tambour à variation de tension » puisque presque tous les tambours africains sont doués de parole et ne sont pas toujours joués sous l'aisselle ! Il s'agit d'un tambour à deux peaux montées sur un fût en forme de sablier. Les deux membranes sont reliées entre elles par une ficelle passant alternativement par l'une et l'autre peau. Le batteur tient généralement l'instrument sous son aisselle, frappe l'une des peaux avec une baguette coudée et fait varier sa tension en écrasant plus ou moins les tendeurs avec le bras. Il lui est ainsi possible d'émettre une multitude de notes et de reproduire avec une certaine fidélité le langage parlé.

La « voix » des grands tambours à membrane peut porter à plusieurs centaines de mètres, voire plus d'un kilomètre en terrain plat non réverbérant (savane sablonneuse par exemple) ou plusieurs kilomètres en milieu réverbérant (montagnes arides).

Dans les années trente, deux anthropologues français, Geneviève et Marcel Griaule séjournent au Mali. Leurs observations sur la cosmogonie et la symbolique du peuple Dogon et le langage qui les exprime restent un document exceptionnel :

Pour qu'il y ait rythme, il faut, selon les Dogons, « que les coups ne soient pas pareils », c'est-à-dire que les sons émis par les battements soient différenciés par l'oreille. De plus, il faut qu'ils soient frappés sur une surface plane et résonnante. Donner des coups réguliers avec la main à plat, c'est « frapper », lága ; mais frapper les mêmes coups avec la main légèrement incurvée de manière à créer une résonance de l'air, c'est bà, « battre » (un rythme). De même si l'on frappe avec une baguette sur un plat en bois ou une calebasse, il y a résonance ; c'est un rythme, bòy (nom d'action de bà).

D'une façon générale, les instruments que l'on frappe avec la main ou une baguette sont dits produire une « parole » ; ce sont la plupart des tambours et la petite clochette gìnu (frappée avec une bague au moment du sígi). Tous les instruments à vent dans lesquels on « souffle » (súdo) produisent en plus de la parole un « chant » : flûtes, trompes, sifflets ; les sons se prolongent davantage, leur résonance est plus grande. Mais quelques instruments à percussion sont considérés comme produisant un « chant » ; ce sont les tambours gòmboy (tambour d'aisselle)…

Les tambours de bois, quant à eux, sont les instruments de « télécommunication » archaïques les plus puissants. Leur portée atteint généralement plusieurs kilomètres même dans des conditions acoustiques défavorables.

Le tam-tam

Un tam-tam est un idiophone à son indéterminé, contrairement au gong. Depuis l'époque coloniale, le vocable « tam-tam » est abusivement utilisé (*génériquement* ?) pour désigner n'importe quel tambour — surtout s'il vient ou est censé venir d'Afrique.

Cet instrument à percussion d'origine asiatique a été apprécié par les compositeurs occidentaux en raison de l'effet mélodramatique produit par sa sonorité profonde et métallique. Il a été introduit parmi les percussions de l'orchestre symphonique au XIX^{e} siècle. Une de ses premières utilisations dans la musique militaire a été décidée à l'occasion de l'exhumation des restes de Napoléon Bonaparte aux Invalides le 15 décembre 1840.

Le tam-tam est le moyen de communication par excellence des régions du Centre et du Sud Cameroun. Il est utilisé pour mobiliser les populations, pour annoncer des nouvelles : deuils, arrivée d'un étranger, présence d'un voleur au village ; pour animer des événements : fêtes religieuses et aussi surtout

pour communiquer avec un parent, un ami. Aujourd'hui les initiateurs à l'utilisation de l'instrument, les joueurs et surtout les fabricants deviennent de plus en plus rares. L'initiation dépend de l'utilisation qu'on veut en faire. Elle est un peu complexe quand il faut annoncer des nouvelles ou converser avec un ami ou un parent. Il faut dès lors avoir un maître qui vous initie d'abord à connaître le « NDAAN », sorte de pseudonyme par lequel on interpelle l'individu ou la communauté à qui le message est destiné. Chaque individu a un « NDAN » : celui de son homonyme. Après cette phase, le reste de l'initiation est la même, c'est-à-dire qu'il faut fréquenter les joueurs de tam-tam en activité, être en contact permanent avec l'instrument, avoir volonté et dextérité. L'initiation peut durer de un à cinq mois. Quant à sa portée, elle dépend de plusieurs facteurs c'est-à-dire : de la qualité du bois avec lequel l'instrument est fabriqué : l'« Ebè » (Bilinga) donne de meilleurs résultats ; du lieu où le tam-tam se joue : la portée est plus grande en altitude ; des dimensions du tam-tam : les plus petits sont aigus, mais les plus grands sont plus perçants, et leur son peut aller à plus de 25 Km quand toutes les conditions ici énumérées sont réunies. Après la pluie, tôt le matin ou le soir, la portée est plus grande et dépend aussi de l'énergie du frappeur.

Les messages véhiculés par le tam-tam sont ésotériques. Cependant, la majorité de la population sait faire la différence entre un tam-tam annonçant le deuil et les autres, sans pour autant pouvoir en décrypter le message. L'instrument étant assez rarement utilisé, les quelques tam-tams qu'on trouve dans les villages ne sont plus accessibles à tout le monde ; l'accès n'est réservé qu'aux joueurs patentés. Aujourd'hui son utilisation est confrontée à trois grandes contraintes, à savoir : la rareté du bois et des fabricants de l'instrument ; la rareté des maîtres disponibles à transmettre les connaissances ; le décryptage difficile des messages. En réalité, le tam-tam dont le décryptage des messages nécessite un apprentissage certain a aussi besoin de grands joueurs. En conclusion, le tam-tam sert beaucoup plus à mobiliser la population qu'à converser avec un individu. (Illustration : Djembé de l'Afrique de l'Ouest)

Les cloches

Les moins connus sont les jeux de cloches à deux tons rencontrés en Afrique Noire. Ils sont constitués de deux cloches jumelles de hauteurs différentes frappées par un même joueur, ou de cloches indépendantes jouées par deux individus. Ce sont toujours des cloches à battant externe. Ces instruments ont une portée sonore limitée à quelques centaines de mètres.

Les cloches des églises pouvaient autrefois être utilisées comme système d'alerte pour des événements graves comme le feu ou les invasions (on sonnait alors le *tocsin*, ou *à toute volée* : à grande vitesse). Le type de sonnerie de cloches d'église accompagnant les cérémonies funèbres s'appelle quant à lui le *glas* : c'est un son régulier au tempo très lent.

Cependant, ces cloches ont pour fonction normale de signaler le passage du temps. Dans ce cas, une séquence particulière de sons peut être produite par un groupe de cloches pour indiquer l'heure et ses subdivisions. L'une des plus connues et celle dite des quarts de Westminster, une série de seize notes qui est émise par le carillon de l'horloge du palais de Westminster dont la grande cloche qui sonne l'heure proprement dite porte le nom de *Big Ben*. La plupart du temps, seules les heures pleines sont sonnées (en général à raison d'un coup par heure, en allant de 1 à 12), parfois en deux séries de coups : le *pic* et le *repic* (ou *rappel*). Dans certains cas, on arrête le carillon durant la nuit pour préserver la quiétude des riverains.

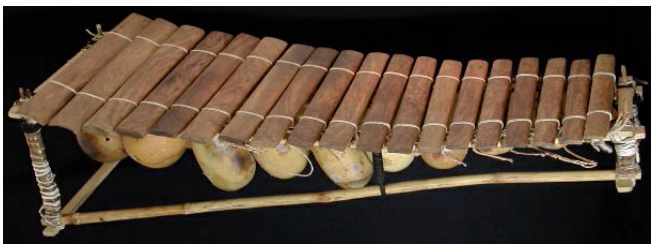
On trouve des systèmes de production de son basés sur des cloches miniatures dans des alarmes, des sonneries de téléphone, de carillon de portes d'entrée ou de réveille-matin par exemple. Pour les sons se répétant rapidement produits par de tels systèmes, le terme est *sonnette*.

Dans les zones où le cheptel bovin, ovin ou caprin est libre de stabulation, ou dans les transhumances, des clochettes appelées *sonnailles* peuvent être attachées à leur cou pour identifier les animaux appartenant à un troupeau particulier et pour aider à les trouver notamment lorsque l'on veut les rassembler. Ces cloches sont généralement fabriquées en tôle souvent rivetée, de forme trapézoïdale, cylindrique ou en forme de coupe. Il existe des concours de « musique pastorale » les utilisant.

Enfin, signalons les clochettes à main, utilisées comme moyen de communication (appeler les domestiques) ou pour ponctuer certaines cérémonies religieuses en donnant le signal de mouvements à effectuer par les fidèles.

Les xylophones

Les xylophones africains, plus connus sous le nom générique de « balafon », sont également de puissants instruments de communication. Ils sont puissants à deux titres. Compte tenu du nombre important de lames (jusqu'à plus de vingt !) ils peuvent simuler avec beaucoup de précision les phonèmes et les hauteurs tonales de la langue parlée. D'autre part, ils sont souvent conçus avec des résonateurs en calebasses comportant eux-mêmes de petits vibreurs amplificateurs.



C'est un instrument de musique fait de lamelles d'un bois spécial, sur lesquelles on frappe avec deux baguettes en bois. Il est surtout utilisé lors des manifestations de réjouissance. Contrairement au tam-tam, c'est un orchestre avec un solo, un accompagnement, une basse, qui interprète les chansons, de façon instrumentale. Les personnes-ressources qui sont aussi des fabricants sont devenues aussi rares que l'instrument. Ils servent à animer les cultes de dimanche. L'initiation est faite avec un maître de musique. C'est une tâche ardue qui demande de la volonté, de la patience et surtout un contact permanent avec l'instrument. Il faut connaître le solfège. Le temps d'apprentissage est fonction du génie de l'apprenti et peut durer de cinq à 12 mois. La portée des xylophones peut aller à plus de 1500 m. Tout le monde peut jouer de l'instrument : petits, jeunes ou adultes des deux sexes, mais c'est la rareté de l'instrument qui limite aujourd'hui son accessibilité et son utilisation. En outre, les grands joueurs ne courent plus les rues. En effet, toutes sortes de messages peuvent être transmis par les xylophones en chansons.

Systèmes de communication sonore originaux

Expérience de télégraphie acoustique faite à Paris, par Dom Gauthey, en 1782

Le 1er juin 1782, l'Académie des sciences tenait sa séance au Louvre, lorsqu'on vit entrer, conduit par Condorcet, un moine, revêtu de la robe des Bénédictins. C'était dom Gauthey, religieux de l'abbaye de Cîteaux. Il avait imaginé un moyen de correspondance entre les lieux éloignés, et il venait en faire l'exposition devant l'Académie.

Le système de dom Gauthey consistait à établir, entre des postes successifs, des tubes métalliques d'une très grande longueur, à travers lesquels la voix se propageait sans perdre sensiblement de son intensité.

Une expérience eut lieu, sur une longueur de huit cents mètres, dans un des tuyaux qui conduisaient l'eau à la pompe de Chaillot. Elle ne laissa aucun doute sur les assertions de dom Gauthey. Cependant, la création d'une « ligne » fut jugée ruineuse et la munificence royale recula devant les dépenses qu'elle devait entraîner.

Des ingénieurs distingués ont étudié, en Belgique, la question de l'établissement des tubes acoustiques. Le savant Babbage se faisait fort de causer de Londres avec une personne résidant à Liverpool. Rumford était plus hardi, il pensait que la voix humaine peut franchir ainsi des centaines de lieues.

Les locataires des prisons communiquent par l'intermédiaire des tuyaux de chauffage central ou d'eau en les frappant selon un code préétabli.

Citons, dans les systèmes « originaux » le projet de Labarthe (au XVIIe siècle), de messages codés par l'intermédiaire de coups de canon…

Lors du débarquement des troupes alliées le 6 juin 1944, les commandos étaient munis de « criquets » métalliques leur permettant d'émettre des signaux de reconnaissance.

Messagerie unilatérale et bilatérale

Nous pouvons constater à travers la description technique de ces différents outils de communication que le mode de transmission binaire - celui de l'informatique et des télécommunications numériques utilisant des suites de 0 et de 1 - est utilisé depuis la nuit des temps, bien que sous une forme différente ! Cette description nous enseigne également que les messages sont émis depuis une source unique vers une infinité de récepteurs humains (cas également de la radio messagerie) situés dans la zone de couverture sonore (notion de cellule ou de zone de couverture radioélectrique). La communication est de type multidirectionnel avec possibilité de dialogues par un système de communication similaire ou différent mais de même portée.

Les relais de transmission

Pour communiquer sur des distances supérieures à celles évoquées précédemment, les sociétés traditionnelles ont organisé des systèmes de relais de transmission. En effet, dans un village de brousse par exemple, il est aisé avec l'habitude de déterminer la provenance d'un message. Si celui-ci concerne des villages ou des individus hors de portée de l'émetteur initial, il peut être réémis autant de fois que nécessaire jusqu'à atteindre l'interlocuteur ou le groupe d'interlocuteurs concernés. Ainsi, un message peut être transmis en quelques minutes sur des distances de plusieurs dizaines de kilomètres !

Structure des messages

Pour les transmissions les plus élaborées (notamment des tambours), un message peut comporter un appel pouvant être émis plusieurs fois afin d'éveiller la vigilance des récepteurs humains (la sonnerie du téléphone !). Vient ensuite le message proprement dit, répété lui aussi plusieurs fois, puis la fermeture de la session (raccrochage du téléphone !). Les messages d'ouverture et de fermeture peuvent, selon une structure sonore immuable dans un contexte ethnogéographique donné, annoncer la nature du message. N'en est-il pas de même pour nombre de nos transmissions de messages électroniques : fréquence porteuse d'un Minitel, d'un fax, d'un modem... ?

Confidentialité

Comme pour la transmission de messages téléphonés ou écrits, le problème de la confidentialité de la communication peut se poser dans certains cas. Les messages délivrés par les divers outils sonores décrits plus haut sont émis dans toute une zone d'audition dont l'émetteur n'est pas maître. Il existe alors plusieurs niveaux de sélectivité de la compréhension. D'une manière générale, les messages sont compris pour tous les locuteurs vivant habituellement dans la zone de transmission. En revanche, le message est abscons pour toute personne ne parlant pas la langue autour de laquelle est structuré le message. Pour les interlocuteurs, le cryptage pourra s'effectuer soit par un code prédéfini, soit dans une langue secrète connue uniquement des initiés, soit encore par l'utilisation de métaphores comportant des niveaux de compréhension plus ou moins abscons selon la catégorie de population à toucher.

Et la tonalité ?

La plupart des grands tambours « parleurs » d'Afrique Noire sont, après fabrication, tels des terminaux portables ; c'est-à-dire sans tonalité. L'objet sonore ne peut émettre qu'après avoir été « initialisé » à l'aide d'un ou plusieurs sacrifices demandés par les esprits après consultation du devin (opérateur !). Bière de mil, mélange de farine de mil et d'eau ou de sang animal, argent, etc., sont offerts à l'objet sonore pour lui « donner de la voix » (tonalité !) ainsi qu'une personnalité et un nom (numéro d'appel !). Ainsi identifié, il deviendra la propriété d'un « sage » du village (abonné !) qui le gardera auprès de lui et gérera ses sorties, ses entrées, son usage et le protégera. Le « réseau » sera celui de la communauté linguistique (réseau public !) ou des seuls initiés (réseau privé !).

Impossibilités techniques

Nous savons que dans les systèmes de transmissions électroniques il n'est pas possible de transmettre tels quels deux éléments binaires consécutifs de même nature. Aussi a-t-on mis au point des systèmes de « bourrages » permettant l'alternance de niveaux (0 et 1). Le même problème se pose dans la transmission de messages codés chez les Hmong. Leur langue possédant huit tons, ils transmettent des messages à l'aide d'un orgue à bouche à six tuyaux en jouant des accords composés de ces six notes. Cependant, comme il n'est pas possible dans leur système de codage de transmettre deux tons similaires consécutifs, disposent-ils d'une syntaxe utilisant des « accords de bourrage » permettant de contourner cette impossibilité !

Conclusion

Nous pouvons constater que depuis la nuit des temps les sociétés traditionnelles se sont affranchies des problèmes de transmission instantanée de messages sur de grandes distances et de la confidentialité de celles-ci. Et cela, au nez et à la barbe de tous les monopoles...

Les messages visuels.

On peut classer les messages visuels en deux groupes : les messages passifs, les messages actifs.

Nous entendons par messages passifs, les messages visuels transmis à l'aide de pictogrammes (les panneaux de signalisation), par le port sur soi d'un signe de reconnaissance (badge, décorations) ou de vêtements particuliers (uniformes), ou de signes particuliers : chaque arrivant en Polynésie française se voit remettre un collier de fleurs de tiaré ou tout simplement une fleur de tiaré que l'on place derrière l'oreille. Si les femmes portent la fleur de tiaré épanouie (de même que la fleur d'hibiscus), les hommes portent seulement la fleur de tiaré et uniquement en bouton. De plus, si la fleur de tiaré est portée sur l'oreille gauche cela veut dire que la personne ne cherche pas de compagnie. Si celle-ci est portée à droite, cela signifie que la personne est disponible ou à la recherche de compagnie.

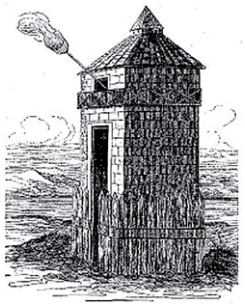
On voit donc l'importance de la communication visuelle passive.

Nous allons, dans le cadre de cet ouvrage, nous intéresser plus particulièrement à ce que nous nommons les messages visuels « actifs », c'est-à-dire créés pour communiquer à distance.

Quelques faits historiques

En 336 avant Jésus-Christ, le Grec Énée, dit le Tacticien, utilise pour la première fois des signaux visuels codés. Dans des vases remplis d'eau, des flotteurs en liège comportent une règle graduée verticale sur laquelle sont inscrits des signes. Le premier poste fait un signal avec une torche et ouvre un robinet situé en bas de son vase ; le poste suivant fait de même. Arrivé à la position de la règle qu'il souhaite, le premier poste ferme le robinet et refait un signal avec sa torche : le poste suivant répète le mouvement et connaît ainsi la position de la règle : il ne reste qu'à traduire.

En 150 avant notre ère, l'historien grec Polybe utilise des signaux alphabétiques à l'aide de deux groupes de cinq torches bien séparés. L'alphabet est divisé en cinq groupes. Les torches de gauche indiquent le groupe de lettres qu'il faut utiliser (par exemple, deux torches allumées signifient deuxième groupe de lettre), les torches de droite la lettre qu'il faut prendre (une torche, par exemple, désigne la première lettre du groupe).



Les Romains franchissent l'étape suivante en mettant en place un système permanent de relais qu'ils placent dans des tours tenues par des stationnaires militaires tout autour de la Méditerranée. Ces tours communiquaient par signaux de torches et on en aurait compté environ 1197 en Italie, 1200 dans les Gaules, 500 en Asie. On connaît l'aspect d'une de ces tours gravée sur la Colonne Trajane et dont on trouvera le dessin ci-contre, extrait d'un ouvrage italien du siècle dernier (« *Telegrafia ottica* » de B. Zanotti).

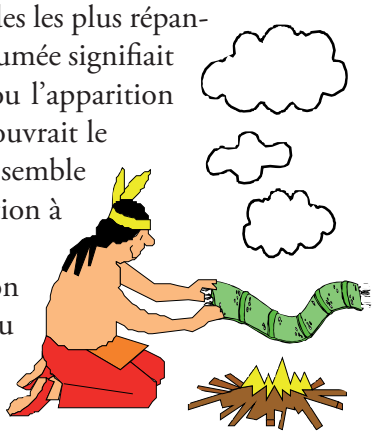
L'art des signaux fut également mis en pratique chez les anciens peuples d'Orient. Les Scythes faisaient usage de feux ou de fumée, comme moyen d'avertissement lointain. Les Chinois, chez lesquels on trouve toujours quelques traces des inventions modernes de l'Occident, avaient placé des phares, ou machines à feu, sur leur grande muraille, longue de 188 lieues. Ils pouvaient ainsi donner l'alarme à toute la frontière qui les séparait des Tartares, lorsqu'une horde de ces peuples venait à les menacer.

A Constantinople, les signaux de feu placés sur une montagne voisine, annonçaient, en peu d'heures, les mouvements des Sarrasins. Le premier poste était près de Tarse. Venaient ensuite ceux des monts Argent, Isamus, Egésus, la colline de Mamas, et le cadran du phare du palais.

Le plus énergique et le plus clair de tous les télégraphes physiques employés par les Orientaux, était celui de Tamerlan. Ce conquérant terrible, quand il faisait le siège d'une ville, n'employait que trois signaux. Le premier était un drapeau blanc, et voulait dire : « Rendez-vous, j'userai de clémence. » Le second jour, Tamerlan faisait arborer un drapeau rouge, qui signifiait : « Il faut du sang, le commandant

en place et les sous-officiers payeront de leur tête le temps qu'ils m'ont fait perdre. » Le troisième et dernier signal était un drapeau noir, et voulait dire : « Que la ville se rende ou qu'elle soit prise d'assaut, je mettrai tout à feu et à sang. »

Les signaux de fumée.



Les Indiens d'Amérique du Nord usaient de signaux de fumée. Les codes les plus répandus, chez les Sioux et les Cheyennes étaient fort simples. Une bouffée de fumée signifiait « attention », deux bouffées signifiaient « tout va bien », trois bouffées ou l'apparition de flammes se traduisaient par « danger, on demande de l'aide ». On recouvrait le feu d'une étoffe et on le découvrait pour obtenir une bouffée de fumée. Il semble que la forme la plus ancienne de ces signes destinés à porter de l'information à distance est le feu, car la fumée qui s'en échappe est visible de loin.

La source la plus ancienne décrivant un tel système de communication à distance par le feu est sans aucun doute le Talmud. Certains passages du Talmud évoquent en effet l'existence d'un réseau de communication établi entre Jérusalem et Babylone. Des feux étaient allumés sur des tours ou des lieux élevés. Il semble que le code utilisé était fonction de la durée des feux allumés, de la hauteur des flammes et peut-être de la coloration : mais il ne s'agit que d'hypothèses, etc.

Par exemple, au temps jadis, c'était la coutume pour le Beth Dine (Cour de justice) en Erets Israël, de répandre la nouvelle de la sanctification de Roche-'Hodèche (Nouvelle Lune) au moyen de feux qu'on allumait sur les collines entourant Jérusalem. Ce signal par les feux était rapidement reçu, puis transmis d'une colline à l'autre, jusqu'à ce que tout le pays fût informé du jour de Roche-'Hodèche, et que tout un chacun sût le temps adéquat pour l'observance des fêtes.

De nos jours, la couleur de la fumée (noire ou blanche) indique les résultats du scrutin lors de l'élection du pape.

Autrefois, les soldats engagés dans une guerre se servaient de messages éclair en réfléchissant les rayons du soleil sur la surface polie de leurs boucliers.

Les phares et les sémaphores.

Le mot phare, vient du grec Pharos, qui est le nom de l'île où se trouvait le Phare d'Alexandrie. Cette origine est conservée dans beaucoup de langues, comme dans l'italien (faro), l'espagnol (également faro) et le portugais (farol). Cependant, certaines langues comme l'anglais ont tout simplement créé un nom composé (*lighthouse*), expliquant clairement la fonction du phare.

Le phare d'Alexandrie fut considéré comme la dernière des sept merveilles du monde antique et a servi de guide aux marins pendant près de dix-sept siècles (du III^e^ siècle av. J.-C. au XIV^e^ siècle). La construction du Phare aurait débuté vers -297 (la date exacte est inconnue) et duré une

quinzaine d'années. Les travaux sont initiés par Ptolémée I^er^ mais celui-ci meurt avant la fin du chantier qui est achevé sous le règne de son fils Ptolémée II.

Les phares ont généralement une fonction « passive » : signaler les écueils, les passes, matérialiser les positions géographiques. Mais il est très probable qu'ils aient été utilisés aussi pour communiquer dans l'Antiquité.

A sa création en 1806 par Louis Jacob sous Napoléon, le *sémaphore* était un poste de guet établi sur la côte, chargé de surveiller les approches maritimes et de signaler par signaux optiques toute activité ennemie (le mot sémaphore vient du grec *sema* : signe, et *phoros* : qui porte).

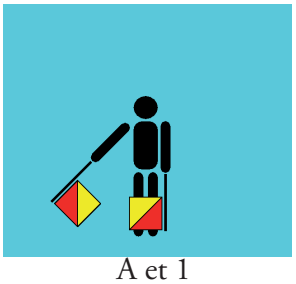
Aujourd'hui, le sémaphore est un poste de surveillance en bord de côte qui assure des missions diversifiées qui vont de l'assistance à la navigation jusqu'à la surveillance du territoire en passant par la régulation du trafic maritime et de la pêche.

Pour exercer ces missions, le personnel du sémaphore dispose d'une *chambre de veille* équipée de larges baies vitrées et de puissantes paires de jumelles donnant sur la zone maritime à surveiller, d'un radar et de moyens de radio communication. Le sémaphore est installé sur un point culminant de la côte si le relief s'y prête ; la chambre de veille est généralement au sommet d'un bâtiment qui parfois s'apparente à un phare (sémaphore du Stiff)

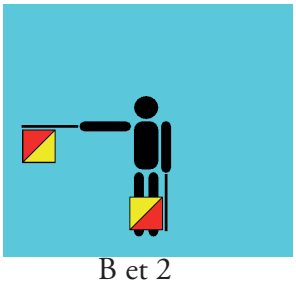
Les sémaphores sont échelonnés tout au long des côtes françaises, chacun couvrant un secteur maritime.

Le réseau des sémaphores est de la responsabilité de la Marine nationale qui les arme en personnel militaire (guetteurs sémaphoriques).

Sous le nom de *sémaphore*, on désigne également le moyen de communication visuelle utilisé dans la Marine pour transmettre des messages d'un navire à l'autre. Il s'agit d'un « alphabet visuel » formé par la position relative de drapeaux portés par un homme :



A et 1



B et 2

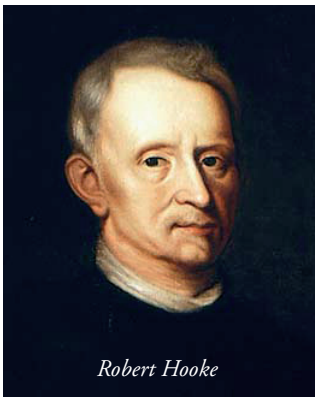
Nous abordons là des procédés de communication semblables aux systèmes utilisés par les premiers télégraphes.

Le télégraphe

Le télégraphe

Comme l'indique son nom, tiré du grec et composé avec beaucoup de justesse de τῆλε, loin, et γράφω, j'écris, un télégraphe est un appareil qui écrit à longue distance, c'est-à-dire destiné à faire parvenir rapidement un message, à l'aide de signaux, entre deux points éloignés. Le mot *télégraphe* a été inventé en 1793 par le Comte Miot de Mélito.

Nous allons d'abord étudier les formes de télégraphes visuels, gardant pour un autre chapitre les systèmes électriques.


Robert Hooke

La première description technique d'un dispositif de transmission de signaux par sémaphore a, semble-t-il, été présenté par Robert Hooke en 1684. Robert Hooke, né le 18 juillet 1635 à Freshwater et mort le 3 mars 1703, est un des plus grands scientifiques expérimentaux du XVII[e] siècle et donc une des figures clés de la révolution scientifique de l'époque moderne. On considère souvent Hooke comme l'inventeur du microscope. Il avait intitulé son système : « *Moyen de faire connaître sa pensée à distance* ».

La machine de Robert Hooke consistait en un large écran, c'est-à-dire une planche peinte en noir, placée au milieu d'un châssis, et élevée à une grande distance en l'air. Divers signaux, de forme particulière, étaient cachés derrière l'écran, et servaient, quand on les faisait apparaître, à exprimer les lettres de l'alphabet. Quelques signaux n'exprimaient pas des lettres, mais des phrases convenues d'avance.

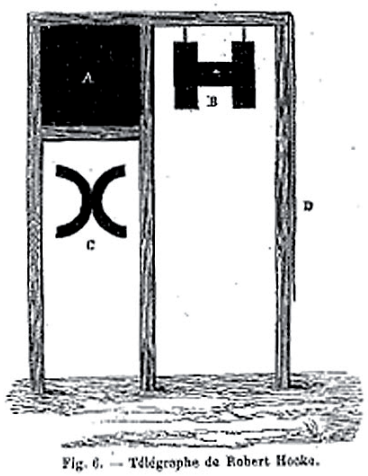


Fig. 6. — Télégraphe de Robert Hooke.

La figure ci-contre représente le télégraphe de Robert Hooke. « A » était la planche peinte en noir derrière laquelle étaient cachés les signaux, « B, C », que l'on faisait apparaître à volonté en tirant la corde « D ».

Quelques années plus tard, en 1690, le physicien français Guillaume Amontons (31 août 1663 - 11 octobre 1705) réalise, dans le jardin du Luxembourg, une première expérience de communication par sémaphore. Fontenelle[8] nous cite cette expérience qui aurait été menée deux fois, et qui consistait à transmettre un message entre deux points par le biais de signaux optiques émis par un poste, et intercepté par le poste suivant grâce à une longue-vue, qui lui-même le transmettait au poste suivant, jusqu'au point d'arrivée. Chaque lettre de l'alphabet avait son signal dont la signification n'était connue que des postes extrêmes. Cette invention ingénieuse n'est cependant rapportée que dans les registres de l'Académie, et il n'est nullement évident qu'Amontons, même si on peut lui accorder l'idée, ait effectivement réalisé l'opération.

Un autre inventeur du nom de Guillaume Marcel était parvenu, après plusieurs années de recherches à construire une machine qui transmettait des avis dans le temps qu'il aurait fallu pour les écrire. Il adressa à Louis XIV un mémoire descriptif, avec des dessins de son appareil. Ce mémoire resta sans réponse, le roi était vieux, il commençait à négliger, pour le royaume du Ciel, son royaume terrestre… Fatigué d'attendre, et dans un moment de désespoir, il brisa sa machine et jeta au feu ses dessins. Il mourut en emportant son secret.

Au XVIII[e] siècle, plusieurs inventeurs feront des expériences analogues, sans plus de succès, aucune de ces démonstrations ne débouchera sur un véritable dispositif de communication à distance.

---

[8] Bernard Le Bouyer de Fontenelle est un écrivain français né à Rouen, le 11 février 1657 et mort, presque centenaire, à Paris le 9 janvier 1757. Son intelligence souple et lucide a très bien servi les lettres et surtout les sciences, qu'il sait excellemment rendre accessibles et même attrayantes, en gardant l'exactitude. La qualité d'homme de lettres fut relevée par la brillante considération attachée à la personne de cet académicien qui fut un familier du duc d'Orléans et de Fleury.

De nombreux textes font allusion au télégraphe et, en 1788, un certain Dupuis tente de transmettre par télégraphe alphabétique des messages entre Ménilmontant et Bagneux.

L'usage envisagé pour les dispositifs télépathiques ou télégraphiques par la littérature de l'époque est principalement la communication amoureuse. Dans le très sérieux *Mechanics Magazine* on peut encore lire, au début du XIXe siècle, à propos du sémaphore « *qu'un amant pourra transmettre de façon manifeste ses sentiments à sa belle. Et sa languissante maîtresse apprendra des longs bras du télégraphe quand elle pourra se consoler dans les bras de son bien-aimé* »[9]. Au XVIIIe siècle, les dispositifs de communications à distance qu'ils soient réels ou imaginaires renvoient donc à un usage galant. Aussi le télégraphe optique qui est connu et expérimenté dès la fin du XVIIe siècle ne se développera pas pendant un siècle, faute d'avoir trouvé une structure sociale appropriée capable non seulement d'imaginer l'intérêt de la communication à distance, mais également de soutenir la construction d'un réseau permanent. Mais ces systèmes seraient sans doute restés à l'état expérimental ou à l'état débauche sans la Révolution française de 1789, avec la création de l'État moderne, un agent social prêt à prendre en charge la mise en place d'infrastructures permanentes, et surtout sans les guerres révolutionnaires. Pour communiquer aussi rapidement que possible, et en secret, avec les armées aux frontières, le pouvoir central avait besoin d'un système assurant à la fois rapidité, discrétion et possibilité de réponse immédiate. Trop de messagers ou d'estafettes à cheval avaient été interceptés, capturés et avec eux les messages qu'ils transportaient.

Vers 1790, une diligence pouvait porter un message de Paris à Strasbourg en *quatre jours.* En 1799, le même message mettra moins de*... 2 heures !*

L'usage veut que le télégraphe aérien soit l'œuvre de son inventeur, Claude Chappe. En réalité, la réussite fascinante du télégraphe optique et aérien n'est pas due seulement à une invention géniale, mais à la complémentarité de toute une famille originaire de Brûlon, petit village de la Sarthe.

Claude Chappe

L'instigateur du projet est Claude Chappe, dit Chappe de Vert, né en 1763, deuxième enfant d'une famille de cinq frères. Après de solides études, il jouit de rentes qui lui permettent d'ouvrir un cabinet de physique à Paris. Il suit ainsi l'exemple de son oncle, le célèbre abbé Jean Chappe d'Auteroche. Il y réalise diverses expériences, notamment dans le domaine de l'électricité et dans différents autres domaines, participant ainsi à l'élan scientifique du « Siècle des Lumières ».

En bon scientifique du XVIIIe siècle, Chappe s'intéresse aux découvertes antiques. La communication visuelle sur de grandes distances a été expérimentée dès l'antiquité. Elle est réalisable avec le principe d'un message relayé de poste en poste. Chaque relai, pour être visible du suivant, doit être placé en terrain découvert ou sur une hauteur. Le message doit également être codé et sa transmission doit s'effectuer au moyen de signaux simples.

Claude Chappe réalise sa première expérience publique de communication à distance et qu'il nomme *tachygraphe* le 2 mars 1791, à l'âge de 26 ans.

Le système consiste en deux cadrans mobiles dotés d'aiguilles et de chiffres, installés respectivement dans son village natal de Brûlon et le village de Parcé distants de 14 km.

L'expérience, qui consistait à envoyer un message dans chaque sens fut réussie. Elle fut authentifiée par un compte-rendu officiel dont voici le texte :

« *Aujourd'hui 2 mars 1791, sur les onze heures du matin, nous officiers municipaux de Brulon, district de Sablé, département de la Sarthe, nous nous sommes rendus avec MM Avenant de La Maisonneuve praticien, demeurant à Brulon, ci-devant château dudit Brulon, sur l'invitation qui nous en était faite, à l'effet d'être*

[9] *Mechanics Magazine,* 24 novembre 1827.

témoins, et d'assurer l'authenticité d'une découverte de M. Claude Chappe, neveu du célèbre abbé de ce nom, tendante à se correspondre, et à se transmettre des nouvelles dans un très court espace de temps.

« D'abord nous sommes montés avec le sieur René Chappe, frère du sieur Claude Chappe, à la terrasse pratiquée sur le haut du château, et y avons trouvé un pendule et un tableau mobile à deux faces dont une blanche et l'autre noire.

« Et de suite le sieur René Chappe nous a fait observer que le sieur Claude Chappe étant actuellement établi à Parcé, distant de Brulon de quatre lieues, pour recevoir ce qui alloit lui être transmis, il nous prioit de lui dicter telle phrase, ou telles séries de phrases qu'il nous plairoit. En conséquence, M. Chenou, médecin, a proposé la phrase suivante : « Si vous réussissez vous serez bientôt couvert de gloire. »

« Aussitôt ledit sieur René Chappe, après nous avoir fait remarquer que le temps étoit pluvieux, et que l'atmosphère étoit obscurcie par un léger brouillard, a receuilli ladite phrase, et ayant procédé à sa transmission par divers mouvements du tableau, ce qui a duré l'espace de quatre minutes, il nous a dit que la susdite phrase étoit actuellement parvenue à Parcé ; que le rapprochement du procès-verbal, dressé par les officiers municipaux dudit lieu, en feront foi.

Fait et arrêté à Brulon, au susdit château, l'heure de midi, lesdits jours en an ci-dessus.

Suivent les signatures : « Chenou, Lemore, Tant, Tison, maire ; Avenant, vicaire ; Audruger Maisonneuve. »

« Et le même jour, sur les trois heures après midi, nous nous sommes transportés, accompagnés des témoins dénommés au procès-verbal de ce matin, au susdit château ; montés à la terrasse du susdit château, le sieur René Chappe nous a prié de lui dicter ce qu'il nous plairoit, pour qu'il put le transmettre à son frère, à Parcé. Après lui avoir dicté la phrase ci-après : « L'assemblée nationale récompensera les expériences utiles au public », il a procédé à divers mouvements du tableau pendant l'espace de six minutes et quelques secondes, et nous a dit que notre phrase étoit actuellement parvenue à Parcé.

Fait et arrêté à Brulon, au château dudit lieu, sur les quatre heures après midi, lesdits jours et an que dessus. »

Suivent les signatures : « Lemore, Chenou, Tison, maire : tant ; Avenant, vicaire ; Audruger Maisonneuve. »

« Le lendemain 3 mars 1791, sur les dix heures et demi du matin, nous officiers municipaux de Brulon, rendus à la terrasse du château de Brulon, avons donné, en présence de MM. Avenant, vicaire, et Audruger de La Maisonneuve, praticien, à transmettre au sieur Claude Chappe, à Parcé, plusieurs phrases très intelligibles, composées de vingt-cinq mots.

« Le sieur René Chappe a effectué diverses manipulations, ce qui a duré environ dix minutes, et nous a dit que la transmission des phrases que nous venions de lui dicter étoit faite ; que le procès-verbal dressé au même moment par les officiers municipaux de Parcé la constateroit. »

Fait et arrêté au château dudit Brulon, lesdits jours et an que dessus.

Suivent les signatures : « Chenou, Lemore, Tison, maire ; Tant ; Avenant, vicaire ; Audruger Maisonneuve. » Source : *Archives de la Sarthe.*

Nous n'avons malheureusement pas trouvé les procès-verbaux des officiers municipaux de Parcé…

Le mot *télégraphe* a été proposé et utilisé en remplacement du mot « *tachygraphe* » inventé par Chappe.

Les techniques du télégraphe Chappe

Le principe du télégraphe optique est simple. Il repose sur un mécanisme visible de loin, amélioré par l'usage d'une lunette et l'utilisation d'un code de transmission.

Comme il doit être visible de loin, le télégraphe est placé sur une hauteur : montagne, colline, ou monument existant tel que clocher d'église, tourelle de château,... Quand ce n'est pas possible, on le place sur le toit d'une construction en bois ou sur une tour, carrée ou ronde, sans tenir compte de l'esthétique : devant l'urgence de la situation, le bois a été le matériau le plus employé, remplacé par la suite par des constructions en pierres. Il n'existe par ailleurs aucun plan-type de construction, à l'exception peut-être des dernières tours plus adaptées aux machines de type Flocon.

L'appareil définitif et complet, appelé poste ou station, comprend donc deux parties : une partie visible de loin, et une partie abritée. Cette dernière est elle-même divisée en deux pièces : l'une d'elle sert à la manipulation des bras du télégraphe et l'autre de salle de repos aux stationnaires.

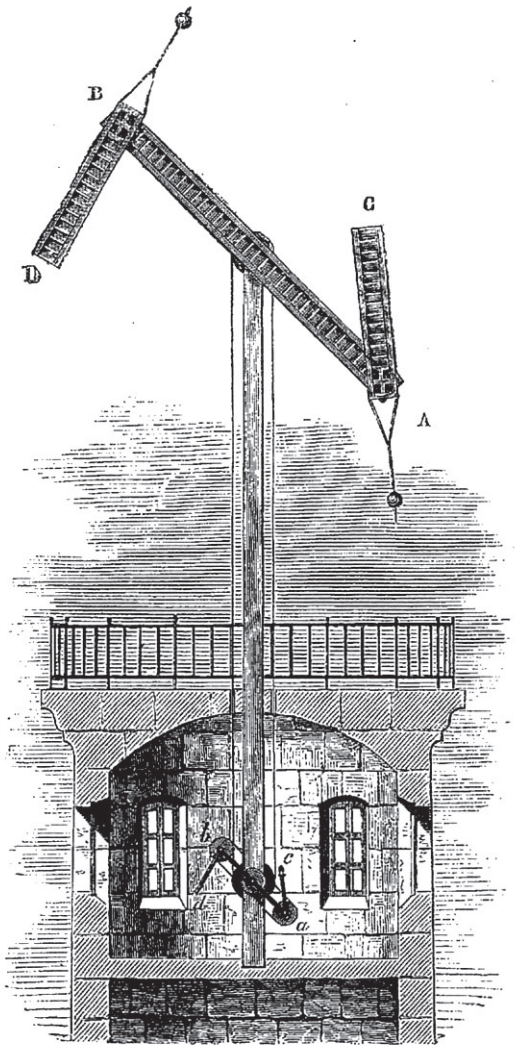
Il n'existe pas de modèle unique de télégraphe, comme il n'existe pas non plus aujourd'hui de modèle unique d'appareil téléphonique. Les modèles ont évolué dans le temps, vers une plus grande robustesse et une plus grande lisibilité.

Le télégraphe proprement dit, ou la partie de la machine qui forme les signaux, se compose de trois branches mobiles : une branche principale AB, de 4 mètres de long, appelée *régulateur*, et deux petites branches longues de 1 mètre, AC, BD, appelées *indicateurs*, *ou ailes*. Deux contrepoids en fer *p, p'* attachés à une tige de même métal, font équilibre au poids des ailes, et permettent de la déplacer avec très peu d'effort. Ces tiges sont assez minces pour n'être pas visibles à distance. Le régulateur est fixé par son milieu à un mât ou à une échelle, qui s'élève au-dessus du toit de la maisonnette dans laquelle se trouve placé le stationnaire.

Les branches mobiles sont découpées en forme de persiennes, c'est-à-dire composées d'un cadre étroit, dont l'intervalle est rempli par des lames minces, inclinées les unes au-dessus des autres. Cette disposition a l'avantage de donner aux pièces une grande légèreté ; elle leur permet aussi de résister aux vents et de combattre les mauvais effets de la lumière. Les branches mobiles sont peintes en noir, afin qu'elles se détachent avec plus de vigueur sur le fond du ciel. L'assemblage de ces trois pièces forme un système unique, élevé dans l'espace, et soutenu par un seul point d'appui : l'extrémité du mât, autour duquel il peut librement tourner.

Les pièces du télégraphe se meuvent à l'aide de cordes de laiton. Ces cordes communiquent, dans la maisonnette, avec un petit appareil, qui est la reproduction en raccourci du télégraphe extérieur. C'est le second appareil que l'employé manœuvre ; le télégraphe placé au-dessus du toit ne fait que répéter les mouvements imprimés à la machine intérieure.

Le mécanisme qui permet de manœuvrer les branches du télégraphe se réduit à une large poulie à gorge, sur laquelle est attachée et fortement tendue une corde de laiton, qui vient s'enrouler sur une autre poulie fixée à l'axe du télégraphe. Quand le levier *ab* du régulateur du petit appareil placé dans la maisonnette est abaissé par le stationnaire, la corde de laiton qui tourne autour de ce levier est tirée, et le bras du régulateur AB du télégraphe mis en action, reproduit le même mouvement. Quand les leviers *ac* ou *bd* du petit appareil de la maisonnette, sont, de la même manière, mis en action, les cordes qui vont



de ces petits leviers *ac*, *bd*, aux ailes AB, BD du télégraphe extérieur, étant tirées, font prendre aux ailes de ce télégraphe la même position.

Tout s'accomplit donc par un jeu de cordes et de poulies, et le stationnaire, sans sortir de sa maisonnette, sans regarder par-dessus sa tête, ce qui lui serait difficile, peut exécuter, à coup sûr, les signaux qu'il doit faire. Le télégraphe placé au-dessus du toit reproduit exactement, comme nous l'avons déjà dit, les signaux de l'appareil intérieur.

Le régulateur AB est susceptible de prendre quatre positions : verticale — horizontale — oblique de droite à gauche — oblique de gauche à droite. Les ailes AC, BD peuvent former avec le régulateur des angles droits, aigus ou obtus. Ces signaux sont clairs, faciles à apercevoir, faciles à écrire, il est impossible de les confondre.

On distingue trois grandes familles d'appareils dits de Lille, de Strasbourg et de Milan. En fait, il s'agit d'améliorations apportées au fur et à mesure de l'ouverture des lignes. Différents facteurs créent également des variantes dans les appareils, pour cause de réparations lors des faits de guerre (en 1814 - 1815) ou du réemploi de matériel émanant des lignes démontées.

Enfin, il existe également des « modèles spéciaux » : télégraphes ambulants, télégraphes horizontaux (modèle Flocon, modèle algérien)...

Chaque station est éloignée d'une dizaine de kilomètres de sa voisine. Elle est donc équipée de deux lunettes afin de permettre la lecture et la vérification du code transmis. Bien que les appareils courants aient donné entière satisfaction, ils sont perfectibles. Différentes améliorations sont envisageables. En 1837, Jacques Gabriel Flocon, administrateur du télégraphe propose un nouveau modèle d'appareil. Son système supprime le régulateur central et le rend fixe. A la place, on trouve un petit régulateur mobile placé en haut du mât. L'ensemble est beaucoup plus léger que le mécanisme d'origine et les manipulations sont beaucoup plus rapides : on passe de 2 à 3 signaux par minute à environ 5 à 6. Les dernières ramifications construites à partir de 1840 en seront équipées.

Le code ou vocabulaire

Le message passe de station en station, chacune distante de la suivante de 6 à 12 Km en moyenne. L'utilisation d'un code est rendue nécessaire pour résoudre deux problèmes :

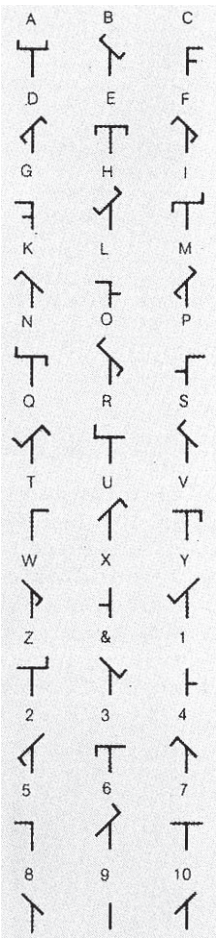
— la lenteur : transmettre un message lettre par lettre aurait été beaucoup trop long : il faut donc le condenser ;

— la confidentialité : le message est compréhensible pour l'expéditeur et le destinataire, mais doit rester incompréhensible pour tous les intermédiaires.

Le code ou vocabulaire est dépendant des pièces mobiles du télégraphe. Pour des raisons de lisibilité, seuls des angles de 45° sont utilisés par les deux ailes, soit 7 positions pour chaque aile. Seules deux positions, horizontale et verticale, sont à retenir pour le régulateur, les obliques étant réservées à la fabri-

cation du signal ou au service. Il reste donc 7 X 7 X 2 = 98 positions et donc signaux de base. Six sont nécessaires pour le service et il reste donc 92 signaux utilisables pour le message.

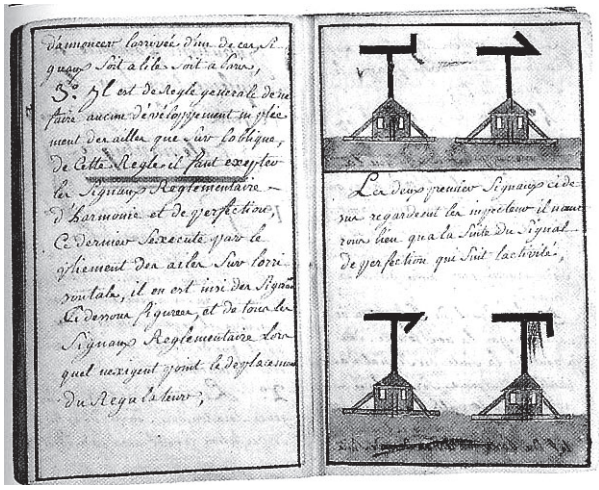
Le premier code en usage avec le télégraphe aérien des frères Chappe comprenait 36 signaux permettant la transmission de n'importe quel message (ci-contre).



Puis en 1794, ils composent un répertoire de 92 pages. Sur chaque page figurent 92 lignes. Chaque ligne comporte un mot ou groupe de mots. On possède donc 92 X 92 = 8464 significations possibles par code (et on peut utiliser plusieurs répertoires complémentaires). C'est le *vocabulaire des mots*. Un second vocabulaire que l'on nomme vocabulaire des phrases est formé, comme le précédent, de 92 pages contenant chacune 92 phrases ou membres de phrases, ce qui donne 8464 idées. Ces phrases s'appliquent particulièrement à la marine et à l'armée. Pour se servir de ce vocabulaire, le télégraphe donne trois signaux.

On émet des signaux par groupes de deux, le premier pour la page, le second pour la ligne de la page.

Le code ou vocabulaire a évolué au fil des temps : il passe de 10 à 50, puis à 98 signaux. Le premier vocabulaire, de 9999 mots, utilisé sur la ligne de Lille exigeait à 90% quatre signaux. Claude Chappe, le mathématicien Delaunay et le premier Directeur de Metz, Mathieu Xavier Durant, mettent au point le système le plus utilisé.



Le répertoire appelé vocabulaire sera détenu, jusqu'aux environs de 1806, uniquement par les directeurs des stations extrêmes. Sur la ligne de l'Est par exemple, seuls Paris et Strasbourg étaient dans ce cas. Il faudra attendre cette date pour que le directeur de Metz, direction intermédiaire, puisse à son tour décoder les messages. Les messages décodés appelés « dépêches » étaient transmis ensuite à leur destinataire par messager.

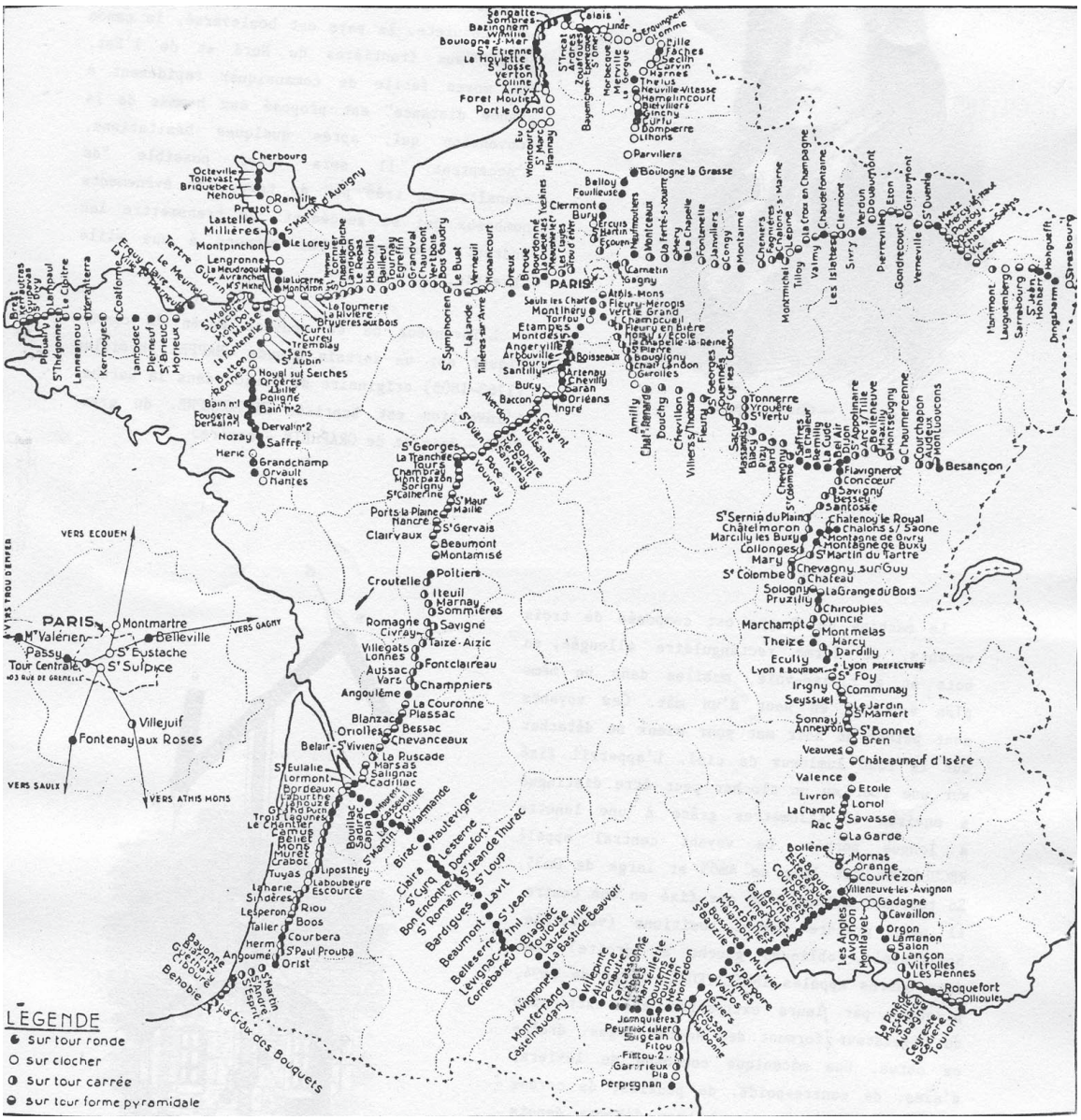
Compte tenu des besoins, deux nouveaux vocabulaires seront mis en service en 1807 et 1841.

On utilisait également des tableaux de chiffres pour la Loterie Nationale ou des tableaux de signaux.

Enfin, pour des raisons que l'on ignore encore (la hantise du secret n'explique peut-être pas tout), le Directeur de Metz, Jean-Pierre Rogelet (1775-1852), utilisait pour enregistrer ses messages en partance une forme ancienne de sténographie (actuellement en cours de déchiffrement, grâce aux travaux de l'Association Mont St Quentin). Il semble que lui seul ait utilisé cette méthode (même lorsqu'il était « simple » Inspecteur).

Le secret de la communication à distance par voie optique consistait à disposer dans plusieurs postes consécutifs des gens qui, par des lunettes de longue-vue, ayant aperçu certains signaux du poste précédent, les transmettaient au suivant et ainsi de suite ; ces différents signaux étaient autant de lettres d'un alphabet dont on n'avait le *chiffre* qu'à Paris et à Rome. La plus grande portée des lunettes faisant faisait la distance des postes, dont le nombre devait être le plus petit possible : et comme les signaux envoyés au troisième poste se faisaient à mesure que le second les voyait faire au premier, la nouvelle se trouvait portée à Rome presque en aussi peu de temps qu'il en fallait pour faire les signaux à Paris.

Le réseau



Convaincue par Lakanal, en date du 27 juillet 1793, « *La Convention nationale accorde au citoyen Chappe, le titre d'ingénieur thélégraphe (!), aux appointements de lieutenant de génie, charge son Comité de Salut public d'examiner quelles sont les lignes de correspondance qu'il importe à la République d'établir dans les circonstances présentes...* ».

En fait, les circonstances sont dramatiques, car les ennemis menacent le nord du pays. La première ligne qui sera établie sera donc celle de Paris à Lille. Grâce à la rapidité des transmissions, les Conventionnels sont convaincus de l'utilité du télégraphe et le réseau commence à se constituer. En fonction des circonstances militaires et politiques, il continuera son expansion jusqu'au milieu du 19e siècle, moment où d'autres moyens de communication prendront le relai.

L'établissement des lignes diffère donc suivant les gouvernements en place et on peut distinguer quatre grandes phases de construction en France même :

— La formation du réseau : il se fera sous la Révolution, entièrement dictée par l'urgence de la situation militaire ;

— L'expansion du réseau : si Bonaparte, Premier Consul, fit fermer les lignes pour mettre fin aux désordres révolutionnaires, Napoléon, Empereur des Français, les fit rouvrir : les lignes impériales prirent ainsi une dimension européenne ;

— Le recentrage sous la Restauration : les Chappe remportèrent leurs dernières victoires en réussissant à le recentrer sur l'Hexagone ; le réseau prend ainsi la forme d'une étoile autour de la capitale, schéma désormais devenu classique ;

— La fin du télégraphe optique : avec la Révolution de 1830 éclate également la disgrâce définitive des frères Chappe : les dernières lignes se feront sans eux, mais les nouveaux moyens de communication se profilent déjà à l'horizon et le télégraphe Chappe arrêtera ses dernières transmissions en France en 1854.

À partir de la Révolution de juillet, la France commence à se lancer dans l'expansion coloniale. L'armée de conquête a besoin d'un système de transmission rapide, sûr et efficace et le télégraphe aérien va franchir la Méditerranée à partir de 1835. Il survivra jusqu'en 1859/1860 en Algérie, donc bien après la fin en métropole. Il sera également introduit en Tunisie à partir de 1848, mais nous ne savons pas pour l'instant ce que ce télégraphe est devenu.

En 1840, le réseau conçu par les frères Chappe et le mécanicien Breguet (ancêtre de l'aviateur et avionneur) représente en France plus de 4000 kilomètres de lignes, disposant de 556 postes de relais formant 8 lignes principales et 11 embranchements.

Un corps important de *stationnaires* (responsables des manipulations des sémaphores) est constitué. Une administration centralisée est mise en place. Mais surtout, l'information est codée et la transmission est assurée par des relais. Il est significatif de constater que nombre de tours modernes de relais hertziens se trouvent situés à l'emplacement des anciens sémaphores du système Chappe. Surtout, ce système représente un modèle d'un ensemble de signes qui constitue une forme économique de transmission. C'est-à-dire qu'avec un nombre restreint de signes on peut émettre, transmettre et recevoir un nombre important de messages.

L'inconvénient du système, comme de tous les systèmes de signes se transmettant visuellement dans l'atmosphère, est que son fonctionnement dépend des conditions météorologiques. Par temps de brouillard, de pluie ou d'orage, ou par trop grand soleil à cause de la réverbération, le télégraphe optique était inutilisable, de même que la nuit…

Les usages du télégraphe

L'imagination sociale télégraphique est bien sûr en décalage avec les usages effectifs. Rabaut-Pommier déclare en 1795 : « *Un jour, lorsque la paix permettra le perfectionnement des inventions utiles, le télégraphe appliqué au commerce, à la physique, à la politique, même à l'agriculture, multipliera les moyens de communication et les rendra plus utiles par leur rapidité. Déjà l'auteur de cette heureuse invention l'a employée à annoncer les orages.* »[10] En fait, l'extension des usages du télégraphe en dehors du domaine militaire est très restreinte. En 1799, Chappe propose au Directoire d'utiliser le télégraphe pour transmettre le cours des changes et annoncer l'arrivée des bateaux dans les ports. En 1801, sous le Consulat, il renouvelle sa proposition en l'étendant à la diffusion des résultats de la Loterie Nationale et à la transmission d'un bulletin d'information officielle approuvé par le premier consul. Seul le projet concernant la Loterie Nationale est retenu. Plusieurs historiens voient là le refus de l'État d'ouvrir ses réseaux de communication au privé. Ce n'est pas l'unique raison : ces projets nécessitent d'étendre le réseau en direction des ports alors que le premier consul vient de diviser par trois le budget des services télégraphiques.

Les raisons de l'échec de l'extension des usages du télégraphe sont plutôt à chercher du côté des insuffisances de la demande. La révolution industrielle est encore balbutiante en France, la demande de trans-

[10] *Le Moniteur universel*, 29 avril 1795.

mission rapide d'informations industrielles et commerciales est restreinte. Pendant la Révolution et l'Empire, les usages du télégraphe sont essentiellement militaires, sous la Restauration plutôt de police. Abraham Chappe décrit bien dans une lettre de 1832 le rôle du télégraphe après l'Empire : les lignes télégraphiques « *apportent au centre du gouvernement, avec la rapidité de la pensée, toutes les sensations politiques* [...]. *Cette communication vérifie tous les rapports administratifs, elle donne plus d'unité à l'action* [...]. *Lorsque le gouvernement doit être prêt à se défendre contre les attaques des partis, lorsque chaque minute doit être mise à profit* […] *un pareil moyen doit être considéré, à juste titre, comme un des ressorts administratifs les plus puissants et les plus dignes d'intérêt. La télégraphie est donc un élément de pouvoir et d'ordre* »[11].

La construction des lignes est le plus souvent liée à une demande spécifique dépendante des événements. La première ligne Paris-Lille est construite sous la Convention pour communiquer avec l'armée du Nord. Le Directoire demande d'établir la ligne de Strasbourg pour pouvoir communiquer avec ses plénipotentiaires lors du congrès de Rastadt. Napoléon, pour resserrer ses communications avec l'Italie, veut faire construire la ligne Lyon-Milan en quinze jours. Après la campagne de Russie, il demande également la construction d'urgence d'une ligne Strasbourg-Mayence. De même sous la Restauration une ligne Paris-Bayonne est construite en préparation de l'expédition d'Espagne de 1823.

De tels principes de construction du réseau interdisent de répondre effectivement à un développement de la demande militaropolicière. En 1829, voulant plaider pour la construction d'un réseau cohérent, Abraham et René Chappe rappellent qu'en 1815 la nouvelle du débarquement de Napoléon dans le golfe Juan ne fut connue à Lyon que trois jours après, de là un télégramme partit pour Paris.[12] La ligne Lyon-Toulon ne sera construite qu'en 1821.

Les autres réseaux européens

À l'étranger, le télégraphe aérien se développe également selon le rythme de l'activité militaire. L'Amirauté britannique construit de 1796 à 1808 des lignes télégraphiques entre Londres et quatre ports de la côte. En 1814, ces lignes seront fermées. De même aux Pays-Bas, un télégraphe est construit en 1831 pendant la guerre d'indépendance de la Belgique, il sera arrêté dès la fin de la guerre.

L'installation d'un dispositif de transmission permanent pour les besoins de l'État ne se développe — à l'exception de la France — que plus tardivement. La Grande-Bretagne installe pour les besoins de l'Amirauté un réseau de sémaphores dans les années 1820. Il est intéressant de constater qu'après avoir fermé les lignes qui servaient pendant les guerres napoléoniennes et avoir déclaré en 1816 à Ronalds, un inventeur de télégraphe électrique, « *que des télégraphes de quelque nature que ce soit sont complètement inutiles* »,

[11] Lettre d'Abraham Chappe du 23 août 1832 (*Archives nationales*, F90 1427).
[12] Abraham et René Chappe, *Mémoire sur la télégraphie*, Imprimerie Béthune, Paris, 1829.

l'Amirauté a fait reconstruire un nouveau système aérien assurant les mêmes liaisons (Deal, Portsmouth, Plymouth) avec des tracés légèrement différents.

Certains historiens comme Jeffrey Kieve se sont étonnés du manque de perspicacité de l'Amirauté qui ne s'est pas emparée à cette époque des possibilités du télégraphe électrique. Je pense au contraire que cela témoigne d'une réelle demande pour un système de communication permanent. Le télégraphe aérien, déjà rodé, paraît plus sûr à l'Amirauté qu'un télégraphe électrique encore balbutiant.[13]

Ce n'est que dans les années 1830 que les autres États européens construiront des liaisons télégraphiques. En 1832, la Prusse construit une ligne Berlin-Coblence, la Suède installe un réseau autour de Stockolm. En 1839, la Russie établit une ligne entre Saint-Pétersbourg et Varsovie. En Espagne, un véritable réseau est installé : Madrid-Irùn en 1845 puis, à partir de Madrid, des liaisons avec Barcelone, Valence, Cadix. La durée de vie de ces réseaux sera courte. Le réseau anglais sera remplacé par le télégraphe électrique en 1847. Sur le continent, la transformation se fera plus tardivement dans les années 1850.

Ces télégraphes sont des télégraphes d'État gérés par les militaires (Angleterre, Prusse) ou par les ingénieurs des travaux publics (Espagne, Suède). Il s'agit d'instruments destinés à renforcer l'unité nationale, à consolider le pouvoir de l'État. Pour la Prusse, le télégraphe qui traverse les États indépendants du centre de l'Allemagne constitue au sens propre un lien entre les deux parties du pays (Rhénanie et Prusse-Orientale) séparées géographiquement. Pour la Russie, la ligne de Varsovie permet de consolider l'annexion de la Pologne. En Espagne, la construction du télégraphe se situe à l'époque où la monarchie doit combattre les républicains et les carlistes. En Suède, la fonction principale du réseau est d'assurer la communication entre le continent et les îles. Ces différents réseaux garderont toujours un caractère national, ainsi la ligne espagnole d'Irún se termine à quelques kilomètres de la ligne française (Béhobie) mais malgré cette proximité l'interconnexion ne sera jamais assurée.

L'exploitation du télégraphe optique aura duré environ un demi-siècle. Les potentialités techniques du système sont en germe depuis le XVII^{e} siècle, mais le télégraphe ne deviendra une réalité que parce qu'il s'inscrit dans un bouleversement majeur des mentalités : celui de la Révolution française préparé par les Lumières. Une utopie française apparaît à l'époque révolutionnaire celle de l'universalité : redécouper l'espace de façon homogène, le mesurer avec une nouvelle unité tirée de la nature, compter le temps d'une nouvelle façon, créer une langue universelle de façon à assurer une communication parfaite et à rendre la société transparente à elle-même.

L'universalité de 1789 va rapidement se réduire à la nation française. La Révolution crée l'État-nation moderne, nation où les citoyens ont les mêmes droits, État où les cellules territoriales sont équivalentes. Cet État-nation a besoin pour assurer sa cohérence et son unité d'un système de communication rapide. Derrière cette transformation des mentalités apparaît une demande de communication. Sous la Révolution et l'Empire, cette demande est essentiellement militaire. Sous la Restauration, elle vient également d'autres secteurs de l'appareil d'État et notamment de la police.

Cette association entre le télégraphe et la création des États-nations n'est pas uniquement française, elle est également présente dans les autres pays européens. Mais si le télégraphe optique est aussi largement associé à la France, au point que de nombreuses histoires des télécommunications ignorent les télégraphes aériens anglais, allemand, espagnol, c'est certes parce qu'il a été créé par un Français durant la Révolution mais aussi parce que l'idée de l'État-nation est largement issue du modèle révolutionnaire. En conquérant l'Europe, sous prétexte de l'éveiller à la liberté, les armées républicaines puis impériales susciteront le sentiment national en Prusse, en Espagne, en Russie.

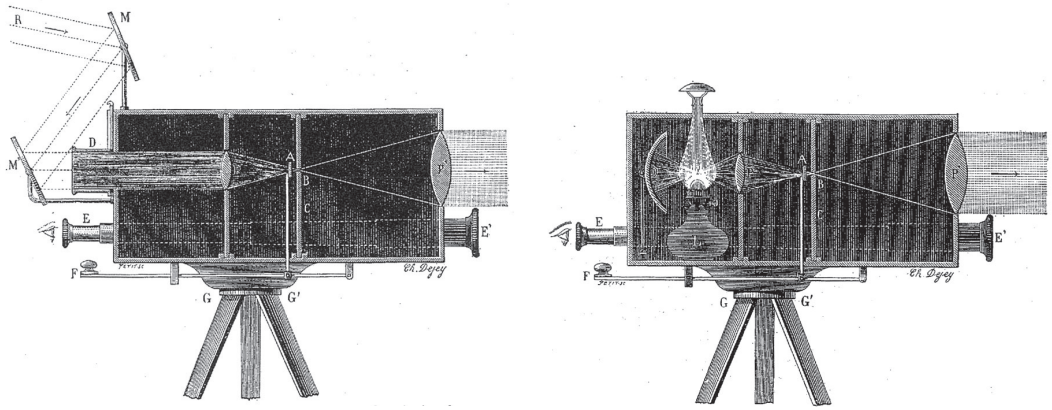
[13] Les difficultés de transmission créées par le brouillard, dans le télégraphe aérien, étaient moindres qu'on ne le croit souvent. D'après le *Times* du 4 avril 1830, le télégraphe aérien ne fut interrompu que vingt-neuf jours en 1829.

D'autres télégraphes optiques.

Un autre système de télégraphie optique avait déjà été expérimenté en l'année 1856 par un employé de la télégraphie française, un nommé Leseurre. Le télégraphe électrique était déjà développé à cette époque (Samuel Morse), mais le dispositif imaginé par Leseurre n'était pas original puisqu'il fut sans aucun doute la reprise d'une idée déjà exploitée dans l'Antiquité ! D'autres savants comme l'allemand Bergstrasser ou Steinheil, ainsi que Gauss avaient déjà imaginé l'utilisation de miroirs pour transmettre des messages.

Le système de Leseurre, qu'il avait appelé *héliographe*, avait surtout comme avantage principal d'être portatif puisqu'il ne pesait que 8 kg ce qui favoriserait son utilisation par l'armée. Pendant le siège de Paris (1870-1871) alors que la plupart des bureaux télégraphiques (électriques) étaient saccagés par les Prussiens et les communications interrompues, l'héliographe de Leseurre permit, pour ainsi dire, de passer par dessus la tête de l'ennemi !

Le colonel Mangin imagina un appareil qui a été expérimenté pendant plusieurs années à l'école militaire de Saumur. Son système utilisait le mode de codage de Samuel Morse sur lequel nous reviendrons. Son appareil qui s'apparentait à une lanterne magique (voir dessins) avait l'avantage de pouvoir fonctionner de jour comme de nuit et d'être facile à transporter.



A gauche : configuration de nuit, à droite configuration de jour.

La portée, de nuit était d'environ 25 Km, alors que de jour elle pouvait atteindre 120 Km !

En 1881 et 1885, Léon Adam, un habitant de l'île Maurice y exerçait les fonctions d'expert de l'amirauté anglaise. Il résolut de mettre en rapport télégraphique optique l'île Maurice, possession anglaise, avec notre île de la Réunion, les tentatives de jonction par un câble sous-marin ayant toutes échoué. En janvier 1883, il obtint l'autorisation d'établir à Maurice une station optique. Léon Adam créa le poste sur l'île de la Réunion, sur le pic du Bois-de-Nèfles, à 1130 mètres d'altitude, et dirigea les rayons solaires, réfléchis par un miroir d'un mètre carré, sur le sommet du Pouce (île Maurice), à 750 mètres au-dessus du niveau de la mer. La distance qui sépare ces deux positions est de 215 kilomètres. En 1885, la réussite fut complète. Du Pouce on voyait très bien les éclats du miroir : ils avaient l'aspect d'une étoile rouge-orange. Plus tard, M. Léon Adam trouve sur le Pic-Vert, à l'île Maurice, un poste plus favorable, qui rapprochait les distances de 25 kilomètres. Il dut enfin changer encore de poste pour opérer en un lieu moins élevé. Le Pic-Lacroix haut de 680 mètres fut définitivement choisi.

Quant aux communications de nuit, les appareils furent réglés et éclairés au pétrole. Dès la première nuit, on conversa entre les deux postes, avec la plus grande facilité, pendant plusieurs heures, et des dépêches furent échangées les jours et les nuits qui suivirent.

Il est intéressant de voir des travaux conçus tout d'abord pour la guerre s'approprier aussi bien aux intérêts de l'humanité.

L'impossible communication marchande

En 1836 une affaire de fraude télégraphique relance le débat sur l'usage de ce moyen de communication. Deux banquiers bordelais avaient soudoyé un employé du télégraphe pour qu'il ajoute des signaux supplémentaires à la suite de l'envoi des dépêches officielles. Ce système leur permettait d'être informés de l'évolution du cours de la rente d'État avant l'arrivée de la presse qui était expédiée par malle-poste. Le dispositif était assez rudimentaire et donnait à cette affaire un côté rocambolesque. Pour éviter les erreurs de transmission, inévitables dans le système Chappe, chaque dépêche était décodée au milieu du parcours par le directeur du bureau local de Tours. Le message était alors réémis vers Bordeaux. Les pirates injectaient des signaux supplémentaires indiquant l'évolution des cours de la Bourse, en aval de Tours. Pour informer leurs comparses qui effectuaient cette opération, les fraudeurs leur expédiaient par la malle-poste de Paris des gants blancs ou gris selon que le cours de la rente était en hausse ou non. La fraude dura deux ans. Quand elle fut découverte, les protagonistes furent traduits devant les assises... mais relâchés. Le monopole télégraphique de l'État n'étant pas défini par la loi, on ne pouvait pas les condamner.

Du monopole de fait au monopole de droit

Les deux banquiers bordelais n'étaient pas les premiers à découvrir la valeur de l'information dans l'établissement des cours de la Bourse. Déjà, sous la Restauration, les Rothschild avaient mis en place un système de courrier privé qui leur permettait de connaître, avant les autres, les principaux événements politiques et les cours des autres places. Ainsi, « *l'assassinat du duc de Berry, en février 1829, fut connu à Francfort par la maison Rothschild bien avant tout le monde. Elle prit alors ses dispositions et n'annonça la nouvelle qu'après avoir fait partir ses courriers et ses ordres* »[14]. À propos de l'intervention de la France en Espagne, le président du Conseil Villèle note dans ses mémoires : « *Le courrier des Rothschild fait de nouveau monter nos fonds d'État. Il répand le bruit qu'il n'y aura pas d'intervention. Les hausses trompeuses qui préparent de nouvelles fluctuations des cours et de fortes pertes ne me disent rien qui vaille.* »

Les banquiers qui n'ont pas les moyens de mettre en place des courriers privés à travers l'Europe pensent à utiliser le télégraphe. D'autres opérations clandestines ont lieu entre Paris et Lyon. Au début de l'année 1832, Alexandre Ferrier lance une souscription pour constituer le capital d'une société privée de télégraphe qui doit pouvoir rejoindre les principales villes européennes.[15] Il envisage un usage essentiellement commercial. Son télégraphe offre « *l'avantage immense de faire embrasser d'un coup d'œil l'état de toutes les places, d'assister à la fois à toutes les bourses et de donner à leurs opérations plus d'aliments en même temps que de sécurité* ». La demande d'informations boursières en province a fortement augmenté dans les années 1820. En effet, d'après Bertrand Gille, c'est à cette époque qu'on commence à souscrire largement à la rente d'État en province.

Ferrier a obtenu l'appui de Casimir-Perier (président du Conseil et ministre de l'Intérieur). Celui-ci lui fait écrire : « *J'ai vu dans cette question d'utilité publique, un progrès de civilisation qui promet à l'industrie des avantages réels, et je suis heureux de pouvoir l'encourager de mon approbation.* » Ferrier peut également se recommander d'une quarantaine de députés : des libéraux du parti du mouvement (monarchiste constitutionnel de gauche) Laffitte, La Fayette, Odilon Barrot, des banquiers comme Benjamin Delessert, des juristes... Il assure également ses futurs souscripteurs de « *l'approbation des négociants consultés sur l'utilité du projet* ». Il s'est enfin entouré des conseils de plusieurs avocats qui concluent que, faute

[14] Bertrand Gille, *La Banque et le crédit en France de 1815 à 1848*, Presses universitaire de France, Paris, 1959, p. 262.

[15] O'Etzel, directeur du télégraphe optique allemand, rencontra, lors d'une visite à Paris, Ferrier qui lui présenta son projet de réseau européen. Cité par Dieter Herbarth, *Die Entwicklung der optischem Telegrafie in Preussem*, Rheinland Verlag, Cologne, 1978, p. 21.

de loi sur le télégraphe, « *l'administration impuissante devra respecter le droit de la propriété et la liberté de l'industrie.* »

Fort de tous ces appuis, Ferrier construit une ligne Paris-Rouen et prépare l'installation d'un réseau national. Il est persuadé d'obtenir l'appui de l'Administration, il écrit à plusieurs préfets en leur demandant de lui désigner « *des personnes de confiance pour leur donner des places de directeurs dans les lignes qu'il va créer* ». Des négociations sont d'ailleurs ouvertes avec le ministère de l'Intérieur pour étudier une collaboration. Puis en juin 1833, l'Administration rompt les négociations et décide de faire voter une loi sur le monopole télégraphique.[16]

Ce revirement du pouvoir politique est intéressant à observer. Dans un premier temps, la position de la bourgeoisie d'affaires libérale (Casimir-Perier, Laffitte) l'emporte, puis finalement une position d'affirmation du monopole étatique est adoptée, dans la loi qui sera votée par le Parlement en 1837. Les opposants au projet de loi à la Chambre des députés, comme à la Chambre des pairs, seront d'ailleurs moins nombreux que les pétitionnaires de 1832.

Les défenseurs de l'usage privé du télégraphe présentent deux options : soit la création de lignes privées, soit l'ouverture des lignes d'État au public. Vatimesnil, à l'aide d'une comparaison poste/télégraphe, résume bien ces deux options : « *Le monopole de la poste aux lettres se justifie 1° parce qu'il est une des sources du revenu public ; 2° parce qu'il ne nuit pas aux particuliers, puisque l'Administration se charge de faire transporter leurs dépêches. Au contraire, le monopole des télécommunications télégraphiques ne rapporterait rien à l'État et il préjudicierait aux citoyens en les empêchant de se servir de ce mode de correspondance si rapide, et par conséquent, si propre à imprimer une nouvelle activité aux relations commerciales. Pour qu'il en fût autrement, il faudrait que le gouvernement établît des télégraphes sur toutes les lignes de communication importantes et les mît au service des particuliers, moyennant une rétribution fixée par la loi.* »

Les deux options envisagées renvoient aux deux formes du libéralisme, politique ou économique. Si on retient une argumentation politique, le monopole d'usage de l'État n'est envisageable que sous un gouvernement despotique, la conquête des libertés assurée par la révolution de juillet 1830 implique la possibilité pour le citoyen de communiquer par tous les moyens possibles. Si on se place d'un point de vue économique, l'État ne peut confisquer pour son propre usage des techniques nécessaires à l'activité économique.

Pour étayer leur thèse, les libéraux font référence à la presse qui n'est pas un monopole gouvernemental, affirmant : « *Une loi sur les télégraphes, comme une loi sur la presse, doit se borner à en régler l'usage et à en réprimer l'abus* ». Toutefois, lors du débat de la loi de 1837, l'opposition mènera moins une bataille contre le monopole d'État que pour l'usage privé. Elle reprendra ainsi les suggestions du comte de Montureux qui avait publié, en avril 1830, dans un journal de Montpellier, des « *réflexions sur la possibilité de faire du télégraphe une branche de revenus pour le gouvernement et de faciliter les opérations commerciales en mettant ce moyen de correspondance à la disposition des négociants* ».

La thèse libérale, qui semblait forte en 1831, est donc très minoritaire lors du vote de la loi de 1837 qui prévoit une peine de prison pour « *quiconque transmettra, sans autorisation, des signaux d'un lieu à un autre* ». Les débats autour de cette loi sont très importants pour comprendre comment la société française des années 1830 se représente la communication. Deux projets communicationnels s'opposent, celui d'une communication libre nécessaire au développement de l'économie de marché, celui de la communication de l'État où « *le télégraphe est l'indispensable complément de notre centralisation gouvernementale* ». Cette vision de la communication a souvent été présentée comme foncièrement rétrograde, comme le dernier sursaut avant la libéralisation qui adviendra dans les années cinquante. Une telle analyse se contente alors de ramasser quelques discours favorables à sa thèse. Elle se condamne par là même

[16] Circulaire du ministre de l'Intérieur aux préfets, 29 juin 1833, *Archives nationales,* F 90-1456.

à ne pas comprendre les conceptions de la monarchie de Juillet. Le débat doit au contraire être étudié dans toute sa richesse.

Les justifications de la loi présentées par le ministre de l'Intérieur Adrien de Gasparin et les deux rapporteurs de la Chambre des députés et de la Chambre des pairs, Joseph-Marie Portalis et le duc de Plaisance, reposent sur les représentations qu'ils se font des usages non étatiques de la communication. Ils en voient essentiellement deux : l'agitation politique et la spéculation boursière. La crainte de l'insurrection n'est pas seulement un phantasme de ministre de l'Intérieur, la monarchie de Juillet a été confrontée jusqu'en 1835 à une série de mouvements sociaux d'une très grande ampleur tant à Paris qu'en province, notamment à Lyon. Le pouvoir peut donc légitimement craindre que le télégraphe ne devienne un instrument entre les mains des comploteurs. Quant à l'utilisation boursière, elle est perçue par de nombreux députés comme un moyen d'agiotage, de « *spéculation immorale, spoliatrice* ». Le député Fulchiron peut ainsi déclarer : « *Jusqu'à présent, je n'ai pas vu établir par des particuliers des lignes télégraphiques dans de bonnes intentions* » ; elles servent à « *établir un brigandage, afin de voler ceux qui ne savent pas les nouvelles de la Bourse de Paris* ». Ce mépris pour l'activité financière et plus largement pour l'économie était assez largement partagé par la classe politique sous la monarchie de Juillet.

Peur de l'insurrection, désintérêt pour l'économie, le refus de libéraliser la communication télégraphique paraît aisément compréhensible. Mais les défenseurs du projet de loi ne peuvent pas en rester là, ils sont face à une véritable opposition.

Un nombre important de députés a soutenu le projet de Ferrier, leur refus doit être plus argumenté. Ils vont donc s'employer à démontrer que le télégraphe n'est pas assimilable à la Poste. L'argument est le suivant : le courrier peut transporter un nombre considérable de dépêches qui arrivent toutes en même temps. Il est donc difficile de manipuler l'information. Une lettre peut être contredite par une autre qui arrive au même moment. « *Mais le télégraphe ne se prête pas à cette liberté, à cette égalité, à cette simultanéité d'action. Il repousse cette concurrence par lui-même et, nécessairement, le télégraphe est un monopole* » Sur une liaison, il est difficile d'organiser plusieurs lignes concurrentes. Les difficultés économiques de la ligne Paris-Rouen construite par Ferrier confirme la thèse de Gasparin : si une seule ligne privée paraît peu rentable, c'est encore plus vrai pour une seconde ligne.

L'aspect monopolistique du télégraphe vient surtout des conditions de transmission. Le trafic potentiel d'une ligne n'est pas considérable et surtout, rien ne garantit qu'une dépêche partie une demi-heure ou une heure après une autre arrive le même jour.[17] « *Le premier ne jouira-t-il pas d'un privilège immense, exorbitant, inadmissible ?* » Toutes ces tendances monopolistiques font que « *les lignes tomberaient infailliblement dans les mains des partis… ou dans celles des plus riches spéculateurs qui enlèveraient ainsi toute chance de succès aux commerçants moins opulents et obtiendraient par le fait un privilège exclusif au préjudice des négociants les plus pauvres* ». Le dispositif de courrier privé des Rothschild montre que cette dernière hypothèse est tout à fait vraisemblable.

Pour empêcher « *un monopole au service de l'intérêt privé, de l'intérêt commercial, jaloux, exclusif, exigeant, profitant d'un immense avantage pour écraser des rivaux, pour spéculer à coup sûr* », Gasparin peut affirmer, « *sans paradoxe, que le seul moyen d'empêcher le monopole du télégraphe, c'est de l'attribuer au gouvernement* ».

En définitive, on retrouve la conception étatique et centralisée du télégraphe qui a pris forme sous l'Empire et la Restauration, mais la conception du monopole est différente. Ce n'est plus un instrument

[17] Les conditions météorologiques peuvent retarder une dépêche. Une statistique réalisée en 1842 et 1843 donne la vitesse de transmission suivante : 50 kilomètres par minute. Toutefois, seules 64 % des dépêches arrivent le jour même, ce pourcentage n'est que de 33 % en hiver (source : statistique du ministère de l'Intérieur). Lardner raconte également que pendant les guerres napoléoniennes un message fut expédié de Plymouth à Londres. Seule la première partie arriva : « *Wellington defeated…* ». Le restant du message bloqué par un épais brouillard ne fut expédié que le lendemain. Il modifiait fonda mentalement le sens : « *…the French at Salamanca.* » (Dr Lardner, *The Elec tric Telegraph*, James Walton, Londres, 1867, p. 40.)

policier et militaire qui trouve en lui-même sa propre légitimité, mais un instrument de l'intérêt général. Le duc de Plaisance envisage que l'État se charge de diffuser les informations boursières et en garantisse ainsi l'objectivité. Au détour de la démonstration, apparaissent en creux les conditions de fonctionnement d'un service de correspondance télégraphique : obligation d'admettre toutes les dépêches sans distinction d'origine, en suivant l'ordre d'inscription, tarif modéré. C'est parce que Gasparin estime que le télégraphe optique ne peut remplir ce cahier des charges qu'il refuse l'ouverture à l'usage privé. Son argumentation est de nature sociotechnique. Certes, la monarchie de Juillet n'est pas encline à libéraliser le télégraphe, mais les contraintes de la technique optique la renforcent dans sa position.

Cette loi clôt un cycle sociotechnique, celui qui associait télégraphe Chappe et télégraphe d'État. Cette association a failli être mise à mal, elle a résisté une dernière fois, mais elle va petit à petit se disloquer au cours des dix années suivantes, pour donner naissance à un nouvel ensemble sociotechnique : communication commerciale/télégraphe électrique.

Le télégraphe libéral

La situation anglaise est toute différente. Dans la conception libérale britannique, la régulation de la société est assurée très largement par le marché. Les infrastructures de communication y relèvent de l'initiative privée. Dans la seconde moitié du XVIII[e] siècle, on assiste à une multiplication de canaux et de routes à péages (*turnpikes*) construits selon ce principe.

L'initiative privée se manifeste également dans le domaine de la télégraphie. Un acte royal de 1825 consacré à l'amélioration du port de Liverpool autorise les administrateurs des Docks « *à établir un moyen de communication rapide entre Liverpool et le pays de Galles, pour avertir les armateurs et les commerçants de l'arrivée des bateaux* ». Deux ans plus tard, une ligne télégraphique sera ouverte, et exploitée par Watson. *La Shipping and Mercantile Gazette* du 4 janvier 1842 fera le bilan de cette liaison télégraphique, elle insistera sur son efficacité et « *la grande importance commerciale de ce mode de communication* ». De 1839 à 1842, Watson ouvrira quatre autres lignes à Hull, Londres, Southampton et Dartmouth.

Bien que possédant ses propres lignes (voir *supra*), l'Amirauté utilise également le télégraphe de Watson. Celui-ci a aussi reçu l'appui de la Compagnie des Indes et de la Lloyd's. Si l'on croit le témoignage d'un contemporain, J. Humphery, cette liaison télégraphique offre un grand intérêt pour les armateurs puisque certains bateaux peuvent rester plusieurs semaines bloqués par des vents contraires, se trouvant ainsi dans l'incapacité de remonter la Tamise. Les incertitudes du transport maritime ont des conséquences sur la disponibilité des marchandises et l'évolution des cours. David Landes rappelle « *que les négociants et banquiers du Londres et du Paris du XIX[e] siècle attendaient avidement que l'on signalât, au large de la pointe de Cornouaille ou d'Ouessant des voiles annonçant de précieuses cargaisons en provenance du Pacifique. Les sommes qui s'y trouvaient en jeu étaient une faible fraction des créances à recouvrer sur les marchés de l'argent et des valeurs ; mais à la fin du mois, c'étaient elles qui faisaient toute la différence entre une liquidation facile et une liquidation difficile* ».

Watson envisage également d'autres usages pour son télégraphe : l'information de gestion des chemins de fer (il élabore notamment un plan pour un télégraphe le long de la voie Liverpool-Manchester en 1836), l'information boursière entre Londres et Paris.

L'utilisation marchande du télégraphe existe donc dans les années 1830 en Angleterre comme en France. Elle a donné lieu à l'installation de réseaux distincts des réseaux d'État.[18] En France, l'État bloquera le développement des réseaux privés, en Angleterre il les laissera se créer. Le libéralisme marchand va constituer un cadre favorable au développement du télégraphe. L'innovation, sous la forme de l'électricité, trouvera là un terrain d'épanouissement.

[18] Il en fut de même en Allemagne, où des réseaux privés furent construits à Hambourg et à Brême.

Conclusions sur le système de télégraphe Chappe

Le télégraphe optique constitua le point de démarrage des systèmes de télécommunications. Même s'il constitue à nos yeux un système techniquement dépassé, il regroupe les quatre caractéristiques de base des télécommunications que d'autres systèmes réorganiseront :

— À défaut d'être instantanée, la transmission est très rapide. Chappe améliore la rapidité en perfectionnant le système de codage ;

— Un réseau permanent est constitué qui s'étend de plus en plus dans l'espace ;

— Un corps technique spécialisé prend en charge l'exploitation ;

— L'information est codée dans un langage « universel ».

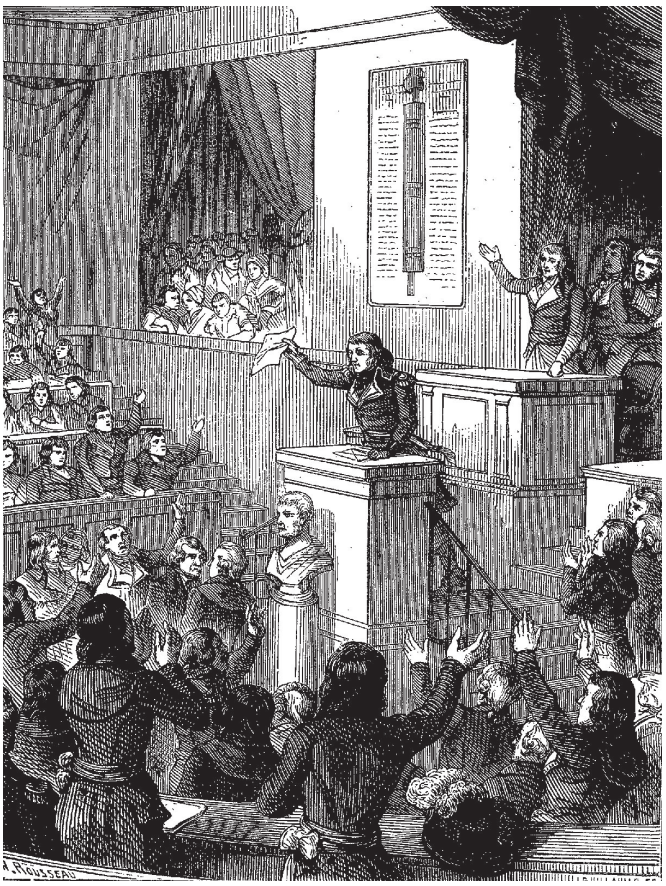
Chappe a intégré les contraintes d'exploitation dans le système de communication : il a défini des signaux d'exploitation (début, fin, interruption, numéro de station…) qui sont autonomes par rapport aux signaux de correspondance.

Le terrain est prêt pour l'avènement du télégraphe électrique.

Avec la découverte de l'électricité, la transmission des messages optiques pourra s'affranchir du problème de la transmission nocturne ou par manque de soleil pour les appareils de type Mangin. Cependant, les mauvaises conditions météorologiques perturberont les transmissions de la même façon qu'avec le télégraphe Chappe. Aussi, la transmission filaire apparaîtra rapidement comme la meilleure solution à une disponibilité permanente d'un moyen de transmission sûr et rapide.

De nouveaux systèmes de codage, plus universels, le Morse en particulier, seront utilisés. Le *chiffrage* des messages permettant de sauvegarder le secret des transmissions.

Nous allons donc aborder maintenant les systèmes visuels de télécommunication électrique.



Carnot annonce à la Convention la nouvelle expédiée, par le télégraphe, de la prise de Condé sur les Autrichiens.

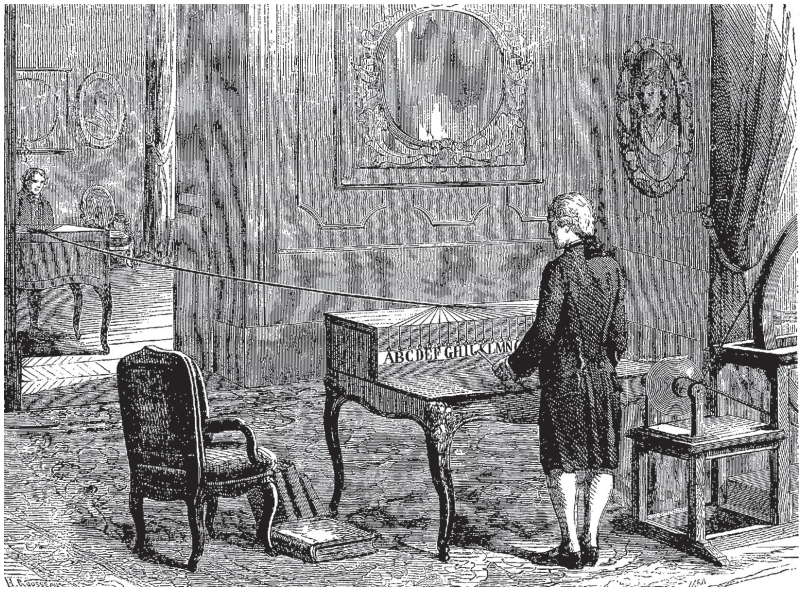
L'électricité dans les transmissions.

En ce XVIII[e] siècle, les phénomènes électriques n'étaient que de simples curiosités de salon. Cependant, très vite, des inventeurs imaginèrent d'utiliser l'électricité comme moyen de transmission de messages.

C'est en 1746 que l'on découvre que l'électricité se propage dans les corps « conducteurs », mais en attendant la pile de Volta, on devait se contenter de l'électricité statique obtenue par frottement de divers corps. L'arrivée de la bouteille de Lyede, ancêtre du condensateur électrique, construite par Pieter von Masschenbroek, permit, entre autres, d'augmenter la « puissance » des décharges électriques. C'est donc à partir de cette invention que des chercheurs ont proposé divers procédés de transmission.

La première mention qui est faite d'un appareil de ce genre pour appliquer l'électricité à la transmission de la pensée, fut publié par un recueil écossais, le *Scot's Magazine*, dans une lettre signée d'une simple initiale, et écrite de Renfrew, le 1[er] février 1753. L'appareil faisait se déplacer des balles devant chaque lettre de l'alphabet, l'émetteur et le récepteur étant reliés par autant de fils que de lettres.

L'appareil proposé par le savant écossais, dont on suppose qu'il s'agissait de Charles Marshall, passait pour savoir *forcer la foudre à parler et à écrire sur les murs*… La lettre du savant anonyme n'attira aucune attention, car l'appareil qu'il proposait ne fut jamais mis à exécution.



L'honneur d'avoir le premier réalisé, dans des conditions pratiques, un appareil de télégraphie fondé sur l'emploi de l'électricité statique, appartient à un savant genevois d'origine française, nommé Georges-Louis Lesage. C'est vers 1760 qu'il conçut son télégraphe électrique, et c'est en 1774 qu'il en fit la démonstration à Genève.

L'instrument qu'il imagina, et que ne fut d'ailleurs qu'un appareil de démonstration, se composait de 24 fils métalliques séparés les uns des autres et noyés dans une substance non conductrice. Chaque fil allait aboutir à un électromètre particulier formé d'une petite balle de sureau suspendue à un fil de soie. En mettant une machine électrique ou un bâton de verre électrisé, en contact avec l'un des fils, la balle de l'électromètre qui y correspondait était repoussée, et ce mouvement indiquait la lettre de l'alphabet que l'on voulait faire passer d'une station à l'autre. C'était, en fait très peu différent de l'invention du savant écossais dont nous parlions plus haut !

L'idée de la télégraphie électrique fit son chemin, et quelques années plus tard, on la trouve réalisée à la fois en France, en Allemagne et en Espagne. En 1787, un physicien du nom de Lomond, avait construit, à Paris, une petite machine à signaux fondée sur les attractions et répulsions corps électrisés[19].

[19] Cité dans « *Voyages en France pendant les années 1787, 1788 et 1789* », par Arthur Young. On trouve un passage amusant dans ce récit : « *Madame Lavoisier, personne pleine d'animation, de sens et de savoir, nous avait préparé un déjeuner anglais au thé et au café, mais la meilleure partie de son repas c'était la conversation. Le soir, visite de M. Lomond, jeune mécanicien très ingénieux et très fécond, qui a apporté une modification au métier à filer le coton. Il a fait aussi une découverte remarquable sur l'électricité. On écrit deux ou trois mots sur un morceau de papier, il l'emporte dans une chambre et tourne une machine renfermée dans une caisse cylindrique, sur laquelle est un électromètre, petite balle de moelle de sureau ; un fil de métal la relie à une caisse également munie d'un électromètre placé dans une pièce éloignée. Sa femme, en notant les mouvements de la balle de sureau, écrit les mots qu'ils*

En Allemagne, Reiser proposa, en 1794, d'éclairer à distance, au moyen d'une décharge électrique, les diverses lettres de l'alphabet que l'on aurait découpées à l'avance sur des carreaux de verre recouverts de bandes d'étain. L'étincelle électrique devait se transmettre par vingt-quatre fils correspondant aux lettres de l'alphabet, ces fils étant isolés sur tout leur parcours dans des tubes de verre.

En Espagne, l'ingénieur Bettancourt[20], dont nous avons parlé à propos du télégraphe optique, avait essayé, en 1787, d'appliquer à l'électricité la production de signaux en faisant passer des décharges dans des fils de Madrid à Aranjuez (58 Km). En 1796, François Salva, médecin catalan établit à Madrid un véritable télégraphe électrique.

On peut citer également Tiberius Cavallo (1749-1809), physicien italien, qui fit des expériences en Angleterre en 1795.

L'invention de la pile faite en 1800 par Volta devait donner nécessairement une vive impulsion (c'est le mot qui convient…) aux recherches concernant la télégraphie électrique.

Le premier télégraphe, *télégraphe à cadran*, fut inventé par un ouvrier doreur nommé Jean Alexandre, que l'on disait fils naturel de Jean-Jacques Rousseau. C'est à Poitiers, où il avait pris sa retraite de commissaire des guerres qu'il fabriqua un appareil qui avait nommé *télégraphe intime*, et qui était en fait un télégraphe à cadran. Malgré de nombreuses démonstrations réussies devant diverses autorités, dont le préfet de la Vienne, il ne parvint pas à présenter son invention au premier Consul. Même le rapport détaillé et très favorable du citoyen Delambre, le 10 fructidor an X, qui demandait seulement 10 minutes d'audience au premier Consul pour lui présenter son invention, resta sans effet. Même le ministre Chaptal, qui devait accorder, au sein du gouvernement, une protection paternelle aux sciences et à leurs progrès, repoussa froidement l'invention d'Alexandre en déclarant que le télégraphe aérien lui était supérieur…

En 1811, le physicien allemand Sœmmering fit connaître à l'Académie de Munich un appareil qui transmettait les signaux par décomposition électrochimique de l'eau. L'appareil était composé de 35 circuits, 25 pour les lettres et 10 pour les chiffres. Le projet de Sœmmering, dans la pratique offrait de nombreuses difficultés, mais, lui aussi avait entrevu les possibilités de la télégraphie électrique : fonctionnement aussi bien de nuit que de jour, les brouillards ne peuvent retarder son action et, supériorité immense, il permet d'exprimer des signaux à une vitesse incalculable et sans construction d'édifices particuliers.

Un dispositif analogue a été expérimenté par John Coxe à Philadelphie.

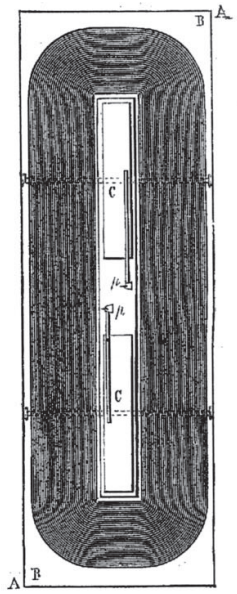
Le vrai tournant arriva avec la découverte de l'électromagnétisme par le physicien danois Œrsted en 1820, puis de l'invention du galvanomètre par le physicien Schweigger. Ampère s'intéresse aux travaux d'Œrsted et dans un mémoire à l'Académie des sciences, il suggère que l'action du courant sur les aiguilles aimantées peut constituer un dispositif télégraphique.

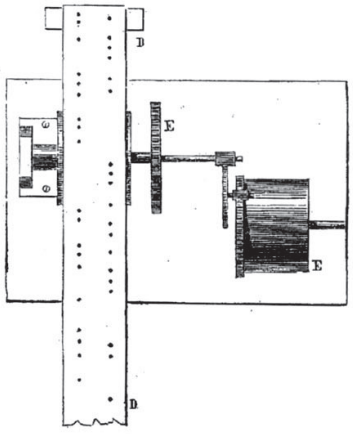
Plusieurs appareils utilisant cette technique furent développés et testés par des savants comme le baron Schilling de Saint-Pétersbourg, Alexander et Ritchie, d'Édimbourg, Gauss et Webert de Gœttingue. En Angleterre M. Wheatstone réalisa en 1837 un télégraphe électrique conçu sur ce même principe, mais c'est un physicien de Munich, M. Steinheil, qui construisit la première application pratique de l'électricité comme agent télégraphique. Son appareil n'était pas un simple appareil de cabinet, mais un instrument avec lequel il établit une correspondance entre son observatoire et un faubourg de Munich séparés de plus d'une lieue.

---

indiquent. D'où l'on peut conclure qu'il a formé un alphabet au moyen de mouvements. Comme la longueur du fil n'a pas d'influence sur le phénomène, on peut correspondre ainsi à quelque distance que ce soit, par exemple du dedans au dehors d'une ville assiégée, ou, pour un motif bien plus digne et mille fois plus innocent, l'entretien de deux amants, privés d'en avoir d'autre ». Ce dernier commentaire est amusant, car on retrouvera le même au sujet du téléphone quelques années plus tard !

[20] Son nom est également orthographié Béthencourt.





Bien que tombé dans les oubliettes de l'histoire, Steinhel réalisa l'appareil que nous allons décrire en juillet 1837.

Cet instrument peut être considéré comme le premier qui ait servi à établir une correspondance régulière au moyen de l'électricité voltaïque.

C'était un simple galvanomètre AA, dont les fils multiplicateurs B, B, entouraient des barreaux aimantés C, C. Ces barreaux se terminaient par un petit stylet, pourvu d'un bec rempli d'encre, *p*, *p*.

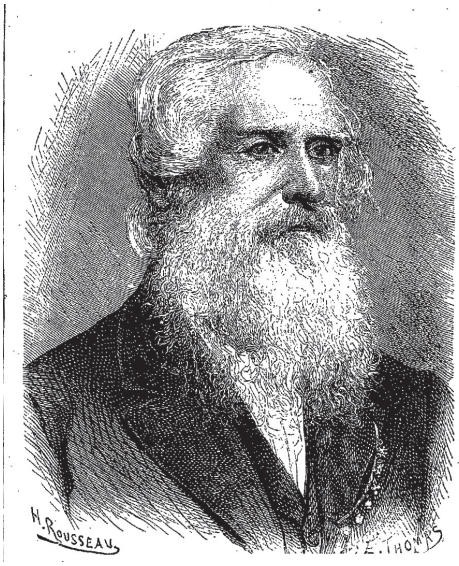
Une bande continue de papier DD se déroulait au-devant de ces deux becs, marchant d'un mouvement uniforme, grâce à un rouage d'horlogerie E, E.

Quand le courant électrique était dirigé dans les fils du galvanomètre, les deux barreaux aimantés se déviant du même côté sous l'influence de l'électricité, l'un des deux becs chargés d'encre s'approchait de la feuille de papier et y déposait un point noir. Quand on changeait la direction, c'était l'autre bec qui venait toucher la feuille de papier et y marquer un point noir ; en combinant ces points de différentes manières, M. Steinheil avait composé un alphabet conventionnel.

Le télégraphe magnétique de M. Steinheil contenait une innovation importante qui permettait d'entrevoir la solution prochaine du problème de la télégraphie électrique : il n'employait qu'un seul courant et qu'un seul fil, ce qui rendait la télégraphie immédiatement pratique. Le physicien de Munich découvrit, en effet, en 1838, la possibilité de supprimer le *fil de retour* du circuit en prenant la terre elle-même comme conducteur de ce retour. Cette découverte était d'importance, car elle diminuait de moitié la longueur du conducteur métallique nécessaire à l'établissement d'un circuit.

Cependant, le problème de la télégraphie électrique n'était pas encore entièrement résolu et ce sont les travaux d'Arago sur l'aimantation temporaire du fer par le courant électrique qui vont permettre la création des électro-aimants et ouvrir la voie au télégraphe électromagnétique.

Le télégraphe Morse

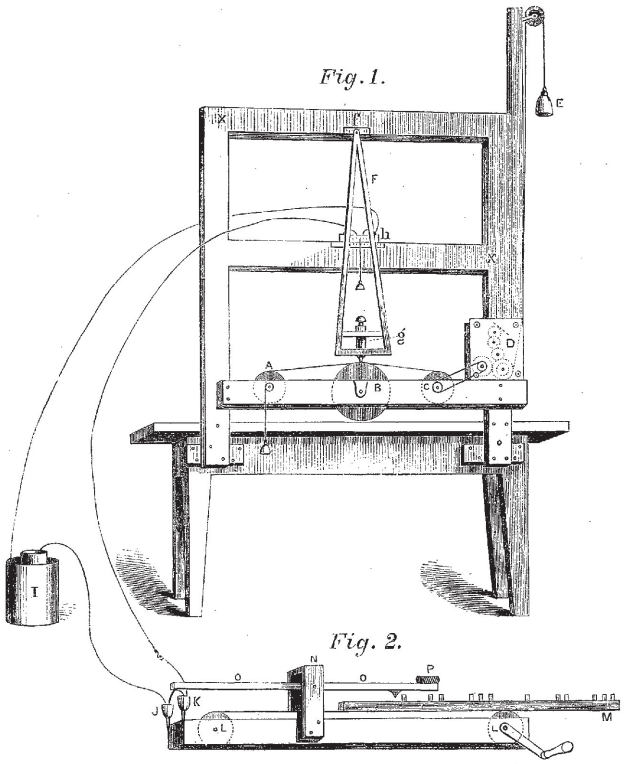


Comme beaucoup d'autres grands inventeurs, Samuel Finley-Breese Morse n'était ni physicien, ni mécanicien : il était artiste-peintre et professeur de peinture. C'est par hasard, pour ainsi dire, qu'il fut amené à s'occuper pour la première fois de télégraphe électrique.

Pendant qu'il étudiait au collège de Yale, Samuel Morse s'était un peu occupé de chimie et de physique, mais de manière tout à fait accessoire. C'est quand il devint professeur à l'*Athénée* de New York qu'il devint ami intime du professeur Freeman Dana qui faisait alors un cours sur l'électromagnétisme. Cette partie de la physique devint un sujet de conversation très fréquente entre les deux amis, et Samuel Morse entra en possession d'un des premiers électro-aimants fabriqués en Amérique qui lui fut offert par le professeur Torrey.

L'idée d'utiliser l'électricité comme vecteur lui vint lors d'un voyage en retour d'Europe à bord du paquebot *le Sully*. L'expérience de Franklin, qui avait vu l'électricité parcourir la distance de deux lieues en un temps non mesurable, le poussa à imaginer une machine capable de transmettre un signal à distance et rapidement.

Nous allons nous arrêter un instant, en le décrivant, sur le tout premier appareil Morse, assez peu connu, mais qui porte en lui le germe des futurs appareils qui furent utilisés par des générations de manipulateurs.



Le premier télégraphe électrique de Samuel Morse

Samuel Morse fabriqua, en 1832, le premier modèle de cet instrument. Comme il était revenu fort pauvre de ses voyages en Europe, il dut se contenter, pour fabriquer ce premier modèle, d'un cadre de tableau pris dans son atelier, de rouages en bois d'une horloge du prix de 5 francs, et de l'électroaimant qu'il tenait de l'obligeance du professeur Torrey. Il cloua contre une table ainsi que le représente la figure suivante l'appareil dont nous allons décrire les rudiments.

XX représente le cadre cloué verticalement contre la table. Les rouages de bois D, mus par le poids E, comme les horloges de Nuremberg, font dérouler, par un mouvement uniforme, une bande de papier continue, sur les trois rouleaux A, B, C, suivant la belle invention du *papier tournant*, due à Steinheil de Munich, comme nous l'avons raconté. Une sorte de pendule F, pouvant osciller autour du point *f*, se terminait par un crayon *g*, qui pouvait laisser sa trace sur le papier passant au-dessus du rouleau B. Le déplacement de ce pendule F pouvait être provoqué par l'électroaimant *h*, lorsque l'électricité partant de la pile I, et suivant le fil conducteur, venait animer cet électroaimant. Selon la durée du contact du crayon et du papier déroulant, on produisait des signes en zigzag.

D'après le nombre de ces traits en zigzag, M. Morse avait combiné un alphabet en chiffres, qui suffisait à toutes les nécessités de la correspondance.

Mais comment pouvait-on produire ces contacts plus ou moins longs du crayon sur le papier ; comment était construit, ce que l'on nomme aujourd'hui le manipulateur, et qui sert à produire à distance les établissements et les interruptions du courant pendant le temps convenable ? Ici était la partie faible de l'appareil, l'organe peu commode dans la pratique et qui fut remplacé bientôt par le *levier-clef*, dont nous aurons à parler plus loin.

Dans l'appareil qui fonctionna de 1832 à 1835, M. Morse employait un *interrupteur de courant*, ou *manipulateur*, qui agissait d'une manière mécanique, et voici comment. Il avait taillé des caractères ressemblant à des dents de scie, il les rangeait en longues files, et les faisait passer d'une manière réglée et uniforme, à l'aide d'un rouage d'horlogerie, sous un levier, pour ouvrir ou fermer le circuit voltaïque (voir la *fig. ci-dessus*). Ces dents étaient fixées sur une règle de bois M, que faisait avancer horizontalement, un rouage d'horlogerie, ou simplement la main tournant régulièrement la manivelle L. Lorsque les dents en saillie des caractères placés sur la barre M, venaient rencontrer un arrêt placé à la partie inférieure du levier OOP, ils soulevaient ce levier et le faisaient basculer sur son point d'appui N, en abaissant son

autre extrémité, à laquelle était attaché l'un des fils de la pile I. Grâce à ce mouvement, l'extrémité du fil conducteur plongeait dans deux petites coupes K, J, pleines de mercure, formait ainsi la communication entre ces deux godets, et, par cette continuité métallique, établissait, le courant électrique, tout à l'heure interrompu. Lorsque la dent avait passé, le levier se relevait, grâce au poids P, et ainsi de suite.

Les saillies des caractères, en passant sous ce levier, produisaient donc des établissements et des interruptions de courant correspondant à ces mêmes saillies.

La figure 43 donne un spécimen de ces types caractères, dont chacun répond à un chiffre depuis 1 jusqu'à 10.

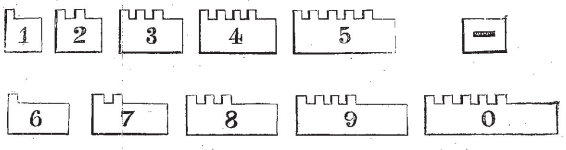


Fig. 43.

La figure 44 donne un exemple des signaux que le crayon formait par le mécanisme qui vient d'être décrit.

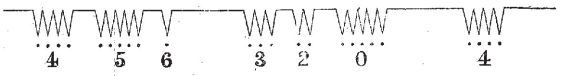
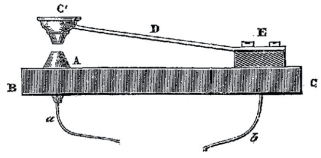


Fig. 44.

Comme nous l'avons déjà dit, le défaut de cet appareil résidait dans le *manipulateur*. Samuel Morse le remplaça bientôt par un appareil beaucoup plus simple, et dans lequel le doigt, appuyant sur un levier, et maintenant ou suspendant le contact pendant un temps calculé, produisait sur le *récepteur* les signaux de l'alphabet conventionnel.



Manipulateur du télégraphe Morse.

C'est en 1835 que fut exécuté l'appareil que nous venons de décrire. Il fut soumis par l'inventeur, à plusieurs expériences publiques, de 1835 à 1836.

En 1837, Samuel Morse, après avoir imaginé son second manipulateur, et modifié le récepteur de manière à présenter la forme que nous décrirons bientôt, en fit la démonstration devant les membres de l'Université de New York. Ces expériences firent grand bruit aux États-Unis : et c'est pour cela que l'on a fixé, par erreur, à l'année 1837, l'invention de cet appareil, qui, en réalité, fut soumis pour la première fois à des expériences publiques, dans l'automne 1835.

Confiant dans la valeur de son invention, M. Morse avait demandé au Congrès des États-Unis l'examen de son système de télégraphie électrique. Au commencement de l'année 1838, il était à Washington, sollicitant du Congrès des fonds nécessaires pour établir de Washington à Baltimore d'une ligne de télégraphie électrique qui aurait démontré la possibilité pratique et les avantages de son invention.

Des expériences eurent lieu à l'invitation du Congrès des États, le 2 septembre 1837, sur une distance de quatre lieues, en présence d'une commission de l'institut de Philadelphie, et d'un comité pris dans le sein du Congrès.

Le résultat de ces expériences excita dans le comité nommé par le Congrès, un intérêt très vif ; mais le scepticisme de quelques membres de ce comité, bien que les conclusions de son rapport fussent favorables, se communiqua à la majorité du Congrès, qui laissa l'affaire sans conclusion. La session législative de 1838 se termina donc sans annoncer aucun résultat pour l'inventeur.

Samuel Morse, en 1839, s'embarqua pour l'ancien continent, espérant attirer l'attention des gouvernements européens sur les avantages de son invention. Il s'adressa à l'Angleterre et à la France. Mais en Angleterre, M. Wheatstone venait d'occuper le monde savant d'appareils de télégraphie électrique, fondés sur d'autres principes, et l'on refusa de délivrer à l'inventeur américain la patente, ou brevet exclusif d'exploitation, qu'il sollicitait.

En France, Samuel Morse obtint facilement un brevet d'invention, pour son *télégraphe magnéto-électrique*. Mais la délivrance des brevets d'invention en France, n'avait aucune signification ni aucune portée pratique. Samuel Morse se décida en conséquence à revenir aux États-Unis, pour reprendre auprès de ses compatriotes et des membres du Congrès, les démarches interrompues.

Sans appui, sans secours, avec peu d'espérance, mais avec toute l'énergie et la ténacité du caractère américain, il lutta pendant quatre ans contre l'indifférence de ses compatriotes et la tiédeur du Congrès.

L'année 1843 fut mémorable pour l'histoire de la télégraphie électrique en général, et pour Samuel Morse en particulier. Ce fut alors qu'il vit sa persévérance couronnée de succès.

C'est en effet grâce à l'appui de miss Ellsworth, fille du directeur des brevets, et au hasard de cette rencontre, que le Congrès américain adopta l'appareil télégraphique de Samuel Morse.

Le *télégraphe magnéto-électrique* était officiellement né et devait se répandre dans le monde entier.

Le génie de Morse a été de concevoir une machine simple, pratique, efficace, bon marché, rustique, facile à utiliser et surtout de réussir à convaincre (non sans mal) ses contemporains de réaliser une expérience suffisamment spectaculaire pour frapper les imaginations.

L'invention de Morse se situe à deux niveaux :

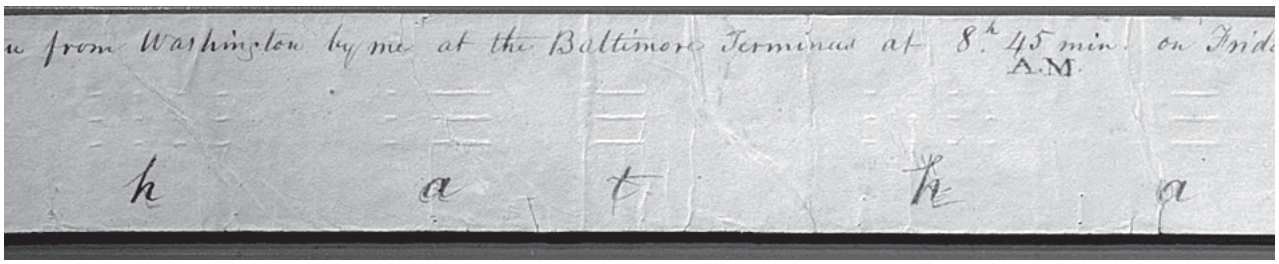
- la machine, manipulateur>fil>transcripteur sur bande de papier
- le code, composé de deux signes : courts et longs.

Si la machine fut détrônée par la suite par les télégraphes automatiques, téléscripteur... le code Morse est resté très longtemps d'actualité chez les militaires (les transmissions numériques modernes l'ayant maintenant supplanté) et chez les radioamateurs qui profitèrent de son efficacité sans rivale dans leur trafic radio en télégraphie.

Le code morse était aux transmissions ce que la bicyclette est aux transports de personnes : la voiture la plus puissante est bloquée dans un embouteillage urbain là où le cycliste passera toujours !

Depuis l'année 1845, aux États-Unis, le télégraphe a été mis à disposition du public, le gouvernement se réservant seulement 1 ou 2 fils sur les lignes établies par des compagnies privées. De ce fait, la télégraphie électrique a pris aux États-Unis un développement immense.

Les dépêches sont transmises d'après leur ordre d'inscription. Cependant, quelques messages d'une nature urgente ont droit à une expédition plus rapide, et prennent un tour de faveur ; telles sont, par exemple, les dépêches du gouvernement ou de la justice, celles pour la découverte de criminels et les nouvelles qui intéressent la presse. La personne qui envoie un message peut le transmettre en langue étrangère ou en chiffre secret.



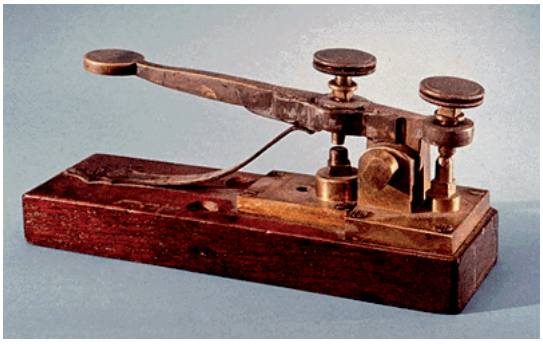
Extrait du message du 24 mai 1844.

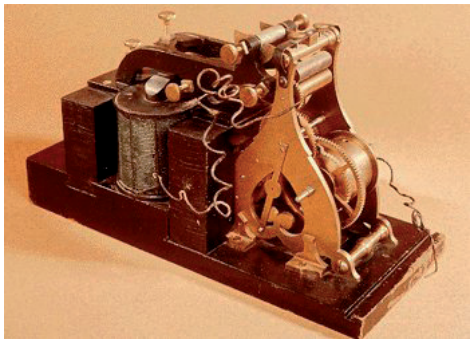
Annotation sur la bande de réception, de la main de Samuel Morse :

This sentence was written from Washington by me at the Baltimore Terminus a 8h45 min. A.M. on Friday May 24th 1844, being tho fist ever transmitted from Washington to Baltimore by telegraph, and was indited by my much loved friend Annie G. Ellsevortte.

Texte du message :

« *What hath God wrought ?* » : Quelle est l'œuvre de Dieu ? Exclamation biblique admirative que je comprends a peu près, vu le contexte (nombres 23 : 23), comme : « *De quels bienfaits Dieu ne nous a-t-il pas gratifié ?* ».





Manipulateur et récepteur ayant servi pour la transmission du message de 1844.

A	.–	N	–.	0	–––––
B	–...	O	–––	1	.––––
C	–.–.	P	.––.	2	..–––
D	–..	Q	––.–	3	...––
E	.	R	.–.	4	....–
F	..–.	S	...	5	.....
G	––.	T	–	6	–....
H	....	U	..–	7	––...
I	..	V	...–	8	–––..
J	.–––	W	.––	9	––––.
K	–.–	X	–..–	.	.–.–.–
L	.–..	Y	–.––	,	––..––
M	––	Z	––..	?	..––..

erreur	.....
début de transmission	–.–.–
fin de transmission	.–.–.

Code Morse de base

Le télégraphe électrique dans les autres pays

En Angleterre,

La plupart des lignes de télégraphie électrique qui fonctionnèrent à cette époque en Angleterre ont été créées par M. Wheatstone. Il s'agissait du *télégraphe à deux aiguilles*.

Cet appareil, qui reprenait le principe d'Alexander et de Schilling sur la déviation d'une aiguille aimantée, a été développé par MM. Cooke et Wheatstone en 1846. On voit deux aiguilles que mettent en mouvement, par l'intermédiaire du courant électrique, deux manivelles.

Pour faire tourner à volonté, tantôt à droite, tantôt à gauche l'une ou l'autre des aiguilles aimantées, il suffit de changer le sens du courant ; et ce changement est produit par le mouvement, à droite ou à gauche, que l'on imprime aux manivelles.

Les positions combinées que peuvent prendre les deux aiguilles ont servi à former un alphabet. Les signes adoptés pour la désignation des lettres sont les suivantes :

A, un coup à gauche de l'aiguille de gauche ;

B, deux coups de la même aiguille à gauche ;

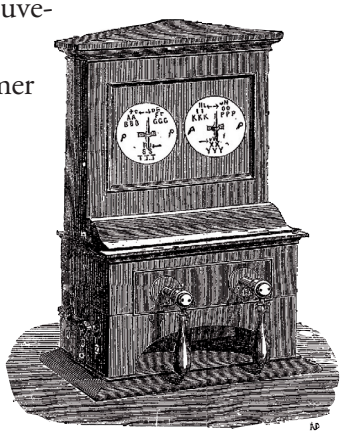
C, trois coups de la même aiguille à gauche ;

D, quatre coups de la même aiguille à gauche ;

E, un coup de l'aiguille de gauche et deux de l'aiguille de droite ;

F, un coup de l'aiguille de gauche et trois de l'aiguille de droite… etc.…

En fait, c'était le même code qui était employé, à cette époque, pour l'alphabet des sourds-muets, avec les doigts.



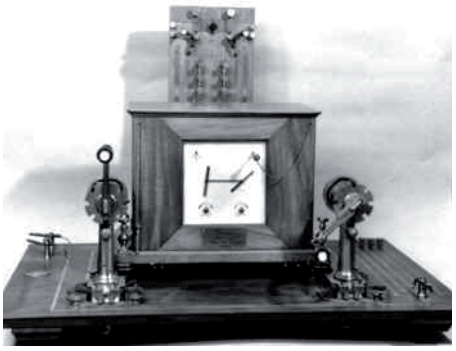
Télégraphe anglais à 2 aiguilles

En France,

La France a suivi de près l'Amérique et l'Angleterre dans l'adoption de la télégraphie électrique. Le monopole du télégraphe accordé à l'État provoqua bien entendu quelque retard…

En 1841, une ligne télégraphique avait été construite en Angleterre pour le service du chemin de fer du *Great Western*, entre Londres et la station de Slough, sur une longueur d'environ 6 lieues. L'établissement de cette ligne télégraphique chez nos voisins fit ouvrir les yeux à l'Administration française : M. Alphonse Foy s'empressa d'aller étudier sur place ce nouveau système.

Il est certain que si les chemins de fer n'avaient pas existé en France, l'adoption du télégraphe électrique aurait éprouvé un certain retard. Une ordonnance royale en date du 23 novembre 1844 ouvrit un crédit de 240.000 francs pour établir, à titre d'essai, une ligne télégraphique sur la voie de chemin de fer de Paris à Rouen.



Ce fut L. Bréguet qui fut chargé des travaux. C'est à lui que furent confiées les expériences nécessaires pour éclaircir le fait de l'emploi de la terre comme conducteur de retour. M. Foy lui confia la tâche difficile d'exécuter un appareil qui reproduisait exactement les signaux du télégraphe aérien (Chappe). L'appareil *Foy-Bréguet*, adopté en France, était passible d'un grave reproche : il exigeait deux conducteurs (deux fils télégraphiques) au lieu d'un seul comme le télégraphe Morse, car il fallait un fil par « branche » du télégraphe. Cet appareil fut abandonné après sept à huit années d'usage, un décret du 11 juin 1854 introduisant divers changements dans l'organisation des télégraphes. Ce fut le système Morse qui le remplaça d'autant plus que le système Morse était déjà utilisé en Allemagne, en Belgique et en Suisse, et il importait que les différents pays, pour faciliter la transmission des dépêches internationales, utilisent le même appareil télégraphique.

En Belgique et en Hollande,

En Belgique, la télégraphie électrique date de l'année 1846. La première ligne (de Bruxelles à Anvers) fut ouverte le 7 septembre1846. On y faisait usage du télégraphe à aiguille de MM. Wheatstone et Cooke. Mais cette ligne fonctionnait mal, et ce n'est qu'au bout de 10 ans, lorsque le gouvernement s'attribua le monopole de ce service, que les lignes furent construites avec activité. Le réseau belge se composait en 1862, de 2.000 km de lignes et de 5.000 km de fils. Le système (de codage) Morse est celui qui prédomine en Belgique.

La Hollande avait précédé de quelques mois la Belgique dans cette voie ; car la première ligne (d'Amsterdam à Rotterdam) fut ouverte le 29 décembre 1845. Ce n'est toutefois qu'en 1852, qu'une loi prescrivit la création d'un réseau télégraphique.

En Allemagne,

La première ligne allemande fut installée dans le duché de Hesse, entre Mayence et Francfort. Le succès de cette ligne éveilla l'attention du gouvernement prussien, qui mit à profit le nouveau procédé télégraphique pour relier le palais de Berlin avec celui de Postdam. En 1850, le réseau télégraphique de la Prusse était de plus de 600 lieues, et sa longueur presque double de celle du réseau français.

Les conditions libérales accordées aux États-Unis pour l'exploitation du télégraphe électrique, n'ont pas été imitées en Allemagne. En Prusse et en Autriche, ce moyen de correspondance est la propriété exclusive et le privilège de l'État ; cependant, le gouvernement le met, sous son contrôle et sous sa surveillance, à la disposition du public.

En Italie,

L'Italie n'est pas restée en arrière des autres nations de l'Europe dans l'adoption du nouveau moyen de correspondance. Les premières lignes électriques furent installées, en Toscane, en 1847, sous la direction du savant physicien Matteucci. La ligne de Gênes à Turin fut ouverte le 9 mars 1851, par les soins de M. Bonelli, directeur des télégraphes sardes.

En 1861, le réseau italien se composait de 6.896 km de lignes, mais ne dépassait guère les États du nord. Ce sont les appareils Morse qui sont employés de manière presque exclusive.

En Suisse,

L'établissement de la télégraphie en Suisse date de 1852. Dix ans après, il y avait près de 3.000 km de fils. On se sert en Suisse de l'appareil Morse.

En Espagne,

Ce n'est qu'en 1854 que l'Espagne, nation retardataire, établit, à titre d'essai, deux lignes électriques entre Madrid et Irun ; le 8 novembre de la même année, le discours de la reine d'Espagne franchissait les Pyrénées par cette voie nouvelle. Le premier appareil employé en Espagne fut l'aiguille aimantée de MM. Wheatstone et Cooke ; mais on ne tarda pas à le remplacer par le système Morse.

En Russie,

La première ligne russe a été ouverte en 1850, entre Tiflis et Borsom (Caucase). À mesure que les lignes de chemin de fer s'établissaient en Russie, les lignes télégraphiques les escortaient.

C'est à la Russie qu'appartint l'entreprise audacieuse de la ligne télégraphique qui va du centre de la Russie à l'intérieur de la Chine.

Jusqu'en Inde…

Une ligne télégraphique mettait l'Angleterre en correspondance directe avec l'Inde (en 1865). Elle passait par Belgrade, Bassora, Bagdad, le golfe Persique, Karachi et Calcutta. Il fallait moins de 12 heures pour transmettre une dépêche de Londres à Bombay !

Seulement l'installation des poteaux télégraphiques a exigé des soins particuliers en raison de la voracité des insectes. Ils furent donc faits en bois-de-fer d'Aracan. Ils ne sont pas simplement plantés dans le sol, mais dans une douille de fer encastrée dans une pierre. De plus, il fallait donner une hauteur minimum de 17 mètres à ces lignes pour qu'un éléphant, avec sa charge, puisse toujours passer dessous. Enfin, dernier « détail » les simples fils de cuivre, suffisants en Europe, durent être remplacés, en Inde, par de petites tringles de fer de 8 millimètres de diamètre, grosseur indispensable à cause des singes qui s'y suspendaient et « *ébranlaient ainsi tout le système par leur gymnastique désordonnée* » (cf. *Merveilles de la Science*, Louis Figuier).

Autres appareils de transmission électrique de textes et d'images originaux.

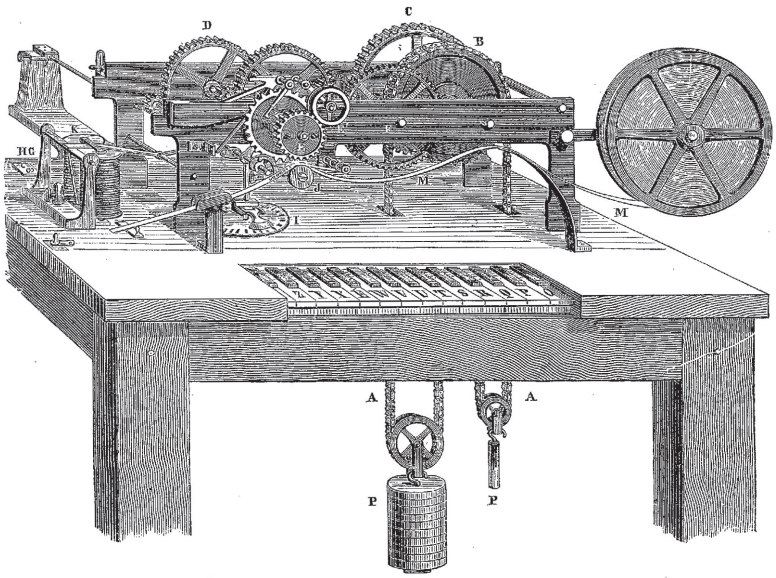
Les ancêtres du Fax.

Le système Morse présentait, et pour longtemps, bien des avantages en termes d'économies de moyens pour la transmission de dépêches ou de tous textes. Cependant, il pouvait être source d'erreurs, au codage ou à la lecture, erreurs, nous le verrons plus loin qui pouvait avoir des conséquences fâcheuses. Un certain nombre de savants se mirent donc à la recherche de procédés pouvant transmettre directement les messages manuscrits, d'éventuelles illustrations, plans ou signature par exemple.

La presse était intéressée également pour la transmission à distance de ses articles en respectant leur composition.

Dans un premier temps, ce fut un professeur de physique, M. Hughes, qui conçut un appareil, amélioré ensuite par Gustave Froment, et qui imprimait les dépêches en lettres ordinaires d'imprimerie. On appela cet appareil *télégraphe imprimeur*. N'ayant plus à « coder » les lettres d'un message, l'opérateur assurait un gain de temps notable puisqu'il pouvait en transmettre environ le double.

Ci-dessous l'appareil de M. Hughes.

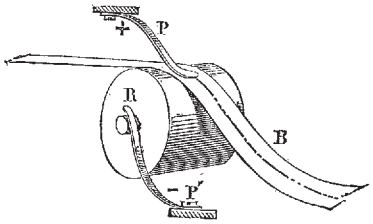


Le télégraphe électrochimique de Bain.

Il semblerait que ce soit le chimiste anglais Humphrey Davy qui eut le premier l'idée de former des signaux par le courant électrique sur un papier imprégné d'une substance décomposable par l'électricité. Ce savant faisait usage de papier imprégné d'iodure de potassium, qui, sous l'influence d'un courant électrique, se décomposait et laissait sur le papier des taches brunes.

Mais l'inventeur incontesté du système électrochimique appliqué à la télégraphie, est M. Bain, physicien anglais. Ces appareils ont été employés en Amérique, à partir de l'année 1843, concurremment avec ceux de M. Morse.

La figure ci-contre représente le style et la bande de papier de l'appareil qui a reçu de M. Bain, le nom de télégraphe électrochimique. Une bande de papier continu B, est entraînée, comme celle de l'appareil Morse, par un rouage qu'on met en mouvement lorsqu'on veut recevoir une dépêche. Cette bande de papier passe sur un cylindre métallique R ; là un ressort de fer ou d'acier P, vient la presser et la maintenir en contact



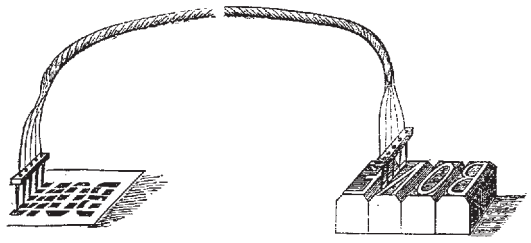
avec le cylindre R. Le papier a été d'avance, imprégné d'une dissolution de cyanure jaune de potassium et de fer (prussiate jaune de potasse). Chaque fois que le courant traverse le papier chimique en passant du ressort P (pôle positif) au cylindre métallique R (pôle négatif), une décomposition chimique a lieu. Le fer du ressort P est attaqué par le cyanogène mis en liberté par la décomposition du cyanure double, et il y a formation de bleu de Prusse (cyanure de fer). On produit ainsi des points et traits indélébiles, d'un beau bleu, se détachant sur le papier blanc ; ces points et ces traits sont les mêmes que ceux qui constituent l'alphabet Morse. Pour que la décomposition puisse avoir lieu, il faut que le papier soit toujours humide, ce qu'on obtient en ajoutant à la solution dans laquelle on le trempe, une matière hygrométrique, l'azotate d'ammoniaque.

On facilite encore cette décomposition en donnant au ressort P une grande surface, ce qui permet un passage plus facile à l'électricité.

L'appareil Bain a été, tant en Amérique qu'en Angleterre, le point de départ d'une foule de nouveaux télégraphes électrochimiques. Un inspecteur des lignes télégraphiques françaises, M. Pouget-Maisonneuve, a perfectionné l'appareil Bain, en faisant passer le ruban de papier entre deux pointes, comme dans l'appareil Morse.

Dans son télégraphe typographique, M. Bonelli fait usage d'un papier chimique, et les signes sont tracés sur le papier, par la décomposition de la substance, imprégnant ce papier. Cette substance, c'est l'azotate de manganèse : le courant électrique décompose ce sel, et laisse à nu de l'oxyde de manganèse, qui forme sur le papier, des traits bruns, fortement accusés.

Mais le papier chimique est l'élément accessoire de l'appareil qui va nous occuper. C'est le principe du télégraphe typographique qui fait l'intérêt et l'originalité de cette invention, et ce principe, le voici :



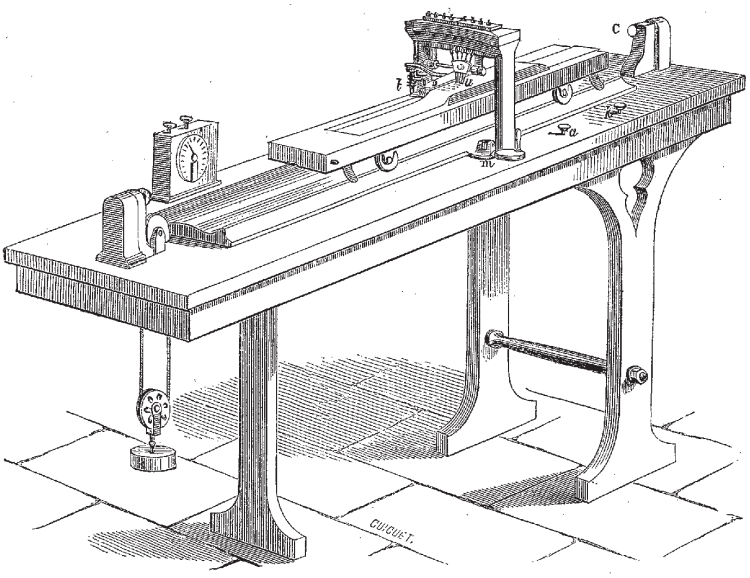
Imaginons un fil télégraphique qui se termine, à chacune des deux stations, par une pointe de platine. Sous la pointe qui représente le pôle positif de la pile, faisons passer un ruban de papier, imbibé d'une solution d'azotate de manganèse et appliqué sur une règle de fer argenté, communiquant avec le sol ; pendant que sous l'autre pointe, qui correspond au pôle négatif, défile une dépêche, préalablement composée en caractères typographiques, également en communication avec le sol. Tant que cette pointe rencontre le relief d'un caractère d'imprimerie, le courant passe, et à la station d'arrivée, le nitrate de manganèse, réduit par le courant, forme sur le papier une tache de couleur brune. Lors que la pointe qui fonctionne à la station de départ, se trouve sur un creux du caractère typographique, le courant est interrompu, et la partie du papier qui défile sous l'autre pointe, conserve sa blancheur.

Mais il est évident que cette succession de taches brunes et d'intervalles blancs, ne suffirait pas pour reproduire la forme des caractères. M. Bonelli a reconnu que, pour reproduire cette forme, il faut mettre en jeu, à chaque station, trois pointes, isolées l'une de l'autre, et en communication avec trois fils conducteurs d'une pile voltaïque. Les trois pointes réunies forment les dents d'une sorte de petit peigne, que l'on place perpendiculairement au centre de la ligne des caractères.

Si, au lieu de faire passer sous ce peigne une composition typographique, on l'appuyait sur une plaque métallique unie, le peigne à la station d'arrivée tracerait sur le papier chimique trois lignes parallèles, comme celles qui servent à écrire la musique, mais très serrées. Maintenant, si le peigne appuie sur un caractère typographique, les dents qui rencontreront le relief détermineront, à la station opposée, autant de petites taches brunes sur le papier mobile, tandis que l'espace qui correspond au creux de la lettre sera blanc, parce que, à la station de départ, les dents qui se trouvent au-dessus du creux sont hors de communication avec le métal des types. Supposons, par exemple, que la lettre D vienne à défiler sous le peigne, ce peigne glissera d'abord sur la barre du D, et à l'autre station les cinq dents marqueront cinq

petits traits parallèles sur le papier ; au moment suivant, la première et la cinquième dent seules toucheront les lignes horizontales supérieure et inférieure du D, et à la station d'arrivée, le papier, qui s'est déjà déplacé d'une quantité égale, recevra les marques rectilignes des deux dents extrêmes pendant quelques instants ; enfin, les pointes extrêmes quitteront le relief de la lettre D, et les trois dents du milieu viendront s'y poser de nouveau, ce qui déterminera, à l'autre bout de la ligne, l'impression de trois taches très rapprochées qui formeront la figure du D. Les lettres ainsi imprimées, sont presque aussi faciles à lire qu'une impression ordinaire.

Tel est le principe du télégraphe typographique. Disons maintenant comment ce principe est mis en œuvre.



Sur une table de fer, longue de 2 mètres, est placé (figure) un petit chemin de fer, terminé à ses deux extrémités, par des arrêts-ressorts, et traversé au milieu, par un petit pont qui porte le peigne *u*. Sur ces rails marche un chariot en fer à quatre roues, long d'un mètre, large de 25 centimètres, qui porte la dépêche, composée en caractères ordinaires d'imprimerie, et une règle en fer *t*, munie d'une bande de papier chimique. Quand les chariots sont préparés aux deux stations, chaque opérateur touche un bouton C, et fait ainsi lâcher prise aux ressorts qui retiennent le chariot, lequel se met aussitôt à rouler, entraîné par un poids qui agit sur lui au moyen d'une corde. Les trois fils conducteurs des trois piles voltaïques se placent aux boutons *m, a, k*.

Si, dans la première station, les caractères typographiques sont placés à gauche sur le chariot, et la règle à droite, dans la station opposée, on observera l'ordre inverse. De cette façon, pendant la première moitié de la course des chariots, les types passent les premiers à la première station, le papier à la seconde, puis le papier à la première et les types à la seconde station. La course des chariots dure douze secondes, pendant lesquelles chaque station a envoyé une dépêche et en a reçu une autre.

Les *composteurs* contiennent de 2 à 30 mots, en moyenne. La composition des dépêches se fait par quelques jeunes ouvriers, qui emploient environ une minute et demie pour une dépêche. La transmission de 25 mots se fait donc en six secondes.

Pour obtenir la dépêche en double, il suffit de bifurquer les courants à leur arrivée et de les faire aboutir à deux peignes au lieu d'un. Ainsi, on peut envoyer au destinataire le ruban de papier sur lequel l'instrument a écrit le télégramme, et l'Administration peut garder le double de la dépêche qu'elle envoie.

Grâce à cet ingénieux système, la composition même d'un journal pourrait servir à la reproduction télégraphique. Une nouvelle, à peine imprimée à Paris, serait expédiée, à Marseille ou à Lyon, imprimée avec les mêmes caractères. La composition qui aura servi au *Moniteur*, par exemple, étant portée au bureau télégraphique voisin, pourrait paraître presque au même instant, à Marseille. Voilà un résultat qui suffit pour faire apprécier l'importance et l'avenir de ce système.

Si l'on veut maintenant établir une comparaison entre la rapidité avec laquelle fonctionne un appareil Morse, et celle qui nous est promise par l'appareil de M. Bonelli, il ne restera aucun doute sur la supériorité de ce dernier. Cinq compositeurs, qui ne seront que de simples ouvriers, pouvant chacun composer 30 dépêches de 20 mots par heure, on aura 450 dépêches par heure et par station, soit 300 par heure en tout. Dans une journée de travail, cela ferait 400.000 mots, ce qui représente le contenu d'un petit

volume in-12 de 300 pages. Avec le même nombre d'employés, on obtiendrait donc trois fois autant d'ouvrage qu'avec le télégraphe Morse ; en outre, les dépêches seraient immédiatement imprimées en double, presque sans erreur possible, par un procédé mécanique aussi sûr que facile à exécuter.

Avec de tels appareils, la télégraphie électrique pourra être mise en pratique par les typographes, et deviendra ainsi un métier accessible au commun des ouvriers. C'est là évidemment un progrès manifeste l'art de la télégraphie électrique se vulgarisera.

Nous avons décrit le télégraphe typographique avec trois fils conducteurs, c'est-à-dire exigeant l'emploi de trois courants voltaïques, tandis qu'il suffit d'un fil au télégraphe Morse, au télégraphe Hughes et au télégraphe à cadran. Tel est, en effet, le système qui fonctionne entre Manchester et Londres. Mais M. Bonelli a récemment simplifié son appareil : il se contente d'un seul conducteur. Les expériences faites à Florence, au mois de février 1867, avec le télégraphe typographique à un seul fil, ont donné un résultat des plus extraordinaires : dans une heure, ce télégraphe a pu composer jusqu'à cent dépêches de vingt mots. Nous ne pouvons toutefois, décrire ici cette disposition nouvelle du télégraphe typographique, qui permet de se contenter d'un seul fil pour la transmission de l'électricité, sans nuire à la netteté de l'impression ni à la rapidité de l'expédition, car M. Bonelli n'a pas encore rendu publique cette importante modification de son système.

Le dernier appareil dont nous ayons à parler, c'est le *pantélégraphe*, de M. Caselli.

M. l'abbé Giovanni Caselli était professeur de physique à l'université de Florence, lors qu'il fut tenté par la solution d'un problème physico-mécanique qui avait paru jusque-là impossible : la reproduction, par l'électricité, des signes de l'écriture à la main, des traits du dessin, et en général, de toute œuvre de la main de l'homme. Quelques tentatives avaient été faites dans cette direction, mais leur insuccès avait confirmé tous les mécaniciens dans l'idée de l'impossibilité de trouver la solution pratique de ce problème.

C'est le physicien anglais Bain, l'inventeur du télégraphe électrochimique, qui, le premier, s'occupa d'exécuter un *télégraphe autographique*, en d'autres termes un appareil reproduisant le *fac-similé* d'une écriture ou d'un dessin quelconque, et réalisant ainsi un effet bien plus compliqué que nos télégraphes imprimeurs, où tout se borne à imprimer sur le papier des caractères uniformes.

M. l'abbé Caselli ne crut pas néanmoins au-dessus des efforts de l'art contemporain la reproduction de l'écriture par l'électricité. Il vint à Paris, installa chez Gustave Froment le *pantélégraphe* qu'il avait construit à Florence en 1856 et pendant six ans, il ne cessa pas un seul jour de se consacrer au perfectionnement de cet appareil.

Il s'agissait d'établir à chacune des deux stations télégraphiques, deux pendules dont les oscillations fussent exactement les mêmes en amplitude et en durée, c'est-à-dire d'installer, à vingt lieues de distance, deux pendules isochrones. Assurer, malgré la distance, l'isochronisme absolu de deux pendules, cela paraissait, à la plupart des physiciens, quelque chose comme la quadrature du cercle ou la pierre philosophale.

Cette pierre philosophale de la télégraphie, M. l'abbé Caselli a fini par la trouver, car en 1863, l'appareil qu'il avait construit, avec le secours de Gustave Froment, donnait des résultats irréprochables. On pouvait, avec cet instrument, reproduire une dépêche d'une ville à l'autre, avec l'exacte fidélité d'une photographie. L'appareil Caselli donne, en effet, de véritables *fac-similés* de l'écriture de l'expéditeur. Il transmet l'écriture même, la signature même de l'expéditeur. Un dessin, un portrait, un plan, de la musique, une écriture étrangère, des traits confus et embrouillés, tout arrive fidèlement et se reproduit dans son intégrité d'une station à l'autre.

Le gouvernement français fut frappé des avantages et du côté brillant de l'invention du savant florentin. Au mois de mai 1863, une loi présentée au Corps législatif, et votée par cette assemblée, proclamait l'adoption du pantélégraphe Caselli par l'administration française et son établissement sur la ligne de

Paris à Lyon. Depuis cette époque, c'est-à-dire en 1867, il a été décidé que le même appareil serait placé également sur la ligne de Marseille à Lyon.

Le 16 février 1865, le public fut admis, pour la première fois, à transmettre des dépêches autographiques entre Paris et Lyon. Une ordonnance ministérielle régla la taxe des dépêches, plans, dessins et figures quelconques expédiés par le pantélégraphe Caselli. Cette taxe est calculée d'après la dimension de la surface du papier employé, à raison de 20 centimes par centimètre carré.

L'administration des lignes télégraphiques met en vente des papiers métalliques, qui sont destinés aux transmissions autographiques, au prix de dix centimes la feuille, quelle qu'en soit la dimension. Ces feuilles sont de quatre grandeurs de 30, de 60, de 90 et de 120 centimètres carrés. L'expéditeur peut, en se servant d'une écriture très serrée, dire beaucoup de choses sur la plus petite des feuilles autorisées ; mais cet avantage est peut-être moins sérieux qu'on ne pourrait le croire au premier abord, car les traits bleus sont toujours légèrement nuageux, comme des traits à la plume sur un papier qui boit ; il y a donc une limite de finesse pour l'écriture des dépêches, qu'on ne saurait dépasser sans rendre la copie illisible.

Mais il est temps d'arriver à la description de cet appareil et à ses merveilleux résultats.

Deux pendules, dont les oscillations sont parfaitement isochrones, sont placés, l'un à la station du départ, l'autre à la station d'arrivée. Ils servent à imprimer un mouvement absolument égal à la pointe traçante qui doit parcourir toute leur surface.

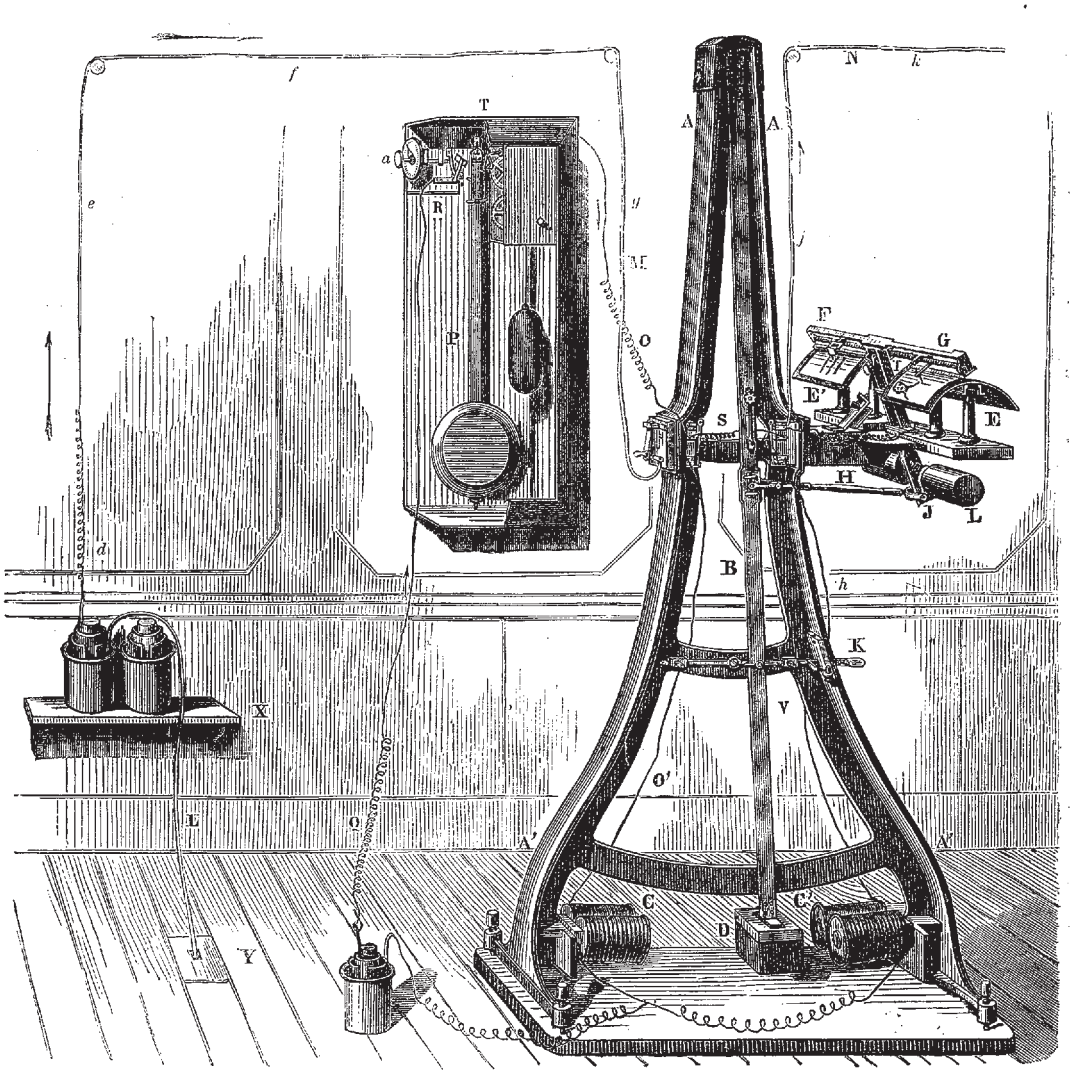
À la station du départ, on écrit, à la plume, la dépêche à transmettre, en se servant d'encre ordinaire et d'un papier argenté. Le papier argenté, portant l'original de la dépêche, est placé sur une tablette courbe de cuivre. Une fine pointe en platine, qui est animée d'un mouvement horizontal, et qui obéit à la pression d'un faible ressort, s'appuie sur la surface de la tablette, et parcourt continuellement cette surface par un mouvement très rapide. Par suite du mouvement de translation horizontale de cette pointe, tous les points de la tablette sont mis successivement en contact avec la pointe du style. Or, ce style métallique, et par conséquent conducteur de l'électricité, est lié au fil de la ligne télégraphique. Comme le fond métallique sur lequel la dépêche est écrite est conducteur de l'électricité, tandis que les caractères sont composés d'encre, substance non conductrice de l'électricité, il en résulte que le courant électrique est établi ou suspendu dans le fil de la ligne télégraphique, selon que le style vient se mettre en contact avec le papier métallique de la dépêche ou avec les caractères tracés à sa surface.

On comprend maintenant ce qui va se passer à la station d'arrivée. Là se trouve une tablette de cuivre toute pareille à celle de la station du départ. Sur cette tablette est tendue une feuille de papier ordinaire, contenant un peu de prussiate de potasse. Un style de fer, qui est en communication avec un style tout semblable, par l'intermédiaire du fil de la ligne télégraphique, parcourt, par un mouvement très rapide, toute la surface de ce papier. Chaque fois que le style de la station du départ rencontre le fond métallique de la dépêche, le courant électrique s'établit, et le style de fer, à la station d'arrivée, imprime un point, une tache sur le papier chimique, parce que le fer du style, sous l'influence de l'électricité, décompose le prussiate de potasse du papier, et laisse une tache bleue, composée de bleu de Prusse, dont l'électricité a provoqué la formation. La réunion de ces points bleus, de ces taches azurées, finit par reproduire tous les traits qui composent la dépêche placée à la station du départ. L'autographe est donc reproduit au moyen d'une multitude de lignes parallèles tellement rapprochées entre elles que l'œil ne saurait les distinguer.

Le difficile en tout cela, c'était d'obtenir une égalité absolue de vitesse entre le mouvement de la pointe traçante qui parcourt la tablette portant la dépêche, à la station du départ, et celui du style qui parcourt la tablette portant le papier chimique à la station d'arrivée. C'est parce que M. l'abbé Caselli a trouvé l'art de rendre isochrones les mouvements de ces deux styles séparés par une énorme distance, que notre heureux physicien a trouvé ce qui semblait la pierre philosophale de la télégraphie électrique.

Après l'explication générale que nous venons de donner, des organes essentiels du pantélégraphe Caselli, il sera plus facile de comprendre les détails de la figure, qui donne une vue fidèle de cet instrument, prise au poste central des télégraphes de Paris.

Pour comprendre cet appareil, il faut examiner séparément le mécanisme qui provoque le mouvement régulier et isochrone du pendule, et le système électromécanique qui permet l'exécution du dessin sur le papier. Nous parlerons d'abord du système qui produit l'isochronisme du pendule.



Entre deux montants de fonte A, A, oscille un pendule BD, de 2 mètres de longueur, et nous n'avons pas besoin de dire que deux appareils identiques fonctionnent, l'un à la station qui envoie la dépêche, l'autre à la station où doit s'inscrire la même dépêche. Ce pendule BD se termine par une masse de fer D, lestée de plomb. Le fer de ce pendule peut être attiré par les deux électro-aimants C, C'. L'attraction de ces deux électro-aimants, tel est donc le principe moteur de cet organe. L'oscillation du pendule BD se transmettant à la tige de bois, H, un ensemble de pièces mécaniques assez compliquées E, GFI, que nous décrirons tout à l'heure, détermine la marche régulière du style métallique, ou pointe traçante, sur toute la surface de la plaque E.

Mais avant d'expliquer ce mécanisme, il importe de dire par quel moyen les mouvements du pendule BD sont rendus parfaitement isochrones avec ceux du pendule semblable placé à la station opposée. Cet isochronisme a été obtenu par M. Caselli, après bien des tâtonnements, en se servant d'une horloge ordinaire, dont le balancier vient interrompre, à des intervalles parfaitement égaux, le courant de la pile qui se rend aux électro-aimants et provoque les oscillations du pendule BD.

L'horloge T est munie d'un balancier P. Le fil Q, partant d'une pile voltaïque dont on n'a représenté qu'un seul élément sur la figure, aboutit à un petit levier métallique, que l'on voit au-dessous du point R, et qui se trouve en contact avec la tige P du balancier de l'horloge, pendant son mouvement d'oscillation. La tige P de ce balancier étant quatre fois plus courte que la tige BD du pendule électromagnétique, ce balancier, d'après la loi physique qui régit les oscillations du pendule (la vitesse des oscillations d'un pendule est en raison inverse du carré de la longueur de ce pendule), décrit deux allées et venues, pendant que la tige du pendule BD en décrit une seule. Dès lors la tige P du balancier exécutant quatre oscillations, tandis que celle du grand pendule n'en exécute que deux, la tige de ce balancier P peut établir et interrompre le courant électrique, à chaque demi-oscillation du pendule électromagnétique BD.

Dans l'état ordinaire, le courant électrique, suivant le fil Q, continue sa marche par le fil O, la pièce métallique S, et se rend, par le fil O', à l'électroaimant C, lequel attire la masse de fer du pendule D. Mais le balancier de l'horloge T, vient en soulevant, au point R, le fil conducteur Q, interrompt, pour un instant, le passage du courant. Dès lors, l'électroaimant C n'étant plus parcouru par l'électricité celui-ci devient inerte, le pendule D s'en détache et tombe de son propre poids. Dans l'intervalle du temps qui suit, la continuité du courant, amené par le fil Q, est rétablie par le départ du balancier de l'horloge, qui ne soulève plus ce fil au point R, et un commutateur, placé à l'intérieur de la pièce métallique S, fait passer le courant dans le fil V, qui le dirige dans l'électro-aimant C'. Ainsi parcouru par l'électricité, cet électroaimant C' attire la masse métallique D, qui venait tout à l'heure de retomber par son propre poids, et lui fait exécuter une demi-oscillation, qui complète son mouvement d'allée et venue.

Toutes ces actions se répétant, c'est-à-dire le balancier P de l'horloge T interrompant le contact au point R, et venant ainsi désaimanter successivement les bobines C et. C', entretient le mouvement oscillant et régulier du pendule électrique BD.

La manivelle K sert à mettre en prise, c'est-à-dire à établir à l'aide d'un contact particulier, la continuité dans tout ce système de communication de corps conducteurs.

Ainsi, c'est le balancier P de l'horloge T qui communique au pendule BD ses oscillations régulières, lesquelles se transmettent, par la tige de bois H, au système mécanique qui détermine la progression du style, ou pointe traçante, sur le plateau courbe destiné à expédier et à recevoir la dépêche.

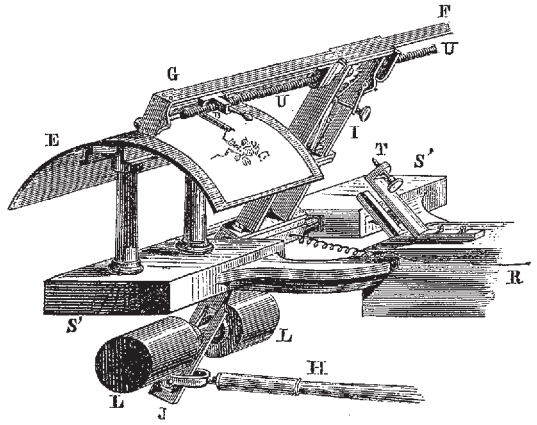
Pour que les deux appareils placés, l'un à la station du départ, l'autre à la station d'arrivée, fonctionnent avec un isochronisme absolu, il faut donc que les deux horloges placées aux deux stations marchent avec un mouvement d'une identité pour ainsi dire mathématique. Ces deux horloges ont été construites parfaitement semblables dans toutes leurs parties, et elles marchent ensemble avec un parfait accord. Cependant, malgré cet accord des deux chronomètres, leurs balanciers ne pourraient jamais osciller d'une manière vraiment isochrone, et imprimer à l'appareil un mouvement identique, s'il n'existait pas un moyen de les mettre encore plus d'accord, c'est-à-dire de les régler l'une et l'autre d'une manière parfaitement identique.

Cet accord absolu des oscillations du balancier P, était un problème mécanique extrêmement difficile. M. Caselli l'a résolu par un moyen nouveau et très ingénieux. Près du point R, il a placé un petit arrêt, ou butoir, que l'on manœuvre au moyen d'un pas de vis réglé par un bouton et un cadran *a* : en tournant le bouton et l'aiguille du cadran, on place ce butoir, ou arrêt, contre lequel vient heurter le pendule, à des distances identiques sur les appareils de l'une et de l'autre station ; et dès lors, l'isochronisme absolu du mouvement du pendule P de l'horloge T, qui commande les mouvements du pendule électromagnétique BD, et par suite celui du plateau courbe E, se trouve parfaitement assuré.

Il faut maintenant expliquer en détail ce dernier système mécanique, c'est-à-dire le jeu de la pointe traçante, sur la plaque E. Pour expliquer ce mécanisme, nous représentons sur une plus grande échelle la partie EG, en conservant les mêmes lettres que dans la figure précédente.

E, représente un plateau métallique courbe, sur lequel on fixe, à la station du départ, le papier métallique destiné à recevoir la dépêche de l'expéditeur, et qui doit se reproduire sur le plateau semblable, à la

station d'arrivée. Sur un même appareil, ces plateaux (E, E' de la figure précédente) sont au nombre de deux dans chaque station, ce qui permet d'expédier deux dépêches à la fois avec un seul fil; mais, comme ils sont identiques, nous n'en décrirons qu'un seul.



Ce plateau métallique courbe, E doit être parcouru sur sa surface tout entière par le style. Il faut pour cela que le style exécute deux mouvements simultanés : il faut qu'il suive la courbe du plateau E, d'une extrémité à l'autre ; et qu'en même temps, il trace des lignes successivement parallèles tout le long de ce même plateau. Voici comment est réalisé ce double mouvement de la pointe traçante. La tige de bois H, mue par le pendule électrique, au moyen de l'articulation J, fait basculer le levier JI, autour de son point d'appui. Un double contrepoids circulaire LL, sert à équilibrer la masse de ce levier, de la vis U et de la règle GF, afin que le centre de gravité du système oscillant tombe au point de suspension de ce même système, à la manière du fléau d'une balance, disposition qui lui donne une grande mobilité, et facilite son déplacement par la plus petite force. Les impulsions successives que reçoit le levier I, par l'intermédiaire de la tige de bois H et de t'articulation J, qui se transmet au levier I, produisent donc le mouvement curviligne de la pointe traçante, dans le sens de l'arc de cercle du plateau courbe E.

Quant au mouvement de translation du même style, il est réalisé à l'aide d'une longue vis taraudée, portée par une règle FG, et pourvue d'une roue à rochet à douze dents, qui est fixée au noyau de la vis. À chaque demi-oscillation du levier I, cette roue tourne d'une certaine quantité, et la pointe traçante se déplace horizontalement d'une quantité proportionnelle. Grâce à ce double mouvement, la pointe traçante parcourt successivement la surface entière du plateau courbe E.

Plaçons maintenant sur la ligne télégraphique l'appareil qui vient d'être décrit et voyons comment le courant électrique, traversant le *pantélégraphe* placé à la station du départ, va agir en suivant le fil conducteur qui réunit les deux stations sur l'appareil de la station opposée, où doit s'inscrire la dépêche X est la pile du poste télégraphique : elle est composée, pour la ligne de Paris à Lyon, d'environ cinquante éléments de Daniell : mais on n'a représenté que deux de ces éléments. L'électricité positive, fournie par cette pile, suit le fil *de*, d'une part, et d'autre part le fil L, pour se perdre dans la terre, au moyen de la plaque conductrice Y. Parcourant le fil *defg* dans le sens que représentent les flèches, cette électricité suit un conducteur placé à l'intérieur de la pièce métallique S, et grâce à la continuité des pièces métalliques, elle vient aboutir à la pointe traçante du plateau courbe E, lequel parcourt successivement, comme nous l'avons expliqué, tous les points de la surface de ce plateau.

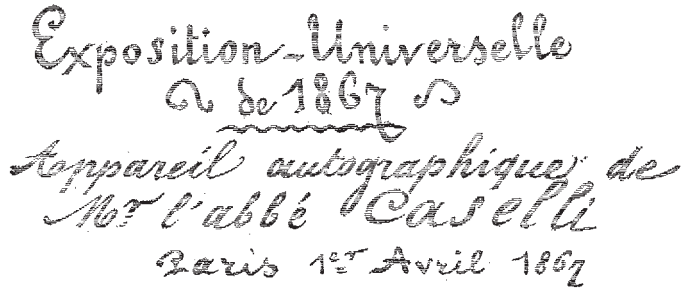
La dépêche que l'on veut transmettre à l'appareil de la station d'arrivée a été préalablement écrite ou dessinée, sur une feuille d'étain, à l'aide d'encre ordinaire. Tant que la pointe du style ne rencontre sur son chemin que la surface conductrice de la feuille d'étain sur laquelle a été inscrite ou dessinée la dépêche, le courant électrique qui a suivi la ligne *defg* et delà le plateau circulaire E, continue son chemin le long du fil *h*, et, grâce à la continuité du bâti métallique AA', elle s'écoule librement dans le sol ; de telle sorte que le courant circule continuellement dans l'appareil, et se perd dans la terre par le fil *h*. Mais lorsque le style arrive sur les parties qui ont reçu le dessin, et qui sont recouvertes d'encre grasse, substance non conductrice de l'électricité, l'écoulement dans le sol est fermé au courant, le quel dès lors s'élance, par le conducteur *jh*, dans le fil de la ligne, et va aboutir au pantélégraphe placé à l'autre poste télégraphique. Parvenue sur le plateau courbe E du pantélégraphe de la station d'arrivée, l'électricité positive rencontre le papier chimique qui est étalé sur ce plateau courbe. Ce papier a été trempé d'avance dans une dissolution de cyanoferrure de potassium et de fer. Le courant d'électricité positive, conduit par

la pointe métallique décompose ce sel, et forme sur le papier une tache de bleu de Prusse. On voit alors apparaître sur le papier chimique qui recouvre le plateau E, une série de traits bleus, qui reproduisent d'une manière identique, les parties encrées qui ont été touchées par le style sur la dépêche placée à la station du départ. Quand le style, ayant parcouru toutes les parties encrées de l'original placé à la station du départ, ne rencontre plus d'encre grasse, l'électricité ne passe plus dans le fil de la ligne, et continue à s'écouler dans le sol.

La dépêche originale est reproduite sur le papier chimique placé à la station d'arrivée, en caractères qui présentent à peu près la forme suivante.

Le poinçon, ou style traçant, met deux minutes à accomplir les mouvements de va-et-vient qui sont nécessaires pour rayer toute la surface métallique accordée à une dépêche, et qui est, comme nous l'avons dit, de 30 centimètres.

Tel est le merveilleux appareil dû à la patience et à la sagacité du savant abbé florentin, et qui constitue assurément une des plus grandes merveilles de la mécanique et de l'électricité.



Le pantélégraphe Caselli, qui reproduit avec une exactitude suffisante, tous les signes de l'écriture et du dessin, avait été, proposé pour transmettre l'écriture, ainsi que des *fac-similés* de dessin. Mais ce dernier objet s'est trouvé sans utilité dans la pratique. C'est à peine si quelques modèles de dessins de fabrique ont été expédiés de Lyon à Paris, depuis l'ouverture du service public de cet appareil. Quel est donc l'emploi auquel ce pantélégraphe est consacré ? Il s'est attiré la préférence des négociants par la certitude de transmettre les chiffres, sans erreur possible de la part des employés. Sur 4.860 dépêches qui ont été échangées entre Paris et Lyon, en 1866, 4853 avaient pour objet des opérations de bourse. Ici, on le comprend, l'exactitude absolue dans la transmission des chiffres, est une condition fondamentale. L'homme d'affaires, l'homme de bourse, consent facilement à payer pour une dépêche qu'il écrit de sa propre main, et qui porte, avec sa signature et son paraphe, l'énoncé exact des sommes et des chiffres qu'il veut transmettre à son correspondant.

Une anecdote, fournie par la chronique télégraphique, viendra ici à point, tant pour terminer un chapitre quelque peu épineux de descriptions mécaniques, que pour appuyer la considération qui précède.

Un négociant d'une de nos villes de département avait expédié à un agent de change de Paris, une dépêche télégraphique ainsi conçue :

Les actions de la Banque monteront, sans doute, à la bourse de demain. Achetez-m'en trois. Mille amitiés. Blanchard.

L'employé du télégraphe supprima, par distraction, un point de la troisième phrase, et la dépêche adressée à l'agent de change, devint :

Les actions de la Banque monteront, sans doute, à la bourse demain. Achetez-m'en trois mille. Amitiés. Blanchard.

Heureusement pour notre spéculateur la hausse arriva ! Que serait-il arrivé si les actions avaient baissé à la Bourse ? Qui aurait été responsable de la perte ?

À partir des années 1870, le développement du télégraphe électrique prit un essor considérable. Des limites techniques apparurent rapidement qui portaient en particulier sur la quantité de messages à transmettre et le temps que cela demandait. Il fallut donc trouver des moyens d'augmenter la vitesse de transmission afin d'accroître le nombre de dépêches transmises dans un temps donné.

Les techniques employées furent de trois ordres :

La première consistait en un système de bande perforée à l'avance par l'expéditeur, qui grâce à un *transmetteur automatique*, travaillait en continu et beaucoup plus rapidement qu'un manipulateur humain. Ce système fut communément désigné sous le nom de *Jacquard électrique* parce qu'il rappelle les cartons perforés du métier Jacquard. Pendant le temps de la rédaction de la dépêche, la ligne était libérée pour d'autres transmissions. Les perforations suivaient le format du code Morse classique et étaient réalisées grâce à un appareil du nom de *perforateur Wheatstone*.

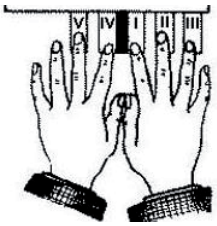
La seconde technique fut la *transmission simultanée*, consistant à envoyer plusieurs dépêches à la fois sur le même fil. C'est le *duplex*. C'est à un savant autrichien, le Dr Gintl, de Vienne, que l'on doit la première idée de la transmission simultanée des dépêches dans le même fil ; mais c'est un Américain, M. Stearn, qui transposa l'idée dans la pratique.

La troisième technique fut la *transmission multiple*. Les systèmes télégraphiques à transmission multiple sont fondés sur le fait que la rapidité de transmission des actions électriques étant incomparablement plus grande que celle que l'employé le plus exercé peut atteindre dans la manœuvre d'un appareil transmetteur, on peut utiliser le temps perdu par la main de l'employé, quand elle est inactive, en appliquant au même fil le travail de plusieurs autres employés, qui se succèdent périodiquement. Dans la pratique, le système de la *transmission multiple* consiste à diviser le temps de la transmission en intervalles réguliers et périodiques. Le système fut imaginé en 1860 par Rouvier, inspecteur des lignes télégraphiques françaises ; mais la première application n'en fut réalisée qu'en 1871, par Meyer, employé de l'administration des télégraphes de Paris, qui s'en servit pour produire des signaux Morse.

L'appareil Meyer a ensuite été abandonné au profit du *télégraphe Baudot* qui en est un perfectionnement considérable. Il avait, en plus de la faculté de transmettre le travail de 4 ou 6 employés, d'imprimer sur une bande de papier les dépêches transmises en caractères typographiques.

Ci-contre, le récepteur Baudot.

et ici, le clavier manipulateur.



Une autre technique qui se rattache aux t*ransmissions multiples* est la *sténotélégraphie*. Le principe utilisé est le même que le télégraphe Morse, sauf que le manipulateur comporte deux touches, une pour les points et une pour les traits du code Morse. Le récepteur quant à lui a deux stylets. On n'a donc pas à faire varier la longueur de l'impulsion pour former les signaux, ce qui augmente donc la rapidité d'émission. Cet appareil, le *sténo-télégraphe d'Estienne* fut adopté par l'Allemagne, l'Italie, la Russie, la Belgique et la Suède, ainsi que par la France bien entendu.

Citons enfin le *sténo-télégraphe* de M. A. Cassagne, ingénieur directeur des Annales industrielles, qui est une application de la *machine sténographique* de M. Antoine Michela. Cette machine fut expérimentée au Sénat, à la Chambre des députés, et au Conseil municipal de Paris en 1881. Elle permet d'enregistrer graphiquement, à la vitesse de la parole, avec une combinaison d'un très petit nombre de signes, environ 200 mots à la minute. M. Cassagne combina le système de télégraphie Morse et la machine Michela, ce qui lui permit d'obtenir un rendement de l'ordre de 400 mots à la minute !

Les applications du télégraphe électrique.

Hors la transmission de correspondance privée, ou des cours de la Bourse, le télégraphe électrique trouva sa place dans des applications particulières.

L'emploi du télégraphe électrique pour le service et l'exploitation des chemins de fer fut d'une importance primordiale. Pour la météorologie, c'est à un savant anglais, l'amiral Fitz-Roy, que l'on doit l'idée de signaler par le télégraphe les perturbations atmosphériques plusieurs jours à l'avance. En France, c'est à Le Verrier que l'on doit la création d'un service télégraphique destiné à prévoir le temps. Dès 1860, les côtes étaient divisées en régions qui contiennent des ports maritimes, et le télégraphe leur expédie chaque jour les indications de prévision du temps à venir. On fit par la suite usage de sémaphores électriques. Toujours concernant la mer, en Norvège, la pêche au hareng fut organisée en fonction du repérage des bancs de poissons dont la position fut transmise par télégraphe électrique.

On retrouve également l'usage du télégraphe pour l'annonce des crues des rivières et des fleuves.

À Paris, on mit en place dans les années 1865/70, 133 postes de secours contre l'incendie. En Amérique, 80 villes étaient déjà équipées d'un tel système, mais également l'Allemagne et la Hollande.

Enfin, bien entendu, les militaires firent usage du télégraphe électrique pour leurs communications. C'est en 1857, à l'époque de la conquête de la grande Kabylie que le maréchal Randon organisa un service de télégraphie. Évidemment, le matériel a été adapté pour être portatif (relativement…). On pense évidemment à cette époque à « chiffrer » les dépêches, car l'interception en est très facile en établissant une dérivation sur la ligne. Pendant le siège de Paris (sept. 1870) les armées allemandes tirèrent un grand parti d'un fil télégraphique qui circonscrivait la ville. L'Empereur d'Allemagne a dit que sans le télégraphe il n'eût pas été possible de faire aboutir le siège. La ligne télégraphique circulaire dont nous parlons ne servait pas seulement à relier les corps de troupe échelonnés autour de Paris ; elle servait encore à assurer l'approvisionnement des armées allemandes.

Autres péripéties et faits divers des débuts du télégraphe électrique.

En 1801, la nouvelle de la mort de l'empereur de Russie, Paul I^{er} (12 mars 1801, mit vingt et un jours à arriver à Londres, par les courriers.

La nouvelle de la mort de l'empereur de Russie, Nicolas, en 1855, parvint à Londres en quatre heures et quart, par le télégraphe électrique.

Autres exemples historiques :

La bataille de Fontenoy, gagnée sur les Anglais par Louis XV et le maréchal de Saxe, fut livrée le 11 mai 1745 ; la nouvelle n'en fut connue à Paris, et annoncée par la *Gazette de France*, que le 15 mai suivant, c'est-à-dire quatre jours après. Ainsi, en 1745, il fallait quatre jours pour connaître le résultat d'une bataille importante livrée à Fontenoy, éloigné seulement de Paris d'environ 75 lieues.

La nouvelle de la bataille d'Austerlitz, livrée le 2 décembre 1805, ne parut au *Moniteur* que le 12 décembre suivant ; elle fut apportée par le colonel Lebrun, aide de camp de l'empereur Napoléon I^{er}. Austerlitz est à environ 400 lieues de Paris.

La prise d'Alger eut lieu le 5 juillet 1830, la nouvelle n'en fut connue à Paris que le 13 juillet au soir.

Après l'avènement du télégraphe électrique :

Le discours prononcé par l'Empereur des Français, le 18 janvier 1858, pour l'ouverture de la session législative, fut transmis de Paris à Alger, en deux heures. Expédié dans la soirée du 18, il était affiché le 19 au matin dans les rues d'Alger.

Pendant la guerre de Crimée, en 1855, au moment du siège de Sébastopol, une dépêche pouvait être transmise en treize heures, du camp français, à Paris, grâce au fil télégraphique qui s'étendait de Paris en

Crimée. Ce fil n'interrompait son cours qu'à divers intervalles, qui, réunis, pouvaient être franchis en douze heures par des courriers. La distance était de 900 lieues (environ 3600 km).

Les communications de l'Angleterre avec l'Inde, nous fournissent un autre exemple comparatif, tout aussi frappant, du progrès qu'a fait dans ce siècle, la rapidité des communications.

Pour recevoir des nouvelles de leurs possessions dans l'Inde, les Anglais étaient contraints, au commencement de ce siècle, d'attendre l'arrivée des bâtiments, qui mettaient cinq mois à ce trajet. Plus tard, par l'établissement des services des malles de l'Inde et du chemin de fer, les communications ont pu se faire, entre l'Angleterre et l'Inde, en deux mois.

En 1858, grâce aux chemins de fer et aux quelques lignes télégraphiques disséminées eu Orient, qui se rattachaient à celles de l'Europe, on recevait, dans la Cité de Londres, en vingt-cinq jours, des nouvelles de l'Inde, éloignée d'environ 5.000 lieues (20.000 km).

Dès 1865, la ligne télégraphique fonctionnait sans aucune solution de continuité, et l'on recevait des dépêches télégraphiques en dix heures !

Si maintenant nous voulions pousser ces comparaisons au-delà de toute espèce de terme, nous n'aurions qu'à citer le prodigieux tour de force que réalise souvent le câble transatlantique[21] de Valentia (Irlande), à Terre-Neuve et à New York. On sait que, par suite de la différence des longitudes, une dépêche expédiée de Londres par le télégraphe sous-marin, qui part de Valentia, arrive en Amérique avant l'heure de son départ d'Europe ! En voici un curieux exemple. Au mois de mars 1867, une dépêche annonçant cours de la bourse de Londres arriva et fut affichée à New York à midi. Or, cette dépêche était partie de Londres, le même jour, à la clôture de la bourse, c'est-à-dire à 16 heures ! La dépêche était donc arrivée avant d'être partie !

Les astronomes et les géographes utilisèrent le télégraphe électrique pour affiner leurs mesures. La longitude d'un lieu n'étant autre chose que le moment où le soleil passe au méridien de chaque lieu, le télégraphe électrique fournit un moyen, idéal pour ainsi dire, de fixer le moment de ce passage. Il suffit que deux observateurs placés à ces deux points, observent au même instant, l'heure d'un bon chronomètre. Le signal du moment où il faut noter l'heure de l'horloge, est donné à ces deux observateurs, par le télégraphe électrique.

Le télégraphe électrique était à peine établi aux États-Unis, qu'il servait, sous la direction de M. Morse, à déterminer la différence de longitude entre Washington et Baltimore. Un signal télégraphique permit à deux personnes en station, l'une à Washington, l'autre à Baltimore, de comparer au même instant, deux horloges mises respectivement à l'heure exacte de chacune de ces villes.

Le même moyen fut employé, au mois de mai 1854, par MM. Airy et Le Verrier, directeurs des observatoires de Greenwich et de Paris, pour déterminer la différence de longitude entre ces deux villes.

M. Le Verrier à cette même époque détermina par le télégraphe électrique la différence de longitude d'un grand nombre de lieux de la France.

En 1866, le câble transatlantique était à peine déposé au fond de l'Océan, que l'on se hâtait de mettre à profit ce fil magique pour déterminer la différence, de longitude entre New York et Greenwich, entre Washington et Londres, etc.

Le télégraphe électrique a permis d'établir, en Angleterre, en France et dans quelques autres contrées de l'Europe, un service d'observations météorologiques, vraiment universelles.

En 1850, le télégraphe électrique de Chicago signala aux patrons de navires des ports de Cleveland et de Buffalo, ainsi qu'aux navires qui parcouraient le lac Ontario, l'approche d'une tempête venant du nord-ouest. L'ouragan ne traverse l'atmosphère qu'avec une rapidité d'environ 25 lieues à l'heure ; il est donc facilement devancé par le télégraphe électrique. Un navire qui s'apprête à partir de New York pour la Nouvelle-Orléans, peut apprendre par ce moyen, vingt heures à l'avance, qu'une tempête règne dans le golfe du Mexique.

[21] Voir plus loin : *Le câble*.

Sur les chemins de fer, le télégraphe électrique est d'une utilité immense. Les services qu'il rend dans ce cas particulier, sont beaucoup plus étendus qu'on ne l'imagine. Pour la facilité du service, pour la sécurité de la voie, le télégraphe électrique était une annexe tout à fait indispensable, des voies ferrées.

En 1848, un convoi de chemin de fer avait apporté à Norwich la nouvelle de la chute du pont suspendu de Yarmouth. Qu'on juge de l'inquiétude et de l'effroi des habitants : ils avaient presque tous leurs enfants en pension à Yarmouth ! Ils coururent en foule à la station du chemin de fer, demandant à grands cris des nouvelles de leurs enfants : « *Tous les enfants sont sauvés !* » dit le télégraphe électrique.

Au mois d'octobre 1846, un déserteur du vaisseau américain la Pensylvanie, en rade à Norfolk, emporta au comptable du navire une somme de 3.000 francs, et prit, avec le produit de ce vol, le chemin de fer de Baltimore. Le fait reconnu, le comptable se rendit en toute hâte à la station télégraphique de Washington, et fit transmettre à Baltimore le signalement du coupable, avec ordre de l'arrêter. Dix minutes après, la police de Baltimore tenait entre ses mains l'ordre d'arrestation, et au bout d'une demi-heure arrivait à Washington la dépêche suivante : « *Le déserteur est arrêté, il est en prison ; que faut-il en faire ?* »

On a vu plusieurs fois, en Amérique et en Angleterre, deux amateurs d'échecs, placés à cinquante lieues de distance, faire leur partie par le télégraphe, aussi facilement que s'ils étaient en face l'un de l'autre.

Un mariage fut célébré en 1846, par l'intermédiaire du télégraphe électrique, entre deux personnes dont l'une habitait Boston et l'autre Baltimore, et qui trouvèrent commode d'arranger, sans se déplacer, cette petite affaire. Mais la validité d'un tel mariage devint, à bon droit, la cause d'un procès.

Pendant la célébration d'une messe de mariage dans une paroisse d'Angleterre, l'une des demoiselles d'honneur de la mariée s'esquiva de l'église, et disparut avec l'un de ses admirateurs. Le télégraphe électrique fut aussitôt mis en réquisition sur toutes les lignes de chemin de fer, pour donner l'ordre d'arrêter les fugitifs, fortement soupçonnés d'aller invoquer l'assistance du forgeron de Gretna-Green. Le télégraphe ne fonctionna que trop bien, car, en même temps que les coupables étaient rejoints, quatre couples de jeunes époux, très légitimement unis dans la matinée, se trouvaient arrêtés sur d'autres points de la même ligne, et voyaient leurs excursions matrimoniales désagréablement suspendues par l'intervention de la police.

Le télégraphe électrique a été mis quelquefois au service de la médecine. Le malade et le médecin étaient installés chacun à l'une des stations ; le malade transmettait les symptômes de son mal, et le docteur donnait la réplique, par l'envoi de son ordonnance. On lisait ce qui suit, dans un journal américain :

« *Hier, avant midi, un monsieur entra dans le cabinet du télégraphe, à Buffalo, et témoigna le désir de consulter le docteur Steven, résidant à Lockport. Prévenu de ce désir, le docteur se rendit au cabinet électrique de Lockport. Le monsieur lui annonça alors que sa femme était gravement malade, et lui fit connaître les symptômes caractéristiques de la maladie. Le médecin indiqua les remèdes à employer. Tous deux convinrent ensuite, si la malade n'allait pas mieux, de se retrouver le lendemain matin aux extrémités de la ligne télégraphique. Le lendemain, le monsieur ne parut point. Sans doute, la consultation avait amené une guérison subite.* »

Ou bien encore, osons-nous ajouter, la malade était morte, en dépit de la consultation électrique…

En France, en Allemagne, en Italie, en Suisse, etc., une autre habitude se généralise. Chaque touriste a soin, avant d'arriver dans une ville, de retenir une chambre dans un hôtel à sa convenance, au moyen d'une dépêche électrique, expédiée de la gare d'une station du chemin de fer. Les voyageurs peu avisés ou trop économes, sont ainsi devancés, et regrettent souvent, en arrivant dans la ville et trouvant toutes les chambres occupées, de n'avoir pas fait usage du télégraphe.

Le 1er janvier 1850, le télégraphe électrique prévint en Angleterre, une grave catastrophe de chemin de fer. Un train vide s'étant choqué à Gravesend, le conducteur fut jeté hors de la machine, et celle-ci continua à courir seule et à toute vapeur vers Londres. Avis fut immédiatement donné par le télégraphe à Londres et aux stations intermédiaires ; ensuite, le directeur s'élança sur la ligne, avec une autre machine,

à la poursuite de l'échappée ; il l'atteignit et manœuvra de manière à la laisser passer ; puis il se mit en chasse après elle. Le conducteur de la machine réussit enfin à s'emparer de la fugitive et tout danger disparut. Onze stations avaient déjà été traversées, et la locomotive n'était plus qu'à deux milles de Londres quand on l'arrêta. Si l'on n'avait pas été prévenu de l'événement, le dommage causé par la locomotive aurait surpassé la dépense de toute la ligne télégraphique. Ainsi, le télégraphe paya, ce jour-là, le prix de son installation.

Un second fait du même genre arriva, pendant la même année, sur le chemin de fer de Londres au Nord-Ouest. Par un de ces jours sombres et brumeux si communs en Angleterre, une locomotive abandonnée par mégarde à elle-même, prit tout à coup son essor et s'élança en pleine vapeur, avec une vitesse effrayante, vers la gare d'Easton. Tous ceux qui la virent s'échapper sans guide, sur un chemin parcouru par de nombreux convois, s'attendaient à des accidents terribles. Mais le télégraphe électrique eut bientôt dépassé la fugitive, et en quelques minutes l'événement était transmis à la station de Camden. On eut le temps de tourner les aiguilles de manière à diriger la locomotive égarée sur une voie latérale, où elle ne rencontra que quelques wagons de charge qui arrêtèrent sa course désordonnée.

Le 22 décembre 1854 il se passa sur le chemin de fer de Rion à Dax, dans le département des Landes, un épisode des plus émouvants. Dans un wagon occupé par plusieurs voyageurs, se trouvait une dame des environs de Dax, avec sa fille, âgée d'environ trois ans. Celle-ci, dans un brusque mouvement, se jette contre la portière qui s'ouvre et l'enfant tombe sur la voie. La mère, éperdue, veut se précipiter après sa fille ; mais les voyageurs la retiennent, et joignent leurs cris à ceux de cette infortunée, pour faire arrêter le train. Malheureusement, ces cris ne sont pas entendus, et l'on arrive à la gare de Dax, où se trouvait le père de la petite fille, attendant la venue du convoi. On juge de la poignante scène qui se passa entre cette mère éplorée et son mari.

Mais déjà le télégraphe électrique avait signalé l'événement sur la ligne, et arrêté à Rion, un nouveau convoi qui se mettait en route. Une locomotive de secours est expédiée, de la gare de Dax, sur le lieu de l'accident. En approchant de l'endroit désigné, la locomotive ralentit sa marche, et bientôt les éclaireurs aperçoivent la petite fille endormie sur la voie, la tête appuyée sur un rail. Elle est aussitôt recueillie, et la locomotive revient à toute vitesse à son point de départ. L'enfant, à son arrivée, se jette dans les bras de sa mère, et après l'avoir couverte de baisers, lui dit : « *J'ai faim, maman, donne-moi du pain !* »

Les journaux anglais ont raconté avec beaucoup de détails le fait suivant, qui produisit à Londres une vive sensation, et qui fournit une preuve éclatante de l'utilité du télégraphe électrique :

Au mois de janvier 1844, un horrible assassinat fut commis à Salthill. L'assassin, nommé John Tawell, s'étant rendu précipitamment à Slough, y prit une place pour Londres, dans le train du chemin de fer qui passait, à cette station, à 7 heures 42 minutes du soir. La police, avertie du crime, était déjà à sa poursuite. Elle arriva à Slough, sur les traces du coupable, presque au moment où le convoi du chemin de fer devait entrer dans Londres. Mais le télégraphe électrique fonctionnait, et pendant que le meurtrier, confiant dans la vitesse extraordinaire du convoi, se croyait en sûreté parfaite, le message suivant volait sur les fils du télégraphe :

« *Un assassinat vient d'être commis â Salthill. On a vu celui qu'on suppose être l'assassin prendre un billet de première classe pour Londres, par le train qui a quitté Slough à 7 heures 42 minutes du soir. Il est vêtu en quaker avec une redingote brune qui lui descend presque sur les talons. Il est dans le dernier compartiment de la seconde voiture de première classe.* »

Arrivé à Londres, John Tawell se hâta de monter dans l'un des omnibus du chemin de fer. Blotti dans un coin de la voiture, il se croyait dès ce moment à l'abri de toutes les atteintes de la justice. Cependant, le conducteur de l'omnibus, qui n'était autre chose qu'un agent de police déguisé, ne le perdait pas de vue, sûr de tenir son homme, comme un rat dans une souricière. Parvenu dans le quartier de la Banque, John Tawell descendit de l'omnibus, se dirigea vers la statue du duc de Wellington et traversa le pont de Londres ; il entra ensuite au café de Léopard, dans le Borough, et se retira enfin dans une taverne du

voisinage. L'agent de police qui, attaché à ses pas, l'avait suivi dans toutes ses évolutions, entra après lui, et tenant la porte entr'ouverte, lui demanda d'un ton calme : « *N'êtes-vous pas arrivé tout à l'heure, de Slough ?* »

À cette question si effrayante pour le coupable, John TaweIl se troubla, et balbutia un non, qui était l'aveu de son crime. Arrêté aussitôt, il fut mis en jugement, condamné comme assassin et pendu.

À quelques mois de là, dit le journal *The Family Library*, nous faisions le trajet de Londres à Slough, par le chemin de fer, dans une voiture remplie de personnes étrangères les unes aux autres. Tout le monde gardait le silence, comme c'est assez généralement l'usage des voyageurs anglais. Nous avions déjà parcouru près de quinze milles sans qu'un seul mot eût été prononcé, lorsqu'un petit monsieur, à la taille épaisse, au cou court, à l'air d'ailleurs très respectable, qui était assis à l'un des coins de la voiture, fixant les yeux sur les poteaux et les fils du télégraphe électrique, qui semblait voler dans un sens opposé au nôtre, murmura tout haut, en accompagnant son observation d'un mouvement de tête :

« V*oilà les cordes qui ont pendu Jo Tawell !* »

Pour conclure, l'utilité du télégraphe et le besoin d'une communication rapide n'étant plus à démontrer de nos jours voici ce que disait[22] Alfred Marshall (1842-1924), économiste britannique :

« *Les préoccupations de plus en plus graves de notre époque, les progrès de l'intelligence dans la masse populaire,* les progrès du télégraphe*, de la presse, et des autres moyens de communication tendent à élargir toujours le champ de l'action collective inspirée par le bien public. Ces transformations, auxquelles il faut ajouter l'essor du mouvement coopératif, et des autres formes de l'association volontaire, sont dues à l'influence de divers mobiles autres que celui du bénéfice pécuniaire. Elles offrent sans cesse à l'économiste de nouvelles occasions de mesurer des mobiles dont il avait paru jusqu'alors impossible de ramener l'action à une loi quelconque.* »

Et encore : « *De même que dans les temps anciens les instruments les plus coûteux étaient les bateaux, et dans certains cas les canaux de navigation et d'irrigation, de même, à l'heure actuelle, ce sont* les moyens de communication *au sens général : chemins de fer et tramways, canaux, docks et bateaux,* télégraphes et téléphones… ».

Enfin, parlant des échanges de titres boursiers : « *Mais le cas le plus remarquable, c'est celui que nous offrent les titres appelés « internationaux" parce qu'ils sont demandés sur tous les points du globe. Ce sont les obligations des principaux gouvernements et de quelques compagnies publiques très importantes, telles que celles du Canal de Suez et du New York Central Railway. Pour les valeurs de cette classe, le télégraphe maintient les prix à peu près au même niveau dans toutes les Bourses du monde. Si le prix de l'une d'elles s'élève à New York ou à Paris, à Londres ou à Berlin, la simple nouvelle de la hausse tend à provoquer la hausse sur d'autres marchés, et si pour quelque raison la hausse ne se produit pas immédiatement, il est probable que cette classe particulière de valeurs sera bientôt mise en vente sur le marché où la hausse s'est produite, à la suite d'*ordres télégraphiques *parvenus des autres marchés ; tandis que, d'un autre côté, les spéculateurs du premier marché feront par télégraphe des achats sur d'autres places.* »

[22] *Principes d'économie politique*, Tome II.

Le câble sous-marin.

Comme nous venons de le voir, le télégraphe électrique allait prendre une importance grandissante et un développement fulgurant. Aussi, dès 1839, en Inde, on chercha à traverser les eaux. En effet, nous n'avions pour l'instant vu que des lignes aériennes courant le long de poteaux et accrochées à des isolateurs. Le problème avec l'eau, qui comme chacun sait est plus ou moins conductrice de l'électricité, c'est que l'on risquait d'avoir une déperdition importante du signal électrique.

Il fallait donc, dans un premier temps, trouver un isolant capable résister en particulier aux sels marins. Le caoutchouc naturel ne se montra pas satisfaisant à ce point de vue et son prix élevé était une entrave supplémentaire à son utilisation.

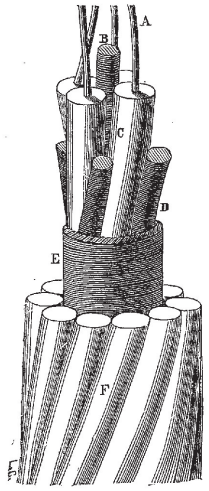
Ce n'est qu'en 1849 que M. Walker, physicien anglais, eut l'idée d'utiliser les propriétés isolantes et de grande résistance à l'eau de mer de la *gutta-percha*.

La gutta-percha est un suc végétal issu, à la manière du caoutchouc, de l'*Isonandra gutta*, arbre fort répandu de Malaisie et de toute l'Océanie. Cette matière se travaille un peu comme le caoutchouc et peut aussi se vulcaniser[23] comme ce dernier.

Ce fut M. Jacob Brett qui obtint du gouvernement français, par un décret du 10 août 1849, d'établir et d'exploiter pour 10 ans, une ligne de télégraphe électrique entre Calais et Douvres.

On fabriqua à cet effet un fil de cuivre d'une longueur de 45 kilomètres recouvert d'une enveloppe de 6 millimètres et demi de gutta-percha. Les points choisis pour l'immersion du fil étaient : la côte de Douvres en Angleterre, et en France, le cap Gris-Nez. *Le Goliath*, bateau à vapeur anglais fut chargé de l'opération d'immersion du câble qui commença le 28 août 1850 en partant de Douvres. Le câble était lesté par des poids en plomb. La profondeur d'immersion variait de 10 à 75 mètres. Pendant les opérations, le câble était entretenu en communication constante avec la station de Douvres afin d'indiquer les phases successives d'immersion.

À huit heures du soir, une dépêche partie du cap Gris-Nez annonçait la bonne fin de l'opération. Hélas, quelques heures après, le télégraphe resta muet. En fait, le câble était sectionné près des côtes françaises, là où se trouvent des écueils et des rochers constamment battus par les vagues. On avait cru que le tube de plomb qui enveloppait le fil le préserverait suffisamment des chocs. Une autre explication à cette rupture fut avancée : un pêcheur, le prenant pour une algue gigantesque (?) l'aurait coupé et rapporté à Boulogne comme trophée d'une plante marine des plus rares !



Il fallait donc trouver un moyen plus efficace pour protéger le fil sous-marin. M. Küper eut alors l'excellente idée de l'entourer d'un cordage en fil de fer. On obtint ainsi un câble souple et résistant dont nous donnons l'illustration ici. Quatre fils A de 1,5 mm de diamètre contenus dans une gaine de gutta-percha C de 7 mm de diamètre, entrelacés avec quatre cordes de chanvre D. Le tout était aggloméré par un mélange de goudron et de suif formant un cordon d'environ trois centimètres de diamètre. Une seconde corde de chanvre E enveloppait ce cordon et le tout était fortement serré au moyen d'un fil de fer galvanisé de 8 mm de diamètre.

MM. Wollaston et Crampton furent les deux ingénieurs en charge d'exécuter la nouvelle installation du câble sous-marin entre Sangatte et cap Southerland près de Douvres. L'opération débuta le 25 décembre au petit jour à bord du *Blazer*. Dans la soirée, le câble reposait au fond de la Manche… mais on avait mal calculé la longueur et il s'arrêtait à 1 km des côtes françaises ! Le lendemain, on raccorda un petit câble provisoire et les dépêches transitèrent sans problème.

[23] La vulcanisation consiste à ajouter, à chaud, du souffre, ce qui modifie les propriétés de la gutta-percha en la rendant rigide et inaltérable par la chaleur.

Après réparation définitive, on inaugura le câble le 31 décembre 1851. Ce jour-là, le courant électrique parti du rivage français vint mettre de feu à un canon placé sur le rempart de Douvres.

Les principales dates de l'installation de câbles sous-marins :
1852 : Holyhead (Angleterre) – Howth (baie de Dublin) Irlande
1853 : Douvres-Ostende
1854 : Varna (Turquie) – Balaclava (près de Sébastopol) Crimée
1855 : Sicile – Italie
1856 : Allemagne – Suisse à travers le lac de Constance
1857 : Malte – Corfou
1858 : L'île de Ceylan – Inde
1859 : L'île de Candie (Smyrne) – Chio et Dardanelles
1860 : Espagne –Baléares et France – Algérie

Le câble transatlantique.

L'idée en revient à M. Gisborne, ingénieur anglais dès 1852. Après avoir établi un câble dans le golfe du St. Laurent, M. Gisborne partit pour New York, début 1854, espérant trouver les fonds nécessaires à cette entreprise.

Il y rencontra un riche capitaliste, M. Cyrus Field qui accepta de le suivre dans cette aventure. Pour connaître des possibilités techniques de cette réalisation extraordinaire, ils s'adressèrent à M. Maury, directeur de l'Observatoire national des États-Unis et au professeur Morse. Ces deux savants ayant donné des réponses positives, M. Field se mit en campagne pour constituer une société financière. Le 7 mars 1854 fut formée la *Compagnie transatlantique*.

La fabrication du câble débuta en 1857. La distance séparant Valentia, sur la côte ouest de l'Irlande de Saint-Jean (Terre-Neuve) est, en ligne droite, de 3.100 km. Compte tenu des probabilités de déviation lors de la pose, on décida de fabriquer un câble de 4.100 km de longueur totale. Avant d'immerger le câble, on fit un test d'isolement et de conductibilité, test qui s'avéra positif.

Le 7 août 1857, les opérations commencèrent. Le 12 août le câble se rompit suite à l'action de forts courants sous-marins dont on n'avait pas soupçonné l'existence. Le *Niagara*, navire de pose du câble était alors à 508 km de l'Irlande avec des fonds de 3.240 m sous la quille… 541 km de câble étaient déjà immergés. On renonça à poursuivre l'entreprise, mais on ne se découragea pas.

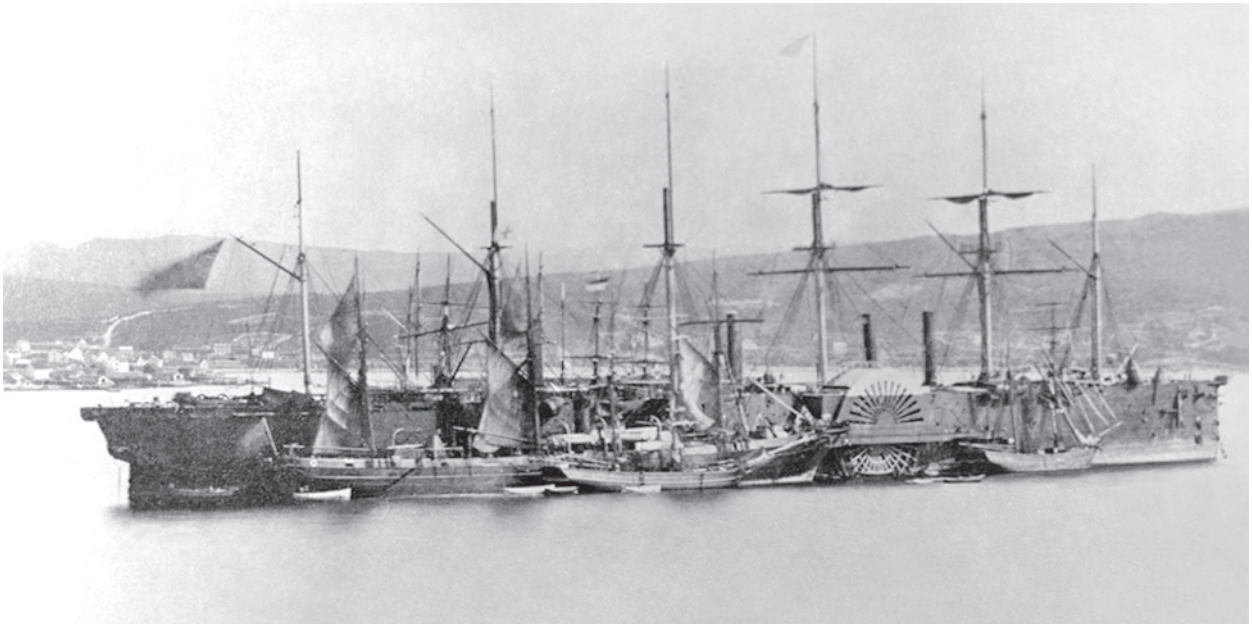
Le jeudi 10 juin 1858, on commença une nouvelle expédition. Grâce à un temps d'une sérénité et d'un calme inaltérable, le *Niagara* ne mit que 6 jours et demi pour remplir sa mission. Le 5 août 1858, la communication électrique entre l'Europe et l'Amérique était établie. Le 18 août, M. Cyrus Field envoya cette dépêche : « *L'Europe et l'Amérique sont unies par une communication télégraphique. Gloire à Dieu au plus haut des cieux, sur la terre paix et bienveillance envers les hommes* ».

Malheureusement, dès les premiers jours les signaux présentèrent des irrégularités et le 5 septembre les communications étaient entièrement suspendues.

En avril 1860 on repêcha environ 8 km du câble. L'armature était complètement rongée, mais le cœur du câble était en parfait état. En étudiant et en expérimentant la composition du câble, on se rendit compte qu'il se comportait comme un véritable condensateur (bouteille de Leyde à l'époque) par induction entre le cœur du câble et son enveloppe.

La solution fut trouvée par l'ingénieur Witehouse qui, pour ainsi dire, inventa le courant alternatif en inversant les polarités alternativement dans le câble. Pour parer aux inconvénients des courants induits, il fallait faire circuler dans le câble des courants faibles, et c'est grâce à l'invention de M. Thomson (*galvanomètre de Thomson*) que l'on put détecter ces courants de faible intensité.

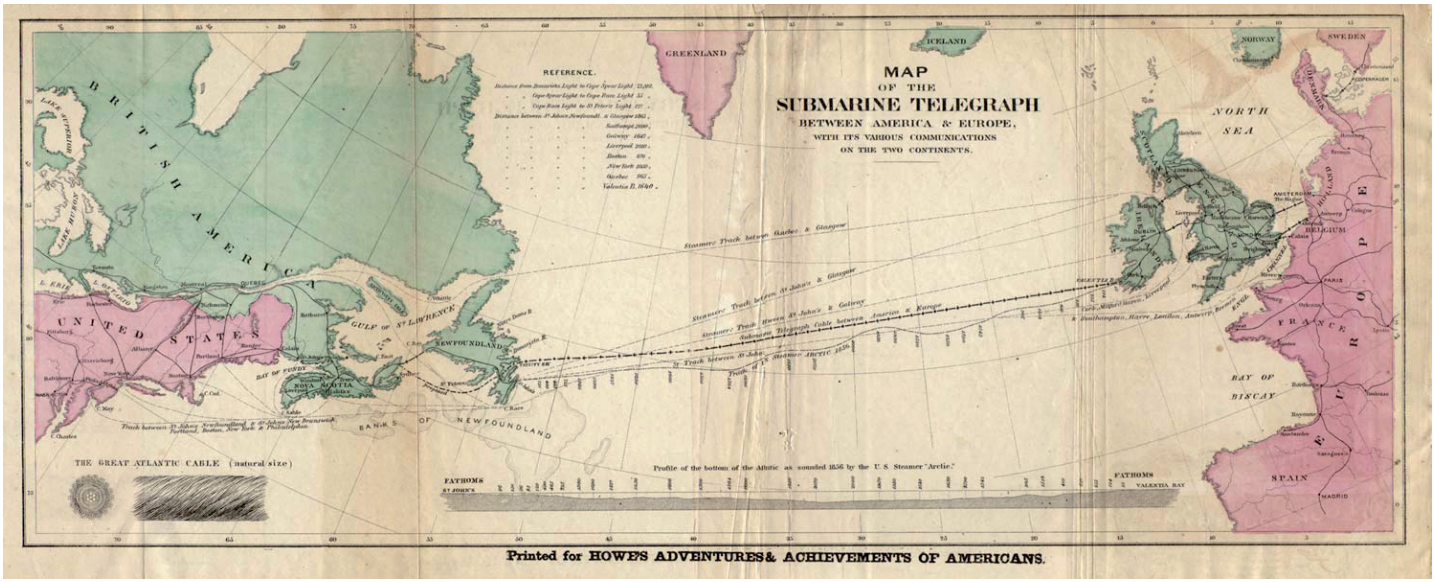
Une troisième tentative eut lieu en 1865 avec un nouveau câble et, le 15 juin de cette année, le *Great-Eastern*[24] était paré.



La pose de ce nouveau câble fut émaillée de nombreux incidents. On contrôlait en permanence la continuité du circuit, et à plusieurs reprises, on devait constater des coupures. À chaque fois, on repêcha le câble qui venait d'être immergé et on constata le même problème : un morceau de fil de fer traversait de part en part le câble qui était coupé ou percé volontairement. Le câble finit par se rompre le 2 août par 3.700 mètres de fond. Jusqu'au 12 août, les ingénieurs et mécaniciens du Great-Eastern firent de

[24] Le *Great Eastern* fut un bateau imaginé par Isambard Kingdom Brunel. Il fut le plus grand navire jamais construit à son époque, avec une capacité d'embarquement de 4 000 passagers sans qu'il soit nécessaire de le réapprovisionner entre la Grande-Bretagne et la côte est des États-Unis. Il fut le premier paquebot géant. Le navire fut construit en partenariat avec l'un des principaux constructeurs de son temps, John Scott Russell, sur les bords de la Tamise, dans les chantiers navals de Millwall, situés en aval du « London bridge » à Londres. Russell était cependant en grandes difficultés financières, ce que ne savait pas Brunel, et qui occasionnerait de nombreux retards. Ce fut le dernier grand projet de Brunel, qui eut un malaise sur le pont du navire et mourut quelques jours plus tard.
Le navire fut lancé en 1858, après de nombreuses difficultés techniques (après un premier lancement raté, il fut remis à l'eau 3 mois plus tard). Il mesurait 211 mètres (692 pieds) de long, 25 mètres (83 pieds) de large, 18 mètres (60 pieds) de haut. Le tirant d'eau était de 6,1 mètres (20 pieds) à lège et 9,1 mètres (30 pieds) à pleine charge, pour un poids de 32 000 tonnes. En comparaison, le *Persia*, lancé en 1856, mesurait 119 mètres (390 pieds) de long et 14 mètres (45 pieds) de large.
La coque fut entièrement construite en tôle d'acier de 19 mm, avec une double coque. À l'intérieur, le navire était divisé en deux compartiments de 107 mètres (350 pieds) de long et de 18 mètres (60 pieds) de haut, différentes cloisons les divisant alors en 19 compartiments plus petits. La propulsion se faisait par roue à aubes (17 mètres de diamètre) et par hélice (7,3 mètres de diamètre). Quatre moteurs à vapeur actionnaient les roues à aubes, et un autre l'hélice. La puissance totale était estimée à 8,000 hp (6 MW). Fin 1858, afin d'éviter une banqueroute causée par les coûts de construction et le surcoût du lancement raté, la Eastern Steam Navigation Company, propriétaire du Great Eastern le revend à la Great Ship Company pour la somme de £160,000. La Great Ship Company décide d'exploiter le navire sur l'Atlantique Nord et espère transporter entre 4000 et 5000 personnes à chaque traversée. Le 17 juin 1860 le Great Eastern appareille de Southampton en direction de New York. Il ne transporte que 43 passagers dont 8 invités. Au retour, seuls 200 billets ont été vendus. Le navire roule affreusement et supporte mal le gros temps ce qui rend la traversée très inconfortable. Le Great Eastern ne fera que 12 voyages en 4 ans, sans jamais faire le plein de passagers, et ponctués de nombreux incidents et accidents qui coûteront cher à la Great Ship Company. Finalement la compagnie est mise ne faillite en 1863 et le navire est désarmé. Le Great Eastern est alors vendu pour £25,000 (son coût de construction avait été de £500,000), et utilisé comme câblier. Il fut notamment utilisé en 1865 pour poser les 4 200 km (2 600 miles) du câble télégraphique transatlantique, ainsi qu'à diverses autres poses de câbles jusqu'à son démantèlement en 1889. À cette occasion, les dépouilles de deux ouvriers furent découvertes. Ils avaient été enfermés vivants dans la double coque 30 ans plus tôt.

multiples tentatives pour repêcher le câble, mais à bout de chaînes et de cordages qui rompaient à chaque fois sous le poids de ce dernier, ils durent déclarer forfait. Ci-dessous, carte du premier câble



M. Cyrus Field rentra en Angleterre et fit construire un nouveau câble légèrement différent en ajoutant du *mastic Chaterton* à la gutta-percha afin de la rendre plus visqueuse et d'alléger aussi l'enveloppe isolante.

Ce fut encore le *Great-Eastern* qui fut chargé de l'opération, mais les hommes chargés des opérations furent sélectionnés sévèrement et leurs vêtements, sorte de camisoles boutonnées par l'arrière ne comportaient pas de poches qui permît d'y cacher de quoi saboter le câble. De plus, on leur fit signer un contrat comportant une clause draconienne : à la moindre tentative coupable, son auteur serait jeté par-dessus bord !

Au mois de juillet, le vendredi 13, le dévidage du nouveau câble commença. Le 27 juillet à 8 heures du matin, le Great-Eastern entrait dans le havre de Heart's-Content. L'opération était terminée. La longueur du câble déroulé était de 2.400 km.

Restait toujours sous les flots le câble de 1865. Comme au moment de sa rupture, on avait déposé une bouée à l'emplacement de l'accident, on s'enquit de le repêcher dans le but de le continuer afin de « doubler » la ligne. Repêcher un câble par 3.475 mètres de fond n'était pas une mince affaire.

Le 1er septembre, après de nombreuses difficultés, ce fut chose faite pourtant.

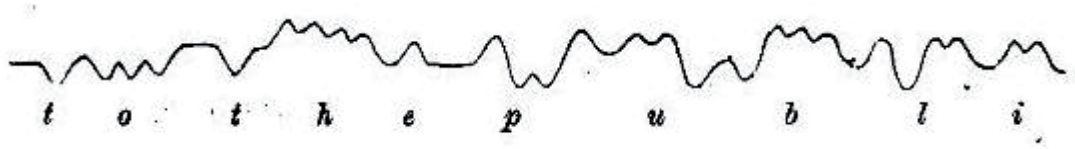
Le 8 septembre le câble de 1865 était complété et devenait le second lien télégraphique entre les deux continents.

Shakespeare qui faisait dire à Puck, le plus léger des sylphes : « *I will put a girdle round about the earth in forty minutes* » (*Je mettrai une ceinture autour de la terre en quarante minutes*) fut dépassé par cette nouveauté qui, si elle faisait le tour de la terre, mettrait moins d'une seconde à le parcourir.

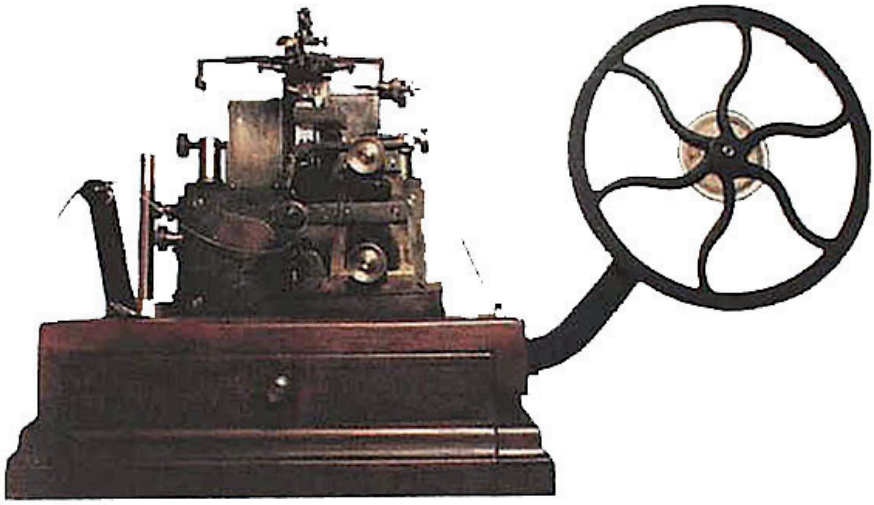
Il restait un petit problème à résoudre dans les transmissions par le câble sous-marin. De par sa constitution de son isolant (gutta-percha), on ne pouvait envoyer que des impulsions de faible intensité ne provoquant pas d'échauffement par effet de résistance. Or ces impulsions étaient trop faibles pour faire réagir les récepteurs Morses ou Hughes classiques. Ce fut sir William Thomson (lord Kelvin) qui trouva la solution. D'abord par l'utilisation d'un galvanomètre à miroir qui amplifiait de façon visuelle le faible déplacement de l'aiguille d'un galvanomètre très sensible. Mais ce procédé visuel était un retour en arrière technologique. Aussi il conçut ce qui fut la première imprimante à jet d'encre, appelé *siphon-*

recorder, constitué d'un tube capillaire et d'un galvanomètre à cadre mobile dont l'aiguille est remplacée par un siphon qui projette sur un ruban de papier une trace d'encre. Le trait obtenu indique les points Morse en se déplaçant vers un bord du ruban et les traits Morse en se déplaçant vers le bord opposé. Afin d'assurer le bon encrage, le moteur d'entraînement du papier actionne aussi une petite machine électrostatique qui électrise l'encre et en force l'écoulement.

Le signal délivré par cet appareil se présentait comme ceci :



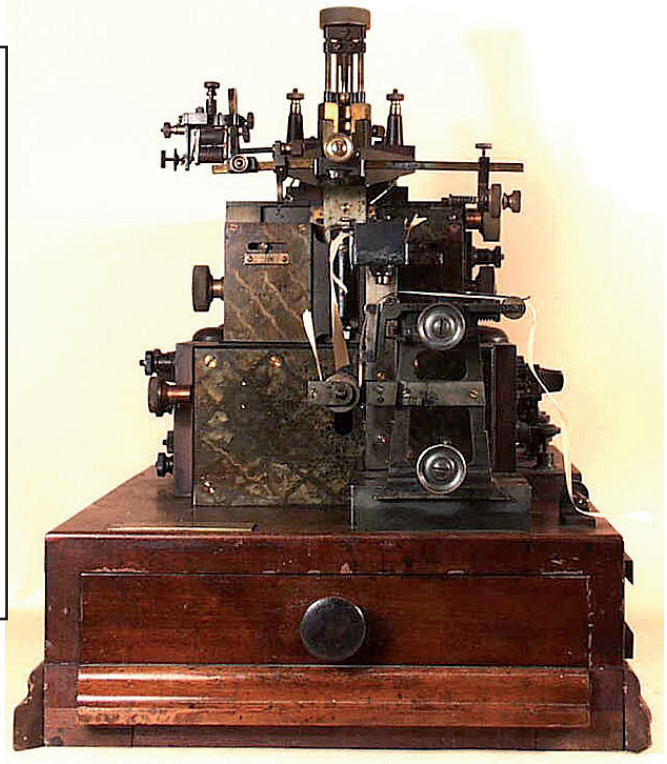
Ci-dessous l'appareil de réception Kelvin :

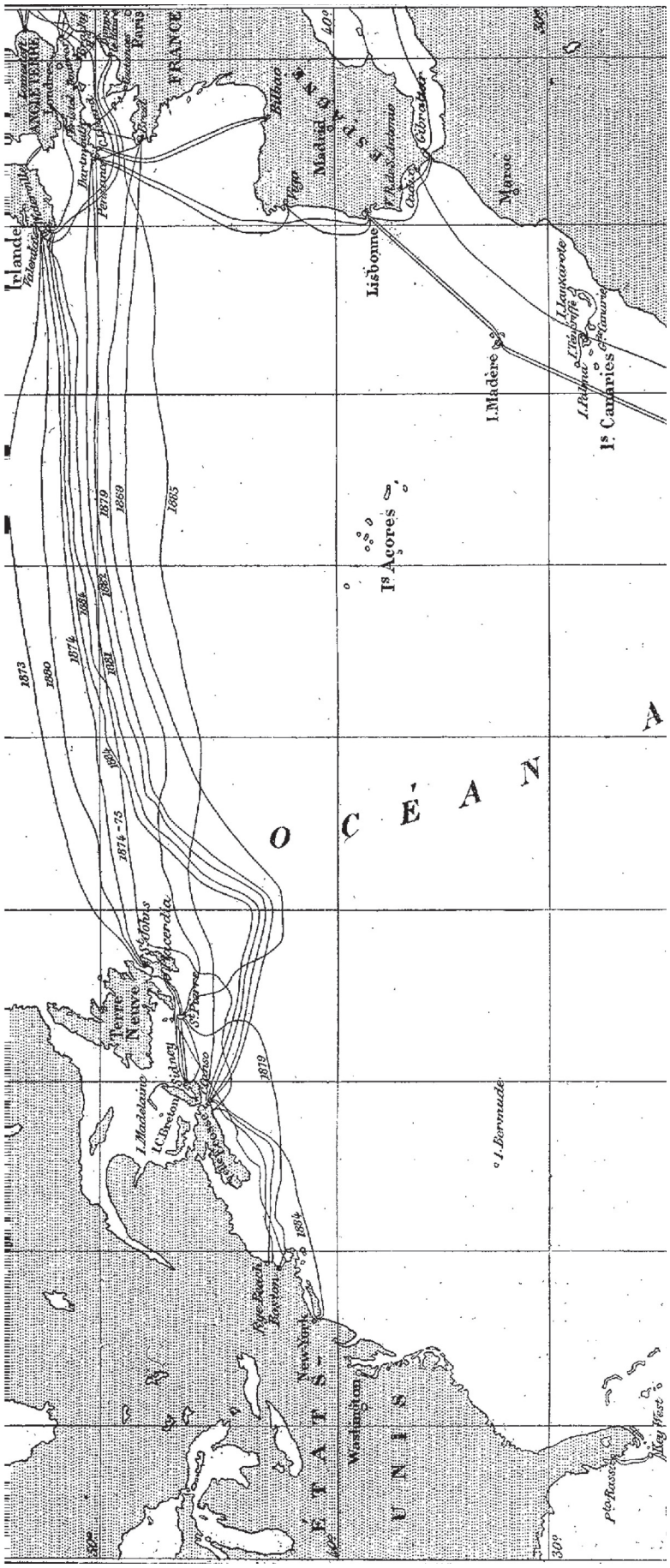


D'autres constructeurs ont encore modifié le *siphon-recorder* en remplaçant les électro-aimants qui provoquent le déplacement du cadre mobile, ou *bobine*, par de simples aimants de force suffisante.

Dans les années 1880, cet appareil est utilisé sur la ligne sous-marine de Marseille à Alger.

Enfin, en 1888, M. Brahsic a appliqué à cet appareil le perforateur Wheatstone en transmettant au moyen de bandes perforées, ce qui permit d'accroître notablement la vitesse des transmissions.





Carte géographique des câbles sous-marins reliant l'Angleterre et la France avec le continent américain. - (1890 environ) -

Nombre de dépêches passées par les câbles transatlantiques :

en 1860	550.000
en 1870	5.000.000
en 1880	15.000.000
en 1883	26.175.000

En 1889, il existait au total 950 câbles sous-marins, pour environ 200.000 kilomètres.

Le premier câble transatlantique français fut posé en 1869 entre Déolen (près de Brest) et Saint-Pierre et Miquelon.

Pour les liaisons téléphoniques, le premier câble transatlantique sera posé en 1956.

Ce n'est qu'en 1976 qu'un câble coaxial, avec des répéteurs immergés tous les 10 km, permit 400 communications simultanées.

Depuis 1986, les câbles sont en fibre optique et transmettent des signaux numériques. Le premier câble de cette nature a été posé en 1988 et autorisait 40.000 voies téléphoniques simultanées. Les répéteurs sont placés tous les 100 km.

En 1995 une nouvelle génération de câble à fibre optique autorise 500.000 voies simultanées.

Le téléphone, petite histoire et technique

Opératrices du téléphone, en France, dans les années 50.

Le téléphone.

Parler ici, être entendu là-bas, combler par le son de la voix des êtres aimés les distances et la séparation… Les traces que nous laissent les écrivains et les poètes concernent plus la conservation et la restitution des sons que leur transmission directe.

Un impossible rêve… et pourtant !

Héritier de la Renaissance, le jésuite orientaliste Athanasius Kircher (1601-1680) fut à l'origine de nombreux projets où l'utopie le disputait à l'imagination la plus échevelée.

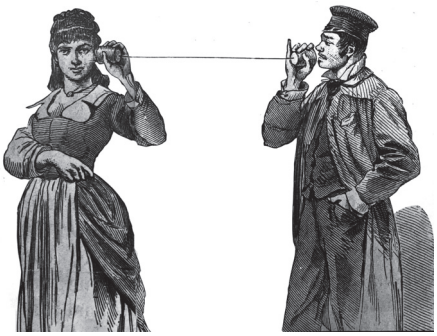
Parmi ceux-ci, cette *ellipsis otica* préfigurait le téléphone.

Il fallut deux siècles, et surtout la découverte de l'électricité, puis de l'électromagnétisme pour concrétiser ce rêve.

Selon des croyances immémoriales, certains éléments naturels, coquillages ou éponges, conservent les sons. À l'écoute des grondements confus qui sortent d'une conque marine, les Anciens pensaient que les bruits de la mer y étaient enfermés pour l'éternité.

Si l'on en croit Platon, par un hiver particulièrement rigoureux, les paroles gèlent et peuvent ainsi se conserver : « *Icy est le confin de la mer glaciale, sus laquelle feut, au commencement de l'hyver dernier passé, grosse et félonne bataille entre les Arismapiens et les Néphelibates. Lors gelèrent en l'air les paroles et crys des hommes et des femmes, les chaplis*[25] *des masses, les hurtys des harnois*[26]*, des bardes, des hennissements des chevaulx et tout aultre effroy de combat. A ceste heure, la riguer de l'hyver passée, advenante la sérénité et tempérie du bon temps, elles fondent et sont ouïes.* »

Dès le XVI[e] siècle, des récits de marins rapportent qu'à proximité du détroit de Magellan, d'étranges éponges retiennent le son et la voix articulée. Il suffirait ensuite de les presser pour prendre connaissance du message…



En 1667, un savant anglais, Robert Hooke, estime possible la diffusion à distance par voie acoustique : un simple fil tendu entre deux cornets permet aux sons de franchir plusieurs centaines de mètres.

Nous avons vu comment le religieux dominicain, dom Gauthey, sur une longueur de plus de 800 mètres, fit transiter le son de la voix par des tubes.

Un allemand, du nom de Huth, rédige en 1796 un traité sur « *l'usage du tube parlant en télégraphie* » qu'il nomme : *téléphone*.

S'il est couramment admis que l'invention du téléphone revient à Graham Bell, c'est surtout parce qu'il a été le premier à déposer un brevet le (14 février 1876 à Washington, le même jour qu'Elisha Gray[27]) et surtout parce qu'il proposait un système qui fonctionnait et était facilement industrialisable.

Il ne faut cependant pas méconnaître les travaux d'autres savants, travaux dont certains d'ailleurs aidèrent Graham Bell à développer son invention.

---

[25] Heurts.

[26] Les chocs des querelles.

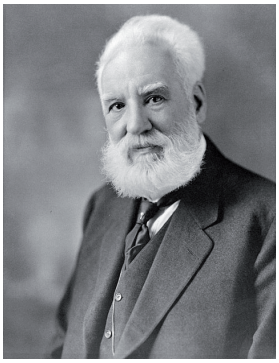
[27] Gray est l'inventeur, en 1876, du télégraphe musical, ancêtre du synthétiseur, basé sur l'oscillateur électrique. Le télégraphe musical est équipé d'un petit clavier et donne du son par le biais de haut-parleurs.

Dès 1837, le physicien américain Page avait reconnu que si un électroaimant est soumis à des aimantations et désaimantations très rapides, les vibrations transmises à l'atmosphère par le barreau aimanté émettent des sons. C'est ce que ce savant appelait la *musique galvanique*.

De 1847 à 1852, Mac Gauley, Wagner, Heef, Froment et Pétrina, combinèrent des vibrateurs électriques qui transportaient fort nettement les sons musicaux à distance. Toutefois, jusqu'en 1854, personne n'avait encore entrevu la possibilité de transmettre la parole, lorsqu'un simple employé du télégraphe, Charles Bourseul, publia une *Note* dans laquelle il imaginait un téléphone primitif. Malgré tous ses efforts, il se heurta au scepticisme général. Son appareil ne fut jamais réalisé, car l'Administration française y opposa une fin de non-recevoir, l'exploitation du télégraphe n'en étant qu'à ses balbutiements.

En 1860, le physicien allemand Philippe Reis construit un premier appareil basé sur la reproduction des sons entrevue par Page en 1837 et pour la transmission électrique, sur le système des membranes vibrantes qui avait été utilisé dès 1855 par Léon Scott, dans son *phonautographe*. L'appareil de Reis, perfectionné par MM. Yeates et Vander était composé d'un transmetteur qui se composait principalement d'un diaphragme fait d'une fine membrane à laquelle est fixé un fil de platine reposant sur une tête de platine réglable, et d'un récepteur. Le récepteur était une simple aiguille à tricoter en acier enroulée d'un fil de cuivre recouvert de soie, pour former un électroaimant, et posé dans une caisse de résonance.

L'idée du téléphone était clairement exposée, mais les savants de l'époque n'apportèrent pas leur soutien à ce génial inventeur, bien qu'un des plus célèbres vulgarisateurs de l'époque, Victor de Parville prophétisât : « *Bientôt on parlera à distance avec la même facilité. La parole se transmettra comme l'écriture* ».



Mais revenons à Graham Bell…

Graham Bell[28] était professeur à l'institution des sourds-muets de Boston. C'est dans le cadre de son activité qu'il étudiait toutes les possibilités de reproduction de la parole. Il dit un jour : « *J'ai fait parler des sourds-muets, je ferai parler le fer !* »

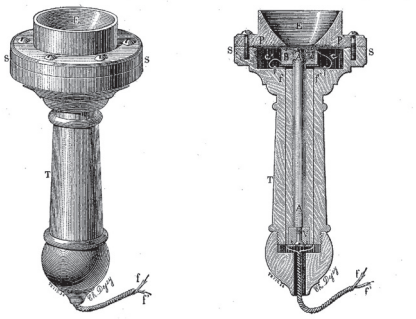
Notre savant professeur avait entendu parler des travaux de ses confrères[29] et en particulier de Meucci[30] et il conçut (officiellement…) le premier téléphone.

[28] M. Graham Bell s'est fait naturaliser américain et 1876, il était né à Édimbourg (Écosse).

[29] Elisha Gray fait déposer par son avocat, le 14 février 1876, un avis de brevet (*caveat*) au US Patent Office (bureau de la propriété intellectuelle américain) concernant l'invention du téléphone. Le même jour cependant, quelques heures plus tôt, Graham Bell dépose le brevet final de la même invention. S'ensuivent plusieurs procès sur l'attribution du brevet, procès que Gray a tous perdus, l'invention du téléphone étant finalement attribuée à Bell, avant toutefois de lui être retirée en juin 2002, la Chambre des représentants des États-Unis ayant statué qu'Antonio Meucci, qui avait déposé une demande de brevet en 1871, était le véritable inventeur du téléphone : Bell lui en avait volé la paternité.

[30] Antonio Meucci (né le 13 avril 1808 à San Frediano près de Florence en Italie, mort le 18 octobre 1896 aux États-Unis) est un inventeur italo-américain dont le rôle dans l'histoire du téléphone a été officiellement reconnue en 2001 par la Chambre des représentants des États-Unis : « *Expressing the sense of the House of Representatives to honor the life and achievements of 19th Century Italian-American inventor Antonio Meucci, and his work in the invention of the telephone.* »
Comment fut découvert le pot aux roses ? Tout débute en 1989. Basilio Catania, ancien directeur général de la CSELT (l'agence de recherche et de développement des télécoms italienne), découvre qu'Antonio Meucci, alors qu'il était ingénieur du théâtre à Florence, a mis au point une « *pipe téléphonique* ». Elle permet de communiquer entre des plateaux techniques distants d'une vingtaine de mètres. Catania poursuit son enquête.

Le téléphone de Graham Bell était un téléphone magnétique, en ce sens que ce sont les vibrations transmises à l'électroaimant qui produisent le courant reçu par le récepteur. Il n'y a donc pas de source extérieure d'électricité. Le courant produit étant somme toute assez faible, la portée d'un tel appareil était relativement limitée. Dès qu'il s'agit de transporter la voix à grande distance, l'invention primitive de Graham Bell était insuffisante, aussi de nombreux travaux furent entrepris pour augmenter la portée de l'appareil.



Ce fut Thomas Edison[31] qui eut l'idée d'employer une pile pour renforcer les ondulations sonores, et il construisit en 1876 le pre-

---

Le 1er mai 1850, après quinze ans passés à Cuba, Meucci débarque à New York. C'est là qu'il réalise une installation destinée à son épouse, paralysée par des crises d'arthrite. L'ingénieur a construit une machine capable de transporter le son entre son bureau et la chambre de sa femme. C'est le « *Télettrophone* ». Dix ans plus tard, il en fait une démonstration à son ami Enrico Bendelari. Un journal new-yorkais de langue italienne, L'*Eco d'Italia*, relate l'expérience et publie les détails de l'invention. Entre-temps, Meucci a été naturalisé.

Et il n'a cessé de déposer des brevets, quatorze en tout. Le 12 décembre 1871, il finit par fonder, avec trois associés, la *Telettrofono Company*, protégée le 28 décembre par un « avertissement de brevet », formule renouvelable, plus économique qu'un brevet.

Un an et demi plus tard, il propose une démonstration de son invention à Edward B. Grant, vice-président de la *Western Union Telegraph Company*, qui lui offre d'utiliser ses locaux et d'y entreposer son matériel. Grant demande aussi à examiner les plans. Une fois ceux-ci en sa possession, Grant repousse systématiquement la date de la démonstration. Au bout de deux ans, quand les associés réclament les plans et leurs appareils, il leur est répondu que tout a été perdu. On est en 1874, l'avertissement du brevet doit être renouvelé.

Mais les associés de la *Telettrofono Company* ne parviennent pas à réunir la somme nécessaire : à l'époque, Meucci dépend de l'aide publique pour vivre. Les droits et les protections vont automatiquement tomber. En mars 1876, Graham Bell dépose le brevet du téléphone. Or il travaillait dans le même laboratoire où Meucci avait entreposé ses appareils. Il dépose son brevet et expérimente son appareil à l'exposition internationale de Philadelphie en 1876. Puis vient le grand succès de Londres où il installe un téléphone à la Chambre des communes.

À Berlin, Siemens commence à fabriquer des téléphones. Meucci peut bien protester. La Western Union Telegraph Company (avec Thomas Edison comme conseiller technique) proteste aussi, mais les deux compagnies finissent par fusionner.

Il a fallu l'enquête de Catania pour mettre au jour les travaux d'une commission d'enquête dont l'attention avait été attirée par les plaintes de Meucci pour ententes illicites : il existait une connexion secrète entre des employés de l'office des brevets et la compagnie de Bell. Et celle-ci s'était engagée à rétrocéder à la Western Union 20 % des bénéfices de l'invention, le téléphone.

En 1896, la mort de Meucci enterre l'affaire. Cent cinquante ans après son arrivée à Manhattan, il aura finalement été réhabilité par un autre Américain d'ascendance italienne, Rudolph Giuliani, maire de New York, qui a fait du 1er mai 2000, le *Meucci Day*.

[31] « *Thomas*, fit durement le maître d'école, *vous ne serez jamais qu'un sot !* » Sous le poids de cette sombre prophétie, l'élève courba le front et pleura. Puis comme, au retour de la classe, ses larmes coulaient encore — grosses larmes intarissables d'un bambin de huit ans — sa mère l'interrogea. Au récit de l'enfant, blessée dans sa fierté maternelle, elle bondit jusque chez le maître d'école et lui cria : « *Monsieur, mon fils est moins sot que vous ! Désormais, instruit par mes soins, il se passera de vos leçons.* »

Cette scène avait lieu vers 1855, dans le petit bourg de Port-Huron (État de Michigan), où Thomas Alva Edison — né le 11 février 1847 à Milan (village de l'Ohio) — venait d'arriver avec les siens. À Port-Huron, certains se souviennent encore aujourd'hui de cette famille Edison : le père, assez peu entendu en affaires, mais réputé pour son « humour » ; la mère, originaire comme son mari du Canada, où elle avait été institutrice ; enfin Thomas, gamin bizarre, renfermé et étourdi, dont sa mère vantait l'intelligence docile, ouverte surtout aux choses scientifiques, mais que tout le village appelait un « bêta ».

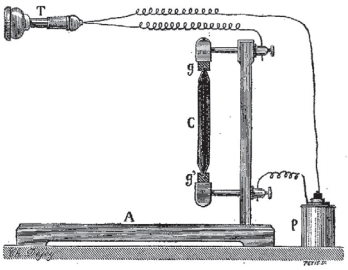
Ne le voyait-on pas sans cesse rôder parmi les chantiers et les quais et poser aux ouvriers mille questions oiseuses sur leur travail ou leurs outils ? « *A quoi sert ceci ? Comment démonte-t-on cela ?* »

Mais l'inventeur, chez Edison, ne devait pas tarder à s'annoncer. Il est alors à Boston où il assure, dans un bureau télégraphique, le service de nuit. Comme il a consacré le loisir de ses journées à lire et à étudier, notre veilleur est souvent pris, durant son service, d'invincibles assoupissements, dont les conséquences risquent d'être redoutables. « *Désormais,* lui dit alors son chef irrité, *vous me télégraphierez la lettre A toutes les demi-heures !* » « *Bien !* » répond le délinquant. Le lendemain, il a établi

mier téléphone à courant électrique. Graham Bell venait de trouver le principe du téléphone ; mais l'appareil était encore bien imparfait : « *On n'a jamais entendu, disait Edison lui-même, un bruit pareil à celui de cette vieille machine bourdonnante.* » Edison « tripota », suivant son expression, la vieille machine... Le professeur Rosanoff rapporta cette phrase de l'inventeur américain : « *Le téléphone n'est pas une invention, c'est une découverte ! Ne savez-vous pas comment le téléphone a été trouvé ? Un jour Bell tripotait des fils et des diaphragmes dans son laboratoire, quand soudain il entendit à travers le fil, la voix d'un assistant qui se trouvait dans une autre pièce. Le téléphone était là tout entier ; le reste était simple. Non, le téléphone n'a pas été une véritable invention, mais un accident. Quand vous faites une invention, vous découvrez d'abord une nécessité, puis vous cherchez les moyens à employer pour satisfaire cette nécessité. Or, jamais Bell n'a eu l'intention d'inventer le téléphone.* »

Thomas Edison en 1878

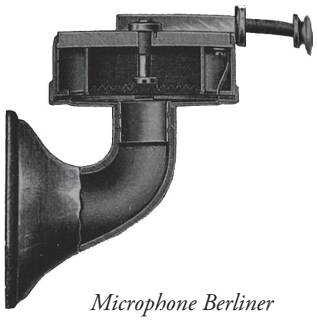
L'idée lui vint de combiner l'appareil de Bell avec le « microphone » récemment découvert par Hughes et surtout d'y joindre une bobine d'induction, grâce à laquelle les sons téléphonés furent perçus nettement et pour ainsi dire à l'infini.



Microphone de Hughes

Avant le perfectionnement dû à Edison, Bell offrait à l'un de ses amis une part d'intérêt dans son entreprise pour 500 francs et l'ami refusait. Quinze ans plus tard, la même part valait plus de 7 millions ! Edison excelle à trouver ce qui manque à une invention faite par un autre et ce qui va la rendre pratique et en centupler la valeur.

Malheureusement pour Bell, les messages transmis n'étaient pas clairs. Son invention comptait sur un bon récepteur, mais un mauvais transmetteur. Émile Berliner[32] entreprend ses recherches dans son petit appartement de Washington, transformé en laboratoire d'électricité. Il y avait même installé un téléphone entre son appartement et celui de sa logeuse. Le principe que Berliner découvre dotait l'invention de Bell d'un bon transmetteur pour toutes les distances. Le 4 juin 1877, son invention est brevetée. En termes simples, Berliner avait mis au point un vrai microphone. En septembre 1877, la compagnie *Bell Telephone* de Boston offre à Berliner une somme d'argent et un salaire en échange de son invention.



Microphone Berliner

Ainsi donc, on sait transformer des sons en vibrations électromagnétiques, les transporter sur un fil électrique et à l'arrivée les transformer en sons audibles. Pour s'affranchir des perturbations provoquées par l'induction produite par les fils télégraphiques voisins des fils téléphoniques, plusieurs systèmes furent mis au point. Le principal fut de supprimer le retour par la terre en construisant des lignes composées de deux fils.

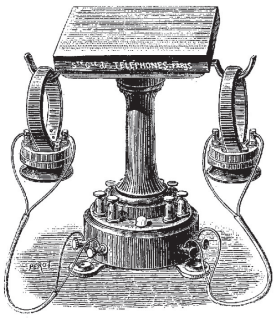
Cette mobilisation de connaissances scientifiques pour atteindre un objectif technique se situe dans un contexte où l'utopie du téléphone commence déjà à circuler. À l'occasion d'un dîner offert à Morse par Edward Thornton, ce dernier déclare (en 1868) : « *J'espère voir un jour des progrès techniques qui permettront de transmettre des conversations orales par le câble transatlantique. Nous verrons ainsi des commerçants de ce côté de l'Océan discuter de leurs affaires de façon instantanée avec leurs correspondants sur l'autre rive.* »

---

entre son appareil et un mouvement d'horlogerie le raccord nécessaire qui, automatiquement, envoie la lettre demandée et assure au dormeur la paix et l'impunité…

[32] *Berliner Gramophone Company*. Première compagnie de disques au Canada, fabricante des disques « *Gram-O-Phone* » et de machines parlantes. Elle fut fondée à Montréal par Émile Berliner (Hanovre, Allemagne, 20 mai 1851 - Washington, D.C., 3 août 1929), inventeur du gramophone et co-fondateur (Allemagne, 1898) avec son frère Joseph, de la *Deutsche Grammophon.*

Cette utopie du téléphone est loin d'être partagée par tout le monde. Un journaliste de Boston déclare : « *Les personnes bien informées savent qu'il est impossible de transmettre la voix humaine par fil, et que quand bien même ce serait possible, cela n'aurait aucun intérêt.* » En 1874, le journal *Telegrapher* rappelle cette vieille plaisanterie très répandue dans le milieu de la télégraphie : « *On avait essayé de parler entre New York et Philadelphie, mais on avait dû abandonner, car l'haleine de l'opérateur de Philadelphie empestait le whisky…* »



Le savant Gray, imagina, au niveau du transmetteur, de faire passer le courant produit par une bobine de Ruhmkorff[33], ce qui en augmentait considérablement la tension. Or, on savait que les courants de plus haute tension parcouraient des distances considérables. Mais ce fut M. C. Ader, ingénieur à la Société générale des téléphones (en France) qui fit la synthèse de toutes ces inventions, avec succès, en créant son transmetteur microphonique qui fut nommé *transmetteur Ader-Bell*. Le dispositif intégrait une sonnerie d'appel du correspondant.

Le premier réseau téléphonique apparut à Boston en mai 1877. Il réunissait cinq banquiers. Aussi, la Western Union qui possède à l'époque le quasi-monopole du télégraphe signe-t-elle un accord avec Bell qui prévoit de limiter son système aux « *conversations personnelles* ». Le téléphone « *ne doit pas être utilisé pour la transmission de messages d'affaires, de cotations en Bourse, d'informations sur le marché, toutes activités qui rentrent en concurrence avec la Western Union*. ».

Les attitudes des États européens face au réseau téléphonique sont contrastées. Côté anglo-saxon, le libéralisme est de tradition (du moins dans un premier temps…) ; côté allemand, le réseau tombe d'emblée aux mains d'une puissante administration. En France, les pouvoirs publics marquent peu d'empressement à l'égard de la nouvelle invention. L'administration des Télégraphes traverse une période de bouleversement : elle vient d'être rattachée à l'administration postale. Elle n'accorde que peu d'importance au téléphone, et c'est ainsi que naquit la *Société générale des téléphones*, citée plus haut, le 10 décembre 1880.

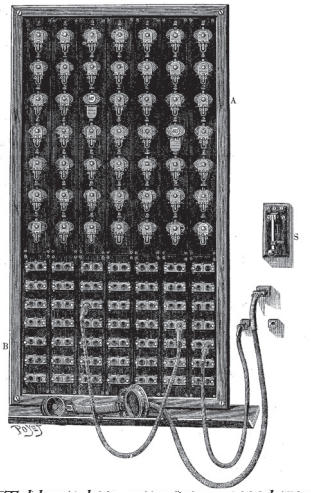


Tableau des annonciateurs et des commutateurs d'un bureau central de la Société des téléphones

C'est à cette Société que l'on doit la création du premier « central » dont la fonction était d'établir la correspondance entre les correspondants. Des réseaux furent créés à Paris, Lyon, Marseille, Bordeaux, Nantes, Lille, Le Havre, Rouen, Calais, Alger et Oran.

Les premiers usagers du téléphone sont les professionnels de la finance et de la Presse. L'usage privé est voisin de celui du télégraphe, comme le décrit un prospectus de New Haven en 1878 : « *Votre femme peut commander votre déjeuner, un cabriolet ou le médecin de famille…* » ; l'homme d'affaires est à la fois dans sa résidence d'été et à son bureau : « *De sa bibliothèque, il donne des ordres à ses employés…* » ; « *Dans la vie domestique, il permet de mettre l'utilisateur en contact instantané avec l'épicier, le boucher ou le boulanger…* ».

En 1878, Graham Bell écrivait : « *On peut imaginer que des lignes soient raccordées de façon souterraine ou aérienne à des domiciles privés, des*

[33] La bobine de Ruhmkorff est un générateur électrique permettant d'obtenir des tensions très élevée (plusieurs milliers ou dizaines de milliers de volts) à partir d'une source de courant continu à basse tension : un accumulateur 12 volts, par exemple. Elle a été conçue vers 1850 par Heinrich Ruhmkorff, mécanicien de précision parisien d'origine allemande. Auparavant Charles Grafton Page, aux USA, et Antoine Masson, en France, avaient réalisé des appareils similaires. Ruhmkorff apporta à la bobine de Masson les perfectionnements nécessaires pour répondre aux besoins, à la fois du milieu médical et des physiciens, d'une source de courant à très haute tension.

maisons de campagne, des boutiques ou des usines… Qui plus est, à l'avenir je pense… qu'une personne en un point du pays pourra communiquer verbalement avec une autre personne se trouvant ailleurs… » D'après un journal de l'époque, Bell espérait qu'il serait bientôt capable d'envoyer sa voix à travers l'Atlantique et de dialoguer avec des hommes situés à 3000 miles comme s'ils étaient dans la chambre voisine. Bell était cependant conscient des problèmes d'affaiblissement du son sur de grandes distances. Des expériences de transmissions téléphoniques sur 1.500 km sont signalées par l'*Electrician* dès 1879, puis à nouveau en 1883. Il n'est pas certain que ces expériences aient effectivement réussi.

L'affaiblissement du signal téléphonique a empêché pendant longtemps l'établissement de liaisons sur des distances plus longues. Ce n'est qu'en 1914 que la ligne New York – San Fransisco sera ouverte, et seulement en 1956 qu'ATT pourra installer la première ligne transatlantique !

Si Bell peut être considéré (avec les réserves données plus haut) comme l'inventeur du téléphone, l'inventeur de la téléphonie est plutôt Théodore Vail.

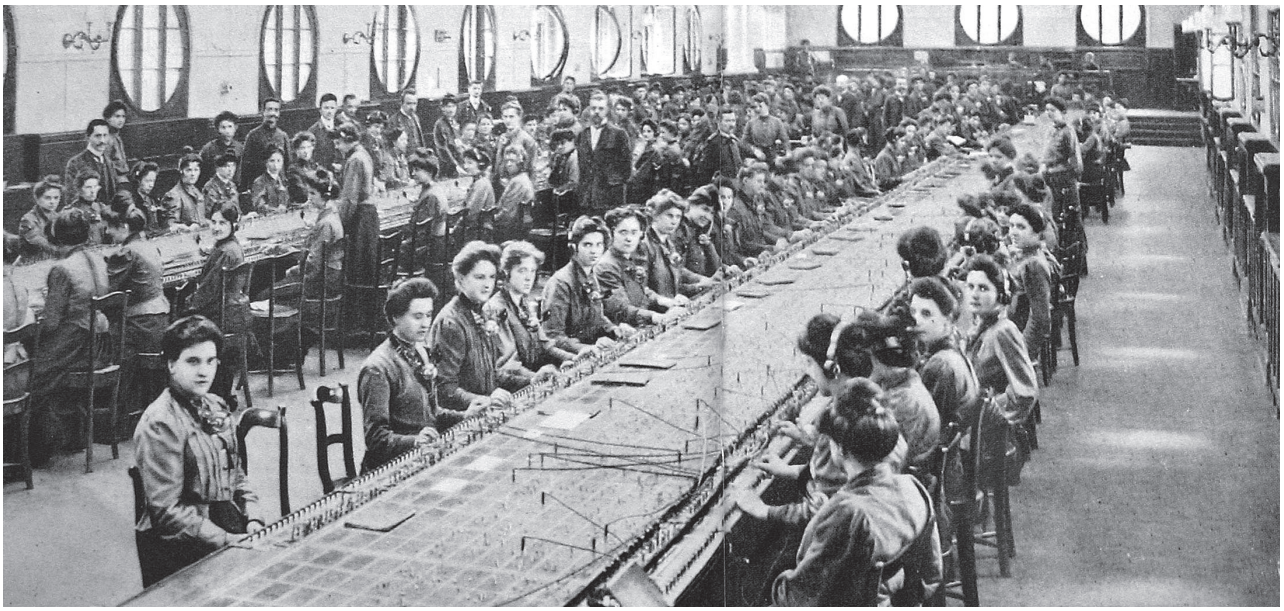
Théodore Newton Vail est né le 16 juillet 1848 dans l'Ohio et décédé en 1920. Il fut le fondateur et le premier président de la compagnie de téléphonie *American Telegraph and Telephon* (ATT), et est le véritable inventeur de l'organisation de la téléphonie en tant que service public et de l'organisation générale des services publics en monopoles, publics ou privés, mais contrôlés par une autorité d'élus aux États-Unis. Théodore Vail définit le téléphone comme « *un système capable d'assurer la communication avec tout correspondant possible, à tout moment.* »

En France, l'évolution est beaucoup plus lente. Le gouvernement s'appuie sur son réseau de télégraphe optique Chappe bien implanté, et néglige le télégraphe électrique de Morse tout comme l'invention de Bell. Au point que le téléphone en France accumulera un retard conséquent jusqu'en 1970.

Établissement et conception des premiers réseaux téléphoniques.

La vie des centraux téléphoniques

En attendant l'installation de l'automatique sur l'ensemble du territoire (qui n'est effective qu'à la fin des années 1970...), les centraux téléphoniques hébergent un personnel nombreux et qualifié. Les plus célèbres figures de ce microcosme sont les demoiselles du téléphone, ainsi appelées parce que cette



Opératrices à Berlin, en 1910

catégorie de personnel était recrutée exclusivement parmi des jeunes filles célibataires, dont l'éducation et la morale sont irréprochables. Elles perdaient généralement leur emploi lorsqu'elles se mariaient... Ces demoiselles sont aussi des cibles parfaites pour les clients mécontents du service. On leur reproche leur mauvaise humeur, la lenteur de l'établissement des communications... Dans le contexte du début du siècle, les abonnés sont surtout des gens fortunés qui ne supportent pas que le « *petit personnel* » ait autant d'influence sur leurs affaires. Pourtant, des concours d'efficacité sont organisés pour améliorer la qualité du service : on met en compétition des opératrices pour assurer le maximum de connexions à l'heure. Les records sont de l'ordre de 400 connexions/heure, ce qui correspond à une communication toutes les dix secondes...

Le travail des opératrices consiste à recevoir chaque appel d'un abonné faisant partie de son secteur, à lui demander le correspondant voulu, et à le mettre en relation avec son correspondant. L'opération se résume ainsi :

— l'abonné décroche son téléphone et tourne la manivelle[34].

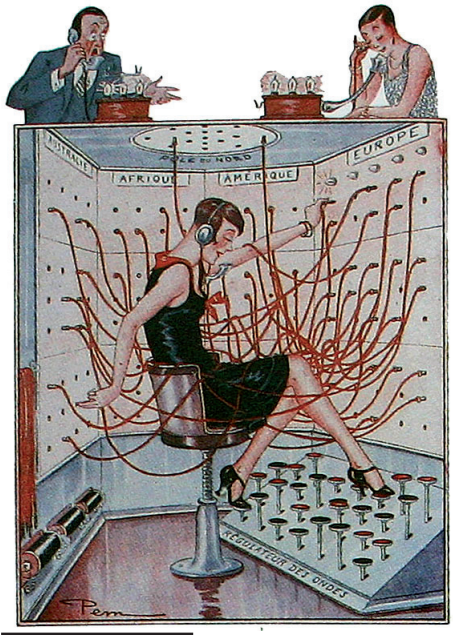
— l'opératrice voit le volet d'appel de l'abonné « chuter ».

— elle branche son casque sur le circuit de l'abonné, demande le numéro du correspondant.

S'il s'agit d'un abonné de son secteur, elle appelle directement ce correspondant, et met les deux abonnés en relation en branchant les deux fiches Jack d'un « *dicorde* »

S'il s'agit d'un abonné d'un autre secteur, ou d'un autre central, elle appelle l'opératrice correspondant à ce central et lui transmet la demande. Elle relie alors l'appelant sur un circuit auxiliaire (*le multiple*) qui le renvoie vers la nouvelle opératrice, qui se charge du reste de l'opération.

Le fait que chaque opératrice ait un secteur géographique attribué fait naître des complicités avec les abonnés. C'est pourquoi l'Administration modifie l'attribution des secteurs régulièrement.



Le métier de téléphoniste est difficile. Dans un premier temps, les demoiselles travaillent debout. La position assise est adoptée le 1er janvier 1890. Le casque est introduit en 1893 au central Gutenberg. Au bureau de la rue Lafayette, les employées se tiennent assises sur des chaises éloignées du bureau de plus d'un mètre. Elles attendent d'être « appelées par l'abonné ». En 1905, elles sont plus de mille au central Gutenberg, réparties en trois équipes de jour, à subir un encadrement de type paternaliste. Comme en Allemagne à la même époque, une discipline extrêmement stricte règne dans les bureaux. Avant 1914, chaque téléphoniste dessert quatre-vingts lignes certains usagers donnent plus de trente communications par jour et dans les services surchargés — pour une journée de sept heures effectives — elle doit assurer six communications à la minute

Médecins français, allemands ou américains étudient les maladies et les accidents professionnels provoqués par ces tâches pé-

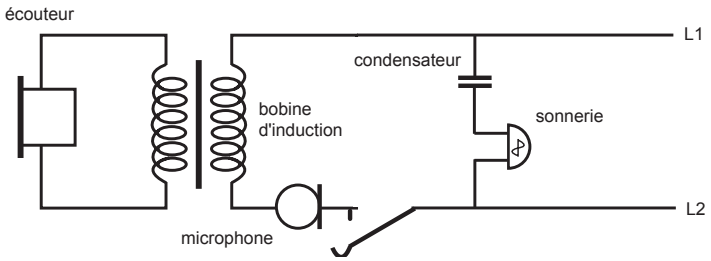
[34] Le rôle de la manivelle est de générer un courant alternatif qui, transmis sur la ligne, provoque la chute du volet d'appel sur le tableau de l'opératrice. Ce courant est généré par une petite « magnéto ». On trouvera ce dispositif sur les postes « *Marty* » en France à partir de 1910. Les abonnés ont longtemps cru que tourner la manivelle plusieurs fois (rageusement…) agacerait les demoiselles du central et les ferait mieux servir. En réalité, lorsque le volet de l'abonné était tombé, il ne se passait plus rien, si ce n'est un imperceptible bourdonnement.

nibles. Ils constatent des lésions de l'ouïe ainsi que différents troubles nerveux qui se manifestent par l'insomnie, l'irritation et peuvent mener à la dépression.

Les métiers féminins du téléphone ne sont pas tous concentrés à l'intérieur des centraux. Dans les usines et les ateliers qui produisent ou réparent des téléphones, on trouve aussi de nombreuses femmes. A la Compagnie française des téléphones, le taux de féminisation du personnel ouvrier avoisine cinquante pour cent. Le clivage entre emplois masculins et féminins y est très net. Aux hommes reviennent les métiers de la mécanique ou du bois, aux femmes les métiers délicats, minutieux et répétitifs : elles sont bobineuses, soudeuses, câbleuses, monteuses, décolleteuses, tourneuses.

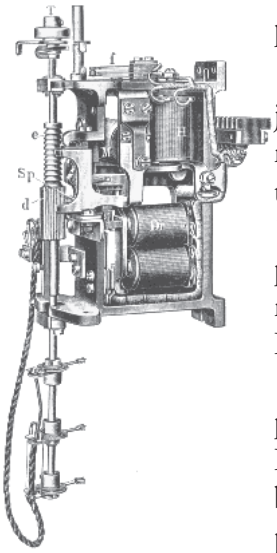
Réseau public à batterie centrale.

Dans ce type de réseau, le courant microphonique est fourni par le réseau lorsque l'abonné décroche le combiné. La détection de l'appel par l'opératrice est soit manuelle (magnéto), comme sur le poste Marty, soit automatique : le fait de décrocher le combiné signale le début de l'appel. Le principe des postes à batterie centrale est schématisé ci-dessous.



Poste Marty - 1924 -

En 1889, Almon B. Strowger, entrepreneur de pompes funèbres à Kansas City, invente un autocommutateur électromagnétique parce que l'opératrice du téléphone, épouse de son concurrent, dirigeait les clients vers le bureau de son mari.

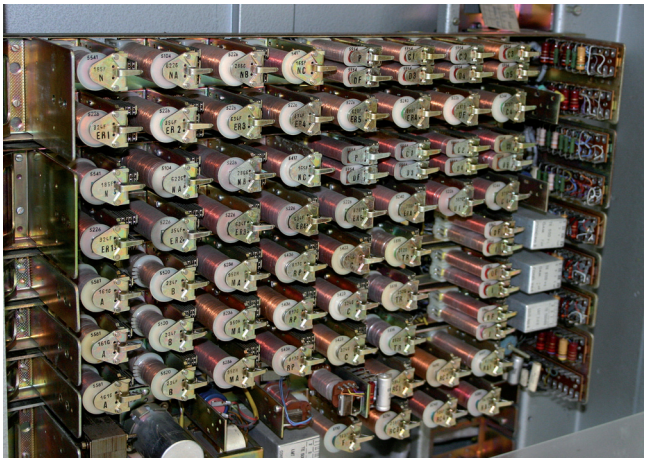

Sélecteur Siemens - 1912 -

En 1897, les premiers cadrans sont intégrés aux postes téléphoniques grâce à l'invention du *sélecteur automatique*.

Le système de commutation électromécanique sera en fonction, en France, jusqu'en 1978. Les centraux téléphoniques sont nombreux, car le signal téléphonique devient trop faible au bout d'une quinzaine de kilomètres. Au début, le téléphone est réservé aux communications locales (téléphone urbain). À partir de 1906, grâce à l'invention de la lampe triode par l'américain Lee de Forest, l'amplification du signal téléphonique devient possible. On peut alors envisager de raccorder tous les centraux entre eux pour constituer un véritable réseau national. Le téléphone devient interurbain.

La pose des grands câbles téléphoniques interurbains devint l'un des vastes projets industriels des exploitants téléphoniques au cours de l'entre-deux-guerres L'utilisation de tracteurs puissants et d'engins mécaniques destinés à creuser le bord des routes principales, afin d'y enterrer les câbles, permit dans la plupart des pays industrialisés la constitution d'un réseau « longue distance ».

Peu à peu, la commutation automatique se substitue à la commutation manuelle. Le travail ne consiste plus à enclencher des jacks ; il faut désormais comprendre des schémas, vérifier des circuits, repérer des dérangements. À la demoiselle du téléphone succède un mécanicien qui



Autocommutateur - 1969 -

travaille dans les entrailles du central, au milieu des rangées, dans cliquetis infernal des relais et sélecteurs.

Contrairement à leurs collègues des centraux, les ouvriers des lignes — les « lignards » — travaillent sans cesse à l'air libre. Leur labeur est particulièrement éprouvant, surtout en cas d'intempéries. Aux États-Unis, où les hivers sont souvent très rudes, les équipes chargées de la réparation des lignes accomplissent de véritables exploits pour rétablir les communications. En France, le 25 juin 1927, à la suite de l'incendie du central téléphonique Ségur, les ouvriers des lignes sont sollicités. La presse se fait l'écho de leur efficacité : « *Dès le jour même, des équipes d'ouvriers des lignes se sont mises au travail, et le dimanche, cinq mille lignes d'abonnés étaient remises en état. Il reste encore au moment où nous mettons sous presse, sept mille abonnés à rétablir, mais ils le seront sur un rythme de six cents à huit cents par jour. À ce propos nous tenons à souligner tout particulièrement l'effort du personnel des P.T.T. pour remettre en marche toutes les lignes.* »

Poste interurbain Jacqueson - 1924 -

Le premier câble souterrain français « grande distance » sera posé entre Paris et Strasbourg en 1924, suivi de Paris-Lyon en 1925.

Jusqu'en 1950, l'établissement des communications téléphoniques internationales est réalisé manuellement par l'intermédiaire d'une opératrice. Il faut attendre 1971 pour que soit ouverte au public la première liaison complètement automatique entre la France et les États-Unis. Le réseau mondial fut automatisé à partir de 1979.

Des chiffres et des lettres

Les premières communications, nous l'avons vu, étaient principalement locales. Le faible nombre d'abonnés fait que l'opératrice les connaît tous. Mais lorsque l'État décide d'implanter les réseaux « grand public » il devient nécessaire de « codifier » les utilisateurs, c'est-à-dire de leur donner une « adresse » téléphonique au même titre que l'adresse postale.

La solution qui fut retenue était simplement d'attribuer un numéro d'ordre chronologique aux demandes d'abonnement. Au fur et à mesure de l'installation de nouveaux centraux, on ajoute en tête du numéro de l'abonné, trois lettres désignant le central auquel il est raccordé.

Les premiers cadrans ne comportaient que des chiffres, aussi on ajouta 26 lettres par recouvrement.

Ainsi, si M. Dupont est le 273e abonné du central Opéra, son numéro devient : OPE 273.

Ce système trouvera ses limites, et le 19 octobre 1996, la France passe à la numérotation téléphonique à 10 chiffres qui offre une capacité de 300 millions d'abonnés. Le 16 septembre 1997, un tirage au sort

attribue des numéros d'opérateurs qui seront opérationnels pour le 1er janvier 1998, date de cession du monopole de France Télécom.

Un numéro de téléphone à 10 chiffres est alors décomposé de la manière suivante (on l'appelle codage E Z AB PQ MCDU) :

E : Exploitant
Z : Zone géographique
AB : Zone départementale
PQ : commutateur de rattachement
MCDU : identification de l'abonné
Détail des zones géographiques :
— Région parisienne : 01
— Région nord ouest : 02
— Région nord et est : 03
— Région sud est : 04
— Région sud ouest : 05
Numéros non géographiques :
06 : Mobiles
07 : NA
08 : numéros à tarification spéciale (depuis 0 800 numéro vert gratuit progressivement plus coûteux jusqu'au 0 898 à 1,2 € l'appel)
09 : à partir du 20/12/05, ouverture de la tranche 09 pour les communications interpersonnelles [pour remplacer les numéros 087x apparus avec l'arrivée de la voix sur IP sur DSL (ex., Free FreeBox, France Telecom LiveBox) et la téléphonie sur Internet (ex., Wengo, Skype). D'autres opérateurs de voix sur IP sur DSL fournissent des numéros géographiques (ex., Neuf Telecom neufBox, Cegetel CBox)]
Opérateurs téléphoniques :
0 : réservé : opérateur longue distance et présélection (en 2004 passe par France Télécom)
1 : réservé : pour les numéros spéciaux (ex: numéros d'urgence 15, 17, 18)
2 : en cours de restitution à l'ARCEP (préfixe de Siris, société rachetée par LD-Com maintenant Neuf Cegetel)
3 : réservé : aux numéros courts (ex : les 36PQ)
4 : Télé2
5 : restitué à l'ARCEP (préfixe de Omnicom puis de Ventelo, société rachetée par LD-Com maintenant Neuf Cegetel)
6 : restitué à l'ARCEP préfixe de Esprit Telecom puis de GTS-Omnicom (Ventelo), société rachetée par LD-Com maintenant Neuf Cegetel)
7 : Cegetel (maintenant Neuf Cegetel)
8 : France Telecom
9 : Neuf Telecom (société rachetée par LD-Com maintenant Neuf Cegetel)

Le réseau téléphonique commuté (RTC)

À l'origine, les « demoiselles du téléphone », comme nous l'avons vu, connectaient manuellement la ligne de l'appelant à celle de l'appelé. Puis les commutateurs ont évolué. Passant de l'électrotechnique aux technologies électroniques puis maintenant informatiques, ils permettent des gains de productivité importants par l'automatisation de tâches répétitives et d'opérations standardisées. Les informations de gestion des appels téléphoniques, appelées la « signalisation », transitent sur un réseau parallèle spécifique : le réseau « *Sémaphore* ».

Ces commutateurs constituent les différents points ou nœuds du Réseau Téléphonique Commuté ou RTC (in english STN : *Switched Telephone Network*). Ils sont reliés par des artères de transmission de différents types : câbles coaxiaux, à fibres optiques, faisceaux hertziens, satellites. Le RTC assure la connexion momentanée, de deux installations terminales afin de mettre en relation deux usagers. Ce réseau est actuellement le plus utilisé par les particuliers pour se relier entre eux ou à Internet. Le RTC public est très étendu, il atteint tous les pays de la planète et compte plusieurs centaines de millions d'abonnés.

Il y a plusieurs types de commutateurs, chacun ayant une fonction spécifique :

Le Commutateur à Autonomie d'Acheminement (CAA) ou commutateur local qui permet de mettre en relation les clients d'une même zone géographique. Ces commutateurs traitent également les numéros d'urgence (15, 17, 18 et 112) en joignant le service local concerné.

Un appel régional passe par le commutateur local qui envoie un signal au commutateur régional appelé Centre de Transit, qui permet d'écouler les communications téléphoniques d'un CAA à un autre CAA.

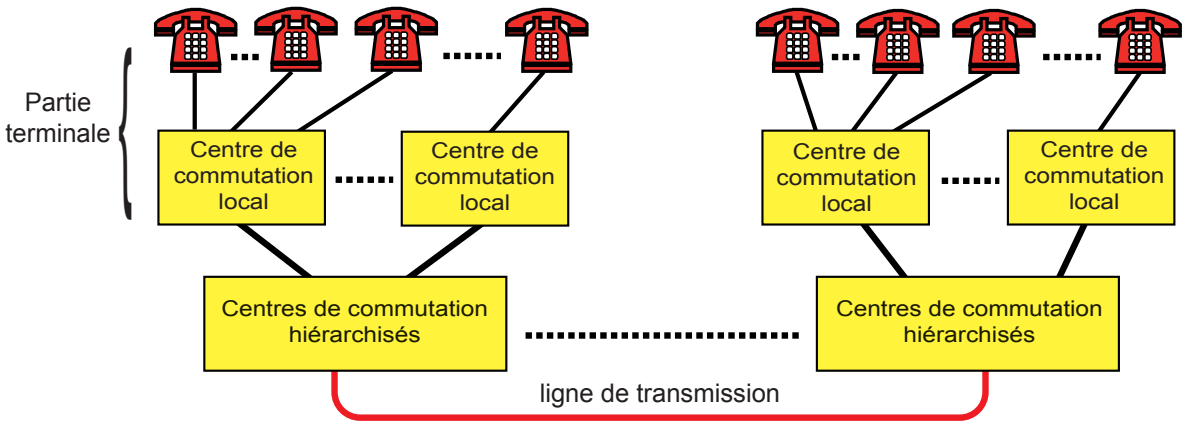
Si le numéro composé est destiné à l'international, c'est un des trois Centres de Transit Internationaux qui traite l'appel (Paris, Bagnolet ou Reims).

Pour offrir des services toujours plus complexes à ses clients, *France-Telécom* a amené de l'intelligence dans son réseau en associant commutateurs et serveurs informatiques. Ces serveurs informatiques commandent les commutateurs et prennent les décisions, c'est le principe du réseau intelligent. Par exemple, ils transforment les numéros spéciaux en numéros classiques, compréhensibles par les commutateurs. Ce principe est aussi utilisé par le service libre appel (numéros verts), les numéros à taxation partagée (numéros Azur et Indigo), le service *audiotel* et le 118-218. Ces numéros spéciaux sont envoyés vers différentes lignes en fonction de l'heure, le temps d'attente du client est ainsi réduit.

Schéma de principe simplifié du RTC

Le RTC est composé de nœuds (commutateurs) s'échangeant des informations au moyen de protocoles de communications normalisés par les instances internationales.

Les systèmes réalisant le RTC sont hétérogènes, ils proviennent de fabricants différents et utilisent des technologies différentes. Cette coexistence de technologies provient de la longue durée de vie de ces dispositifs, souvent supérieure à une vingtaine d'années.



Chaque poste téléphonique est rattaché à une seule armoire de répartition connectée à un commutateur local (*local switch*) dont la distance peut aller de quelques centaines de mètres jusqu'à quelques kilomètres réduisant d'autant la bande passante des signaux transmis du fait de l'augmentation de l'atténuation.

La faible bande passante (300 Hz – 3400 Hz) du RTC et d'autre part son rapport signal/bruit (de l'ordre de 40 dB) limitent la qualité du signal analogique transmis (voix) et donc le débit du nombre de bits transmis (informatique).

Les supports de transmission pour l'acheminement du signal entre commutateurs peuvent être faits par :

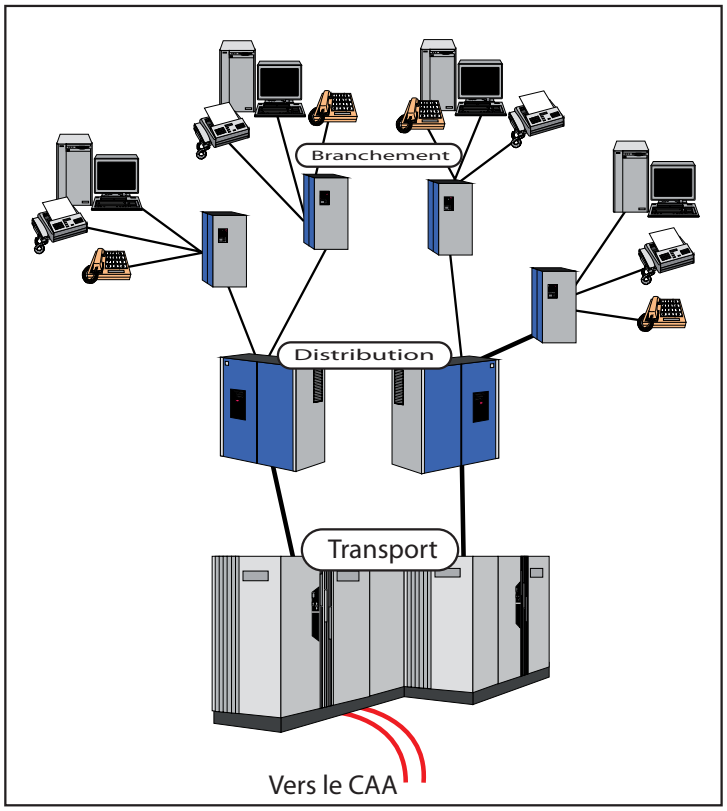
— des conducteurs métalliques (paires torsadées, câbles coaxiaux),

— par des liaisons en espace libre avec des faisceaux hertziens (via des antennes et des satellites)

— par des fibres optiques. La topologie du réseau est arborescente et conçue autour de nœuds de commutation contenant l'intelligence du réseau. Les signaux sont aiguillés dans ces nœuds, puis par la suite transmis par multiplexage fréquentiel (analogique) où chaque « conversation » se trouve transposée autour d'une fréquence et par multiplexage temporel (numérique) où les échantillons de plusieurs « conversations » sont transmis les uns à la suite des autres, de façon répétitive. En ce qui concerne les fibres optiques, une nouvelle technique de multiplexage dite en « longueur d'onde » a été développée. C'est grâce aux possibilités d'amplification, de modulation et de changement de fréquence qu'offre l'électronique que s'est développé le multiplexage permettant de transmettre un grand nombre de communications sur un même support : fil de cuivre, câble coaxial, fibre optique ou ondes hertziennes.

La boucle locale.

La boucle locale est la partie comprise entre le client et le centre local de rattachement du réseau France Télécom. On distingue 3 zones essentielles :



— La partie « Branchement »
— La partie « Distribution »
— La partie « Transport »

La partie « Branchement »

C'est la partie reliant les clients aux points de raccordement. Ces liaisons sont réalisées avec des câbles en cuivre. Une ligne est composée d'une paire de fils transmettant la voix et les données sous forme de signaux électriques.

La partie branchement développe le câblage en façade. Généralement, les logements particuliers et les petits immeubles accueillent une paire de fils de cuivre par ligne posée directement sur leur façade, tandis que la plupart des immeubles disposent d'une gaine technique chargée de recevoir les câbles de chaque résident et d'une armoire technique regroupant les connexions.

En France, la plupart des câbles sont organisés par regroupement de 7 paires de fils de cuivre, cette structure permet d'optimiser le diamètre des câbles. En fonction de la capacité d'abonnées recherchée, les câbles reproduisent ce type de regroupement par multiples de 7.

La connexion n'est pas toujours possible par câble. Par exemple, en zone montagneuse, on utilise la transmission radio. Des équipements émettent et reçoivent les communications par faisceau hertzien : c'est la boucle locale radio (nous reviendrons plus loin sur ce type de liaisons et de réseaux).

La partie « Distribution »

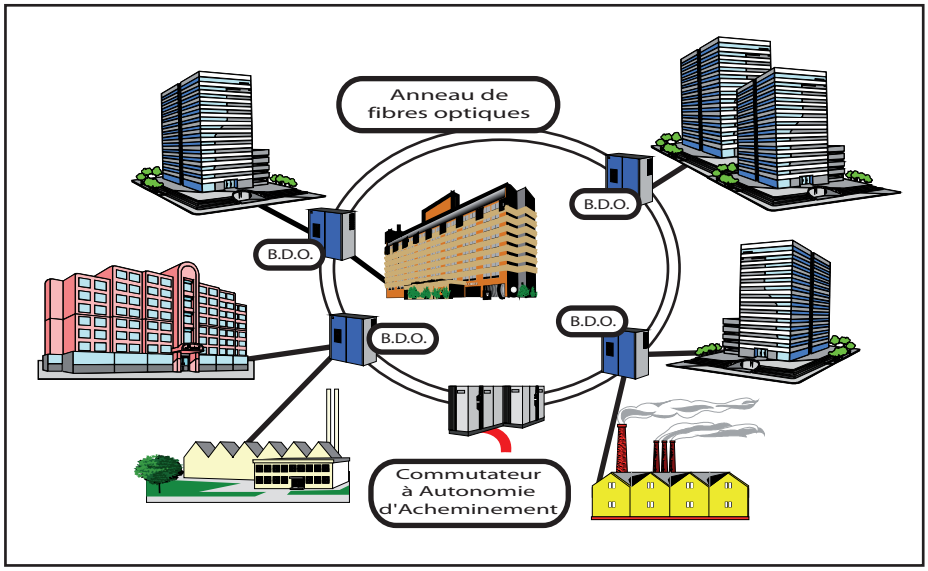
C'est la partie des câbles de moyenne capacité, qui relient les points de raccordement à un Sous-Répartiteur.

La partie « Transport »

La partie transport, est la partie qui connecte chaque Sous-Répartiteur à un Répartiteur via un câble de forte capacité. Chaque paire de cuivre correspondant à un client est reliée au répartiteur (jusqu'à une distance de quelques km). Le répartiteur reçoit l'ensemble des lignes d'usager et les répartit sur les équipements d'usager du central téléphonique grâce à une « jarretière », terme consacré du fait que la paire de fils est tendue entre deux points, l'un associé à l'adresse géographique, l'autre associé à un équipement téléphonique. Le répartiteur est donc un dispositif passif de câblage centralisant les lignes de la zone de desserte du Centre à Autonomie d'Acheminement (CAA) et assurant la correspondance entre une ligne et un équipement téléphonique.

Les CAA sont capables de mettre eux-mêmes les clients en relation.

La structure en anneau



L'organisation dite en anneau, fut créée pour répondre aux attentes des industriels, PMI et PME.

Utilisant la technologie des fibres optiques, l'anneau fait circuler des données, à travers des Boîtes de Distribution Optique (B.D.O.) qui concentrent les fibres optiques. On garantit ainsi un débit et une qualité très élevés.

En cas d'incident sur une des voies, les données peuvent toujours circuler en utilisant la partie intacte de l'anneau, la communication est dite « sécurisée ».

Communication entre le téléphone et le central

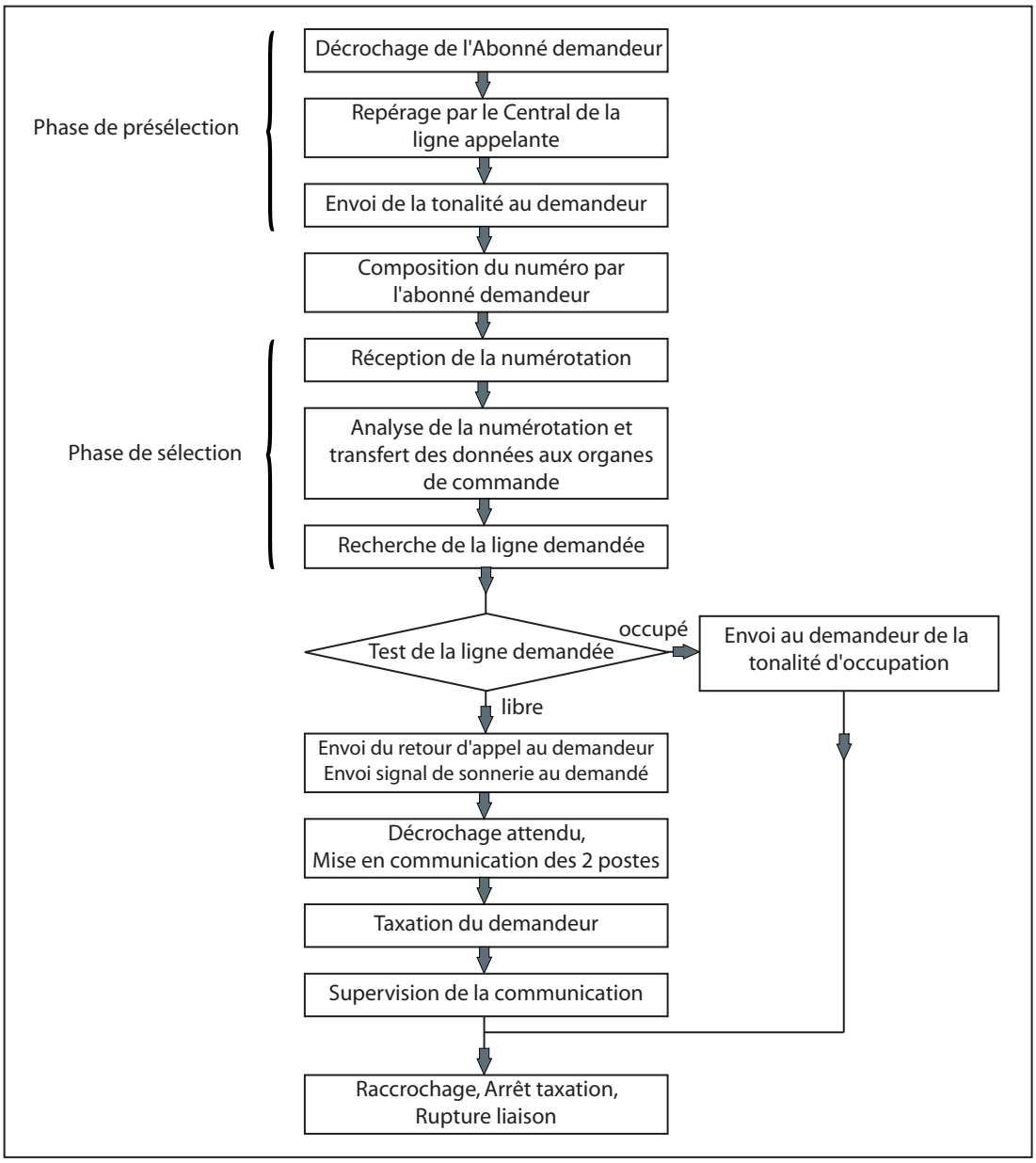
C'est la norme TBR21 (janvier 1998) qui fixe les caractéristiques électriques des signaux émis par le combiné téléphonique ou n'importe quel équipement branché sur la prise.

Phases d'établissement d'une communication.

Liaison entre le téléphone et le central téléphonique.

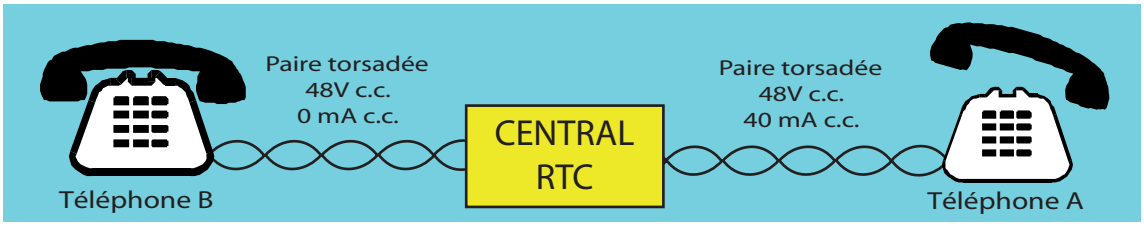
Chaque téléphone grand public est généralement connecté à un central RTC (réseau téléphonique commuté) par une simple paire de fils de cuivre d'un diamètre d'environ 0,5 mm. Ces câbles ont une impédance caractéristique de 600 Ω. Cette liaison avec le poste de l'abonné est dite boucle locale (local

loop) et, lors d'une communication téléphonique, transporte une composante continue d'alimentation du poste ainsi que le signal vocal. Mais les nouveaux systèmes utilisent des câbles coaxiaux ou fibres optiques pour accéder à une bande passante accrue.



Décrochage du combiné

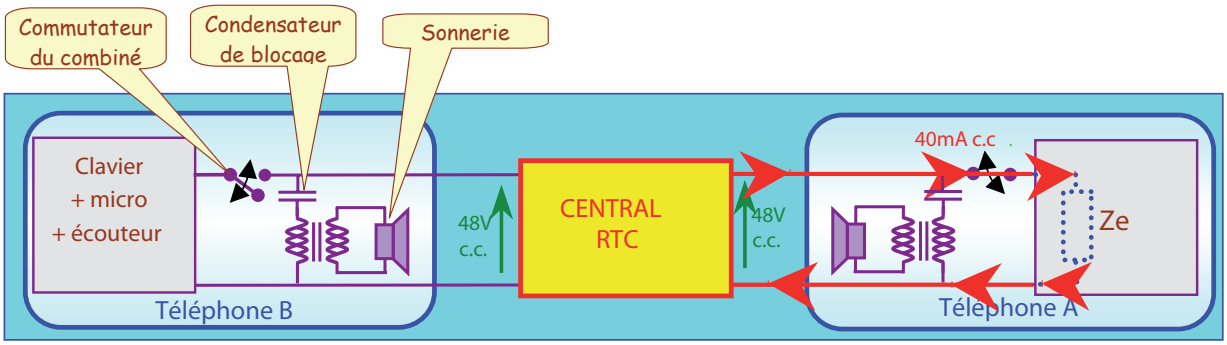
Lorsque le téléphone n'est pas décroché, il est soumis à une tension continue d'environ 48 V venant du central (attention à ne pas toucher : cela peut secouer !). Le choix d'une tension continue est antérieur à l'existence des centraux téléphoniques. À l'origine, les batteries étaient situées chez l'usager (*batterie*



locale). Le but était de polariser le microphone à charbon avec un courant d'environ 30 mA. À ce moment-là, l'utilisation du courant alternatif (secteur) n'existait pas encore.

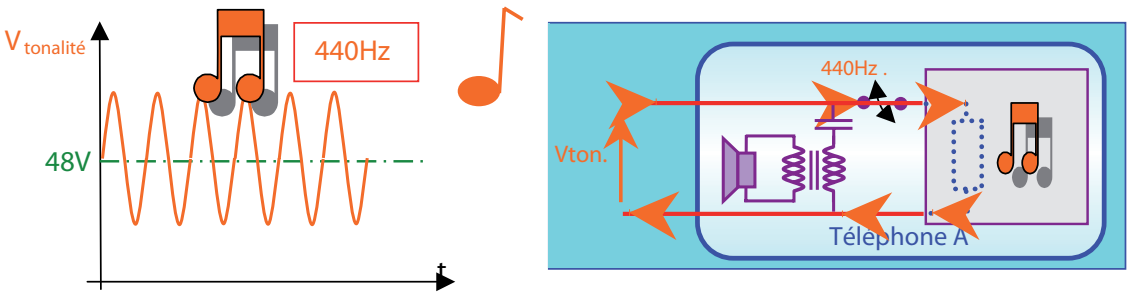
Au repos, l'impédance présentée par le poste est associée au circuit de sonnerie dans lequel est inséré un condensateur qui empêche la circulation d'un courant continu. Dans l'attente d'un appel, les postes étant soumis à une tension continue ne consomment aucun courant.

Lorsque l'on décroche (*off-hook*) le combiné du poste (A), le commutateur se ferme, alors le poste présente une impédance assez faible et consomme un courant continu de l'ordre de 40 mA, signalant ainsi son souhait au central d'établir une communication, c'est la prise de ligne. La tension continue peut alors descendre entre 10 V et 22 V lorsque la ligne est chargée (téléphone décroché). Cette chute de tension s'explique de deux manières : sur un commutateur public, elle est provoquée par la ligne d'abonné, qui présente une résistance de boucle dépendant de sa longueur et du diamètre des fils. D'ailleurs, sur les anciens postes téléphoniques à cadran, on pouvait insérer une résistance d'ajustement du courant de ligne pour ne pas dépasser les 40 mA. Sur un commutateur privé, les lignes sont en général courtes, une régulation de courant est mise en œuvre et de ce fait réduit la tension d'alimentation du poste téléphonique.



Tonalité

Après la fermeture du commutateur du combiné, le central du réseau public acquitte la demande de connexion en superposant à la tension continue, un signal sinusoïdal de 440 Hz (note de musique « LA »), c'est l'invitation à numéroter : la tonalité (*dial-tone*). Les autocommutateurs privés fournissent une tonalité de fréquence égale à 330 Hz. On perçoit ce changement lors de la composition du « 0 » pour émettre un appel sortant.



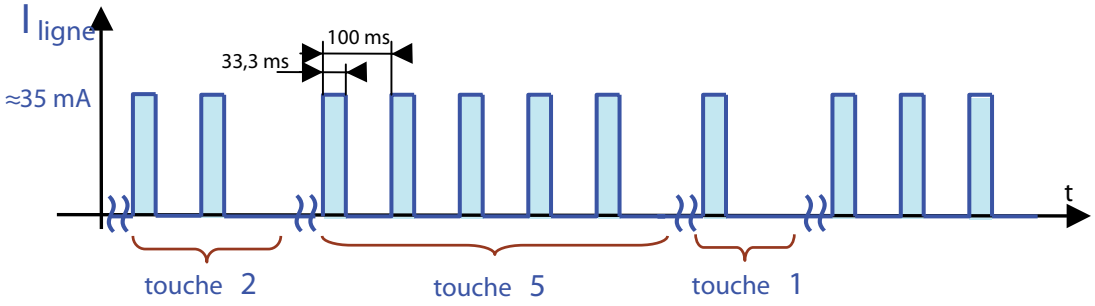
Numérotation décimale

Ce procédé de numérotation par impulsions (dite aussi *par ouverture de boucle*) est utilisé par les téléphones à cadran rotatif (poste à disque) et par certains modems. Dans ce cas, le courant continu est interrompu un nombre de fois correspondant au chiffre envoyé, générant ainsi des impulsions à « 0 ».

Une impulsion pour le chiffre 1, deux impulsions pour le chiffre 2, et ainsi de suite… jusqu'à dix impulsions pour le chiffre 0.

Chaque impulsion dure 100 ms, soit 33,3 ms pour la ligne fermée (présence de courant) et 66,7 ms pour la ligne ouverte. Pour composer le 1, il faut 100 ms ; pour faire le 2 il faut 200 ms, ainsi de suite jusqu'au 0 où il faut 1 s.

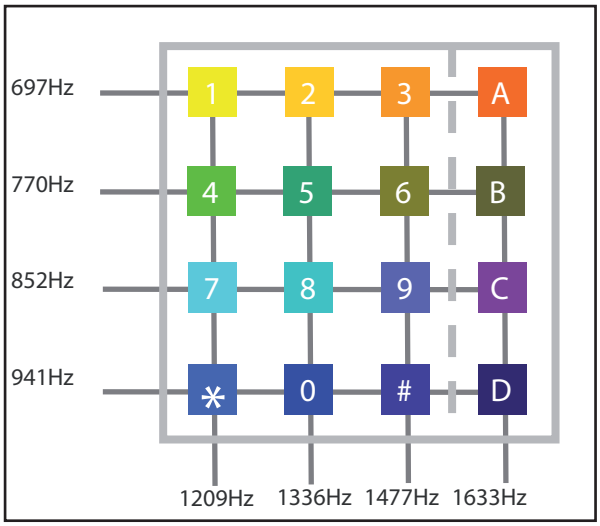
Un intervalle de temps d'au moins 200 ms doit séparer 2 trains d'impulsions. Ce principe ancien est lent.



Numérotation par fréquences vocales ou DTMF (*dual tone multi frequency*)

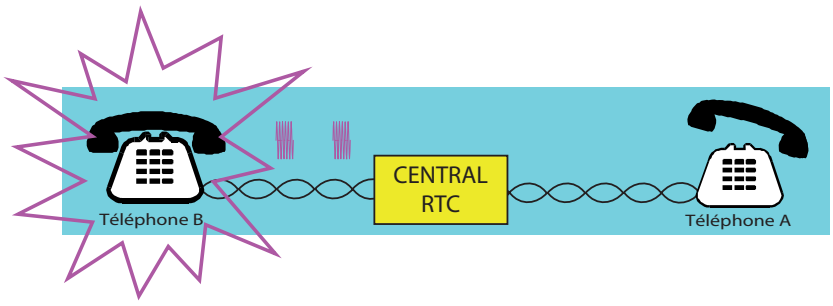
Le DTMF est un procédé de numérotation qui génère des sonorités codées, il doit émettre des fréquences spécifiques dans la gamme 300 Hz – 3400 Hz. Mais si l'on attribue une fréquence simple à chaque chiffre, un sifflement (ou un son propre et fort) peut provoquer une erreur de numérotation !

Ce problème d'interférence est résolu simplement, par l'émission de deux fréquences simultanées par chiffre. Il est très peu probable que deux fréquences spécifiques, dont les valeurs sont premières entre elles, soient présentes à l'arrière-plan du microphone pendant la numérotation. Ces fréquences sont normalisées au plan international (norme UIT-T-Q.23). Sur le clavier du téléphone, en appuyant sur une touche, on émet les deux tonalités correspondant à l'intersection de l'axe horizontal et de l'axe vertical.



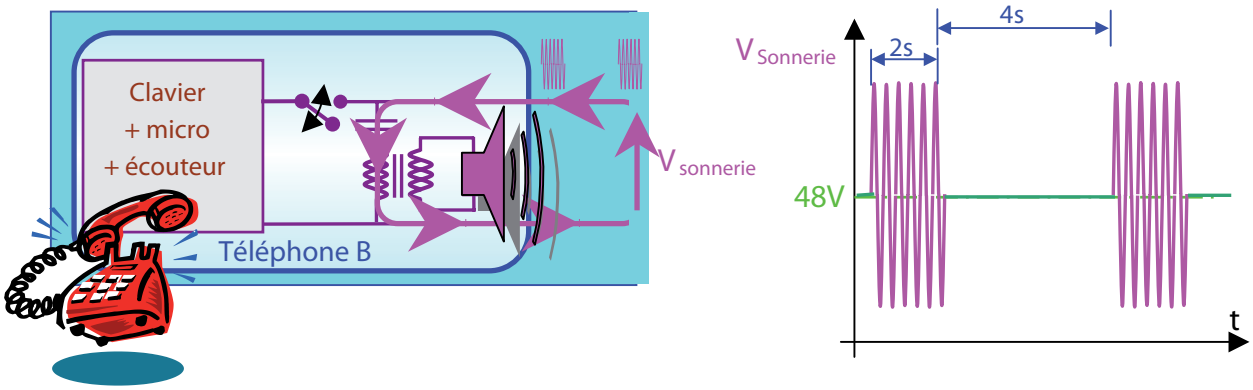
Pour éviter les problèmes de distorsion et de génération d'harmoniques, aucune fréquence n'est harmonique d'aucune autre fréquence. De plus, il est impossible de synthétiser une fréquence à partir de la somme ou de la différence de deux autres fréquences, pour éviter les erreurs de numérotation dues aux produits d'inter modulation. Actuellement, la durée d'enfoncement d'une touche et l'intervalle de temps entre deux manœuvres successives ne peuvent être inférieurs à 40 ms.

Activation de la sonnerie



Après que l'abonné du poste A ait composé le numéro du correspondant (B), le RTC via les commutateurs va acheminer l'appel, puis actionne la sonnerie du poste B par l'intermédiaire du dernier central autocommutateur local.

Pour activer la sonnerie, le central envoie vers le poste B un signal sinusoïdal de fréquence environ 50 Hz et de tension de 50 à 80 V efficaces par rafales, activé pendant environ 2 secondes et désactivé pendant environ 4 secondes. Ce signal est superposé à la tension continue de 48 V.



Le décrochement du poste B établit un courant continu d'environ 40 mA dans la ligne. Alors, le central RTC supprime la sonnerie et met en liaison les deux correspondants. Lorsque la liaison est établie, on a pratiquement une ligne point à point.

On utilise une tension de 80 V, relativement élevée, pour pouvoir activer les sonneries peu efficaces des anciens téléphones. Dans les nouveaux postes équipés de sonnerie électronique, un signal numérique TTL (5 V) suffit, mais le niveau TTL est incompatible avec les anciens téléphones.

Transmission de la voix

L'énergie vocale humaine se situe en grande partie dans cette gamme de fréquences, ce qui permet d'obtenir une conversation fiable (mais sans être excellente). C'est surtout cette limitation de bande passante qui fait que l'on a du mal à saisir la différence au téléphone entre « b », « p » et « d ». La variation de tension audio est de 5 à 500 mV crête, générant une dynamique de 40 dB très inférieure à celle d'un système Hi-Fi (70 - 90 dB).

Lorsque les deux correspondants sont en liaison, les signaux vocaux envoyés et reçus sont dus à une modulation de l'amplitude du courant continu dans la bande de fréquences 300 Hz à 3,4 kHz. A l'intérieur de chaque appareil, un dispositif « *antilocal* » évite que le signal émis par le microphone ne soit transmis à l'écouteur. La communication s'effectue en duplex intégral, elle est bidirectionnelle, le courant sur la ligne étant la somme du courant continu et des deux courants variables émis par chaque poste.

Pendant la phase de communication, les commutateurs supervisent la communication pour détecter le raccrochage de A ou de B. Si un des 2 accroche, la liaison est libérée (ou relâchée), c'est la phase de libération qui à nouveau met en œuvre la signalisation. La taxation est aussi arrêtée.

Numéris, le réseau numérique à intégration de service (RNIS) de France Télécom.

L'information est numérisée de bout en bout, jusque chez les abonnés. Une ligne d'abonné peut véhiculer ainsi plusieurs canaux, ce qui permet de nouvelles facilités et de nouveaux usages.

Le RNIS de France Télécom a pour particularité d'être construit sur le réseau RTC : du point de vue matériel, la migration vers Numéris se fait essentiellement en modifiant les deux extrémités de la ligne de l'abonné.

La technologie RNIS (Réseau numérique à intégration de services - ou en anglais : ISDN, Integrated Services Digital Network) permet d'utiliser des données numériques sur la boucle locale, et ainsi d'offrir de meilleurs débits aux utilisateurs distants. Les opérateurs téléphoniques ont mis au point la technologie RNIS en vue de créer un réseau entièrement numérique. Le réseau RNIS fournit donc une connectivité numérique de bout en bout en transportant des données numériques sur une ligne de téléphone analogique.

La technologie RNIS utilise la signalisation hors bande, le delta (canal D), pour l'établissement de l'appel et la signalisation. Lors de la mise en place d'une connexion TCP, un échange d'informations, appelé établissement de la connexion, s'effectue. Ces informations sont échangées sur le chemin par lequel les données vont ensuite être transmises. Les informations de contrôle et les données partagent toutes deux le même chemin. C'est ce que l'on appelle la signalisation in band. La technologie RNIS, elle, fait appel à un canal séparé pour les informations de contrôle, le canal D. C'est ce que l'on appelle la signalisation hors bande.

RNIS consiste, logiquement, en 2 types de canaux de communication :

- Un canal de signalisation (canal D - Data Channel - couche 2 : Commutation de paquet : Protocole LAP-D) (16 kbit/s pour les accès de base ou à 64 kbit/s pour les accès primaires)
- Des canaux de transfert (canaux B - Bearer Channel - Couche 1 : Commutation de circuit : PPP, HDLC). Bien qu'ils soient transportés par les mêmes fils électriques, les canaux B sont distincts les uns des autres. (64 kbit/s chacun)

Ces canaux sont full duplex et les canaux B peuvent être utilisés séparément, ou réunis à plusieurs pour créer une liaison fonctionnant à un multiple de 64 kilobits/sec.

Il existe deux types de raccordement RNIS :

- L'accès de base S0 (Basic Rate Interface = BRI) comporte deux canaux B, et un canal D (à 16 kilobits/sec). On l'appelle aussi connexion 2B+D. Il se contente d'une ligne téléphonique ordinaire.
- L'accès primaire S2 (Primary Rate Interface = PRI) aux USA et au Japon : comporte 23 canaux B et un canal D (à 64 kilobits/sec). On l'appelle parfois «connexion 23B+D» et nécessite une ligne débitant 1,6 mégabits/sec (normalisée sous le vocable T1). Et en Europe, comporte 30 canaux B et un canal D (à 64 kilobits/sec). On l'appelle parfois « connexion 30B+D ». Il nécessite une ligne débitant 2 mégabits/sec (normalisée sous le vocable E1).

Le réseau Transpac

Créé en 1978, Transpac est un réseau mondial de transmissions de données par paquets (on dit souvent « réseau X25 »). Au départ, les données sont fragmentées en paquets de 4096 octets (ou caractères) au maximum, précédés chacun du code du destinataire, de l'indication du message auquel le paquet appartient et de sa place dans le message. Recevant des paquets de différentes provenances, le premier commutateur les mémorise le temps de les « raccrocher » les uns aux autres suivant leur destination, pour constituer des « trains ». Arrivés à destination, les paquets d'un même message sont assemblés dans l'ordre et envoyés au correspondant.

L'opération s'effectue en moins d'une seconde. Cette technique du « circuit virtuel » comporte trois avantages : rapidité, économie, fiabilité puisque les paquets peuvent emprunter plusieurs itinéraires.

Le réseau Transpac est utilisé notamment :

- pour acheminer le trafic Télétel (Minitel – serveurs)
- pour la monétique et le paiement par carte
- pour constituer des réseaux d'entreprise
- pour échanger des courriers et des fichiers intra- et inter- entreprises à grande vitesse.

Comme la plupart des réseaux de données numérisées, le réseau Transpac n'est pas conçu pour la transmission de la voix, ni des images animées en temps réel.

Depuis le 1er juin 2006, Transpac a été intégré à *Orange Business Services*.

Le réseau à large bande ATM

Asynchronous Transfer Mode (Mode de transfert asynchrone) ou ATM, est un protocole réseau qui transmet les données par « cellules » de 53 octets plutôt que par paquets de longueurs variables comme IP ou Ethernet[35].

ATM a été conçu pour fournir un standard réseau unifié qui pourrait supporter un trafic réseau synchrone, aussi bien qu'un trafic utilisant des paquets tout en supportant plusieurs niveaux de qualité de service.

ATM cherchait à résoudre les conflits entre les réseaux à commutation de circuits et les réseaux à commutation de paquets en proposant une interface vers un flux de petites cellules, de 53 octets marqués par des identifiants de circuits virtuels. Les cellules sont habituellement envoyées à la demande selon une certaine fréquence dans un flux de bits synchrone : ce qui est asynchrone est l'envoi des cellules, non le flux qui les transporte.

À l'origine, ATM était censé être la technologie permettant le « *Broadband Integrated Services Digital Network* » qui remplacerait le RTC existant. La suite complète de standards ATM propose des définitions pour les couches de niveaux 1, 2 et 3 du modèle OSI classique à 7 couches. Les standards ATM étaient dessinés sur des concepts destinés aux télécommunications plutôt qu'aux réseaux informatiques. Pour cette raison, un immense travail a été réalisé pour intégrer dans ATM le plus possible de technologies et conventions existantes en télécommunications.

ATM est donc une technologie hautement complexe, dont les fonctionnalités s'appliquent aussi bien aux réseaux globaux des sociétés de télécommunications (telco) qu'aux LAN[36] plus réduits.

Beaucoup de sociétés de télécommunications ont mis en place de grands réseaux ATM et beaucoup d'implémentations DSL[37] utilisent ATM. Cependant ATM a échoué à être largement répandu en tant que technologie LAN et sa grande complexité a été un obstacle à son développement en tant que technologie réseau intégrative comme ses inventeurs l'avaient imaginée…

La plupart des bonnes idées d'ATM ont migré dans MPLS[38], un protocole de niveau 2 de commutation de paquets (packet switching). ATM reste utile et largement déployé comme couche de multiplexage dans les réseaux DSL, où ses compromis correspondent bien aux besoins de cette application.

ATM survivra probablement aussi pour un certain temps dans les interconnexions à haute vitesse dont les responsables se sont déjà engagés dans le déploiement d'ATM comme façon de combiner le trafic PDH[39]/SDH[40] et le trafic de paquets dans une architecture simple.

Nous compléterons l'étude des réseaux téléphoniques avec le réseau « mobile » après avoir étudié les transmissions par radio.

---

[35] *Ethernet* est un protocole de réseau informatique à commutation de paquets

[36] Un réseau local, souvent désigné par l'acronyme anglais LAN de *Local Area Network*, est un réseau informatique à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise. Dans le cas d'un réseau d'entreprise, on utilise souvent le terme RLE pour *réseau local d'entreprise*.

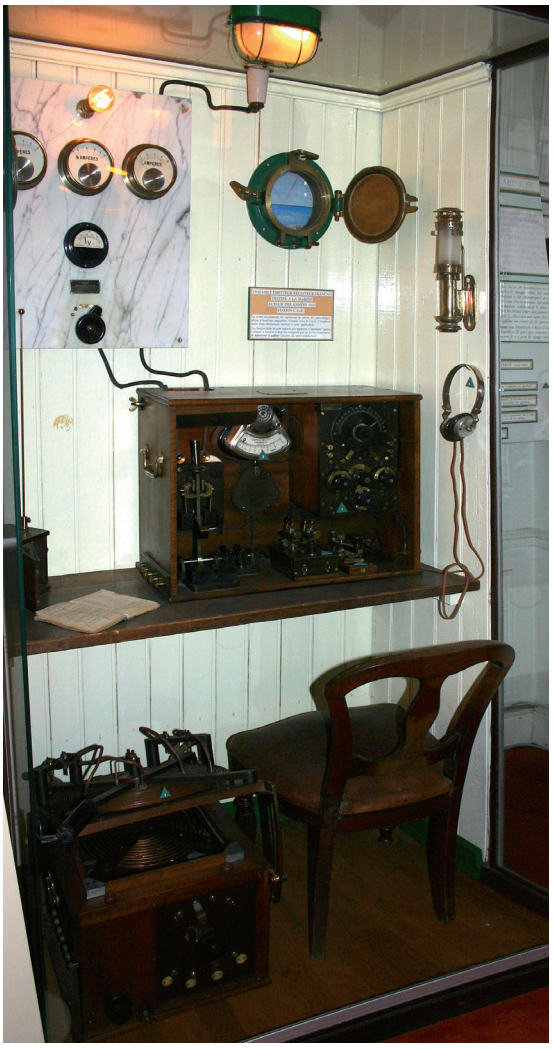
[37] *Digital Subscriber Line*, un mode de codage des données.

[38] *MultiProtocol Label Switching* (MPLS) est un mécanisme de transport de données

[39] PDH (en anglais *Plesiochronous Digital Hierarchy*) est une technologie utilisée dans les réseaux de télécommunications afin de véhiculer les voies téléphoniques numérisées.

[40] SDH (en anglais *Synchronous Digital Hierarchy*) est un ensemble de protocoles pour la transmission de données numériques à haut débit.

La T.S.F.



Reconstitution du Poste T.S.F. du Titanic (Musée Européen de la Communication à Pignerolle - 49 -)

De même que pour le téléphone, l'invention de la Télégraphie Sans Fil, ne peut revenir à un seul chercheur.

Il est apparu très vite que les moyens de transmission par fil étaient un handicap de taille au développement universel de la communication, en particulier avec les navires ainsi que dans tous les endroits géographiquement difficiles d'accès.

Heureusement, la réunion des techniques de télégraphie, puis plus tard de téléphonie, avec la découverte des ondes radio fit sauter les dernières barrières ouvrant la voie aux communications modernes.

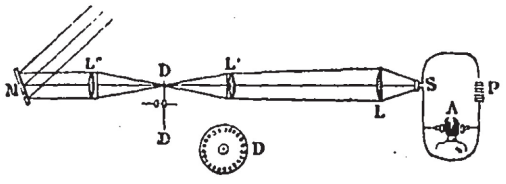
C'est ce que nous allons étudier maintenant.

Le Radiophone. (par le comte Th. Du Moncel.)

La première expérience de transmission de la parole sans l'utilisation d'un fil fut conduite par Graham Bell en 1880. Il avait étudié les propriétés du sélénium dont il disait ceci : « *Quand il est à l'état vitreux, il est de couleur brun foncé, presque noir à la lumière diffuse, et a une surface extrêmement brillante. Réduit à l'état de pellicule fine, il est transparent, et paraît d'un beau rouge quand il est frappé par la lumière. Quand, après avoir été fondu, il est refroidi très lentement, il présente un aspect tout différent ; il devient d'un rouge pâle, avec aspect granuleux et cristallin, ayant l'apparence métallique. Il est alors parfaitement opaque, même en pellicules minces. Cette variété de sélénium a été longtemps connue sous le nom de granulaire ou cristalline ou métallique, ainsi que l'a appelée M. Regnault. C'est cette variété de sélénium qu'Hittorf trouva être conductrice de l'électricité à la température ordinaire, et il trouva également que sa résistance diminuait constamment en la chauffant jusqu'au point de fusion, mais qu'elle augmentait ensuite subitement en passant de l'état solide à l'état liquide. On a vu d'ailleurs que la lumière agissait d'une manière considérable sur cette substance.* »

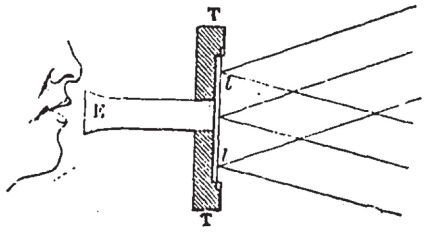
Dans le numéro du 1er octobre 1880, du journal « *La Lumière électrique* », il disait : « I*l est aisé de comprendre que si le photophone pouvait être mis en action à une distance un peu grande, ce qui n'est pas facile à admettre en raison de l'affaiblissement rapide de l'intensité lumineuse avec la distance, il pourrait rendre quelques services pour la défense des places assiégées, dans certains travaux de géodésie, et peut-être même à la guerre, comme complément de la télégraphie optique…* »

Dans son premier mémoire sur le « *Radiophone* », Graham Bell détaillait ses expériences avec des figures que nous reproduisons ci-dessous, accompagnées du commentaire suivant : « *Je fus alors frappé de l'idée de produire des sons sous l'influence de la lumière, et, en étudiant plus à fond la question, je pensai que tous les effets d'audition produits sous l'influence électrique pouvaient être obtenus par des changements d'intensité d'un rayon lumineux projeté sur le sélénium, et qu'ils ne pouvaient avoir pour limite que celle à laquelle s'arrête l'action de la lumière sur cette substance ; or, comme cette limite peut être assez reculée par la projection de rayons parallèles concentrés sur la plaque sensible par un réflecteur parabolique, je pensai qu'il serait possible d'établir, par ce moyen, des communications téléphoniques d'un point à un autre sans le secours d'aucun fil conducteur, entre le transmetteur et le récepteur. Il était évidemment nécessaire, pour rendre cette idée pratique, de construire un appareil susceptible d'actionner la lumière sous l'influence de la parole, et c'est ainsi que je fus conduit au système dont je parle aujourd'hui.* »



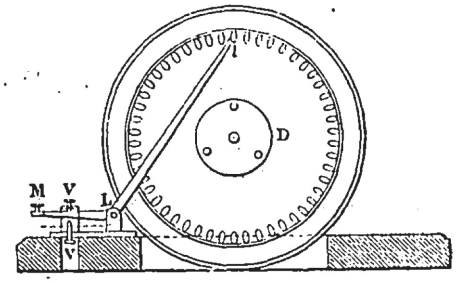
La figure ci-dessus montre la manière de reproduire des sons par la rotation d'un disque muni de trous et interceptant le faisceau lumineux agissant sur le disque de sélénium. L'auditeur est en A, ayant un

téléphone à chaque oreille ; le disque de sélénium est en S, la pile en P, et le disque tournant en DD, au point de croisement des rayons réfléchis. Ces rayons tombent sur un miroir M, qui les réfléchit à travers une première lentille L", d'où ils sortent pour se projeter, après s'être croisés, sur une seconde lentille L' qui les rend parallèles pour atteindre une troisième lentille L ; celle-ci les concentre sur le disque de sélénium, et c'est au point de croisement D des rayons qu'est placé le disque percé de trous DD que l'on aperçoit vu de face au bas de la figure.



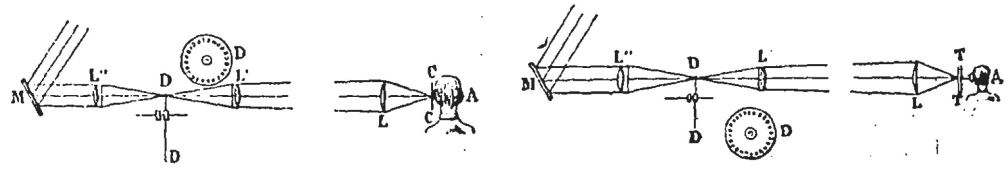
Le radiophone fig. 36

La figure 36 représente le miroir téléphonique derrière lequel on parle pour transmettre la parole par l'action des rayons lumineux ; la lame de mica argenté *ll* forme, comme on le voit, la lame vibrante d'un téléphone TT, ayant, une longue embouchure E, et les rayons lumineux projetés angulairement sur cette lame se trouvent déviés de leur direction normale de réflexion par les vibrations de la lame, ce qui équivaut à des extinctions proportionnelles à ces vibrations.



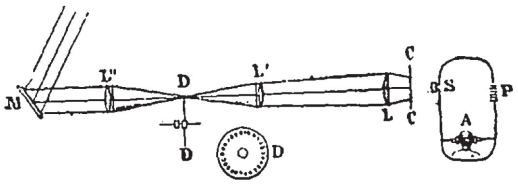
Le radiophone fig. 37

La figure 37 montre le disque tournant D sur une plus grande échelle que dans la figure 35. Devant les trous de ce disque se trouve un levier obturateur articulé L*l* dont la branche la plus courte, LM, constitue une clef Morse, mobile entre deux butoirs V. En effectuant avec la poignée la manœuvre du Morse, on obtient une obturation saccadée et plus ou moins longue des rayons lumineux, et par suite les sons longs et courts des parleurs télégraphiques dans le système Morse.



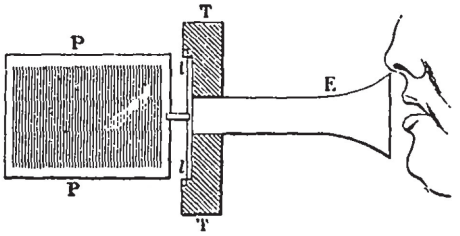
Le radiphone fig. 38 et 39

Les figures 38 et 39 représentent la disposition de la première expérience sans l'intervention du circuit téléphonique, et par conséquent les sons produits dans ces conditions résultent de l'action directe de la lumière sur les plaques où elle se trouve projetée ; l'auditeur a alors, comme on le voit, la plaque appliquée à l'oreille.



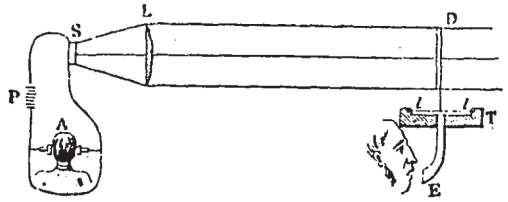
Le radiophone fig. 40

La figure 40 représente la première expérience avec l'interposition du disque mince de caoutchouc durci CC sur le trajet des rayons lumineux avant leur concentration sur le sélénium S.



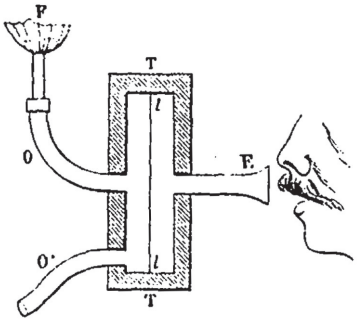
Le radiophone fig. 41

La figure 41 représente le premier dispositif au moyen duquel le rayon lumineux se trouvait actionné par la voix pour reproduire la parole ; la plaque percée de fentes longitudinales se voit en PP, et elle est, comme on le remarque, fixée à la membrane vibrante ll d'un téléphone T. C'est derrière cette plaque PP que se trouve la seconde plaque percée qui doit être fixe. D'après cette disposition, on comprend facilement que si deux plaques sont disposées de manière que les fentes se correspondent à l'état normal, les vibrations de la voix agissant sur le diaphragme, et par suite sur la plaque mobile, devront provoquer des extinctions plus ou moins grandes de la lumière, en rapport avec l'amplitude des ondes sonores.



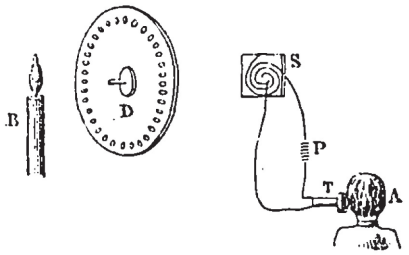
Le radiophone fig. 42

La figure 42 indique comment ce système est disposé pour actionner la plaque de sélénium S en rapport avec le circuit des téléphones. Les deux plaques sont représentées en D vues sur la tranche.



Le radiophone fig. 43

La figure 43 représente le moyen employé par M. Bell pour impressionner par la voix la flamme d'un bec de gaz. Le jeu du système est facile à comprendre par l'inspection de la seule figure.

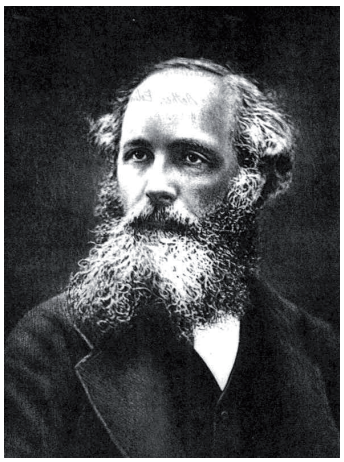


Le radiophone fig. 44

La figure 44 montre la disposition de l'expérience au moyen de laquelle on prouve que la lumière d'une bougie peut produire des sons en agissant sur un système à sélénium. Il suffit, comme on le voit, de placer, entre ce système et la bougie, le disque percé de trous dont nous avons parlé.

Tel est le résumé du premier travail de M. Bell sur la radiophonie, travail déjà bien riche, comme on le voit, en observations curieuses et nouvelles, et qui a provoqué immédiatement l'étude des savants des différents pays sur cette nouvelle branche ouverte à la science.

Ce système avait peu d'avenir en l'état des connaissances de l'époque. Sa portée était limitée, mais l'idée était là : transporter les sons à distance sans fil !



James Clerk Maxwell

Bien que de nombreuses découvertes dans le domaine de l'électricité aient été nécessaires au développement de la radio, celui-ci commença réellement en 1873, avec la publication, par le physicien britannique James Clerk Maxwell (1831-1879) de son « *Traité d'électricité et de magnétisme* ». Par raisonnement mathématique, il établit que toute perturbation électrique donne naissance à des oscillations électromagnétiques de fréquences diverses, non perceptibles par nos sens, qui rayonnent dans l'espace, comme le son, la lumière et la chaleur.

Quelque quinze ans plus tard, le physicien allemand Heinrich Hertz générait, pour la première fois, de telles ondes avec une source électrique. Il chargea électriquement un condensateur, puis le court-circuita à l'aide d'un *éclateur*. Dans la décharge électrique qui s'ensuivit, la quantité de charges électriques déplacées dépassa le point neutre, développant une charge de même valeur et de signe opposé sur les armatures du condensateur, puis ces charges électriques continuèrent de passer par va-et-vient d'une armature à l'autre du condensateur, créant ainsi une décharge élec-

Oscillateur de Hertz et Récepteur Hertzien

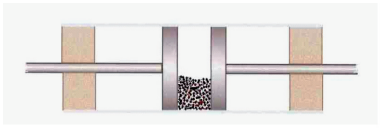
trique oscillatoire apparaissant sous la forme d'une étincelle. Une partie de l'énergie de cette oscillation fut rayonnée par l'éclateur sous forme d'ondes électromagnétiques, que l'on nomma ondes hertziennes.

Heinrich Rudolf Hertz

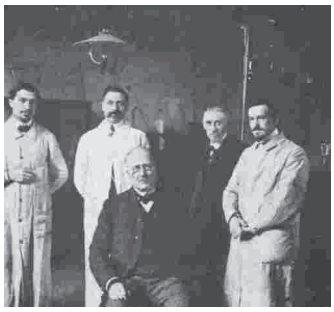
Les travaux de Hertz comprenaient plusieurs montages qui allaient constituer pour longtemps la base technologique du développement de la radio. Son expérience, réalisée en 1887, s'organisait autour des deux éléments fondamentaux d'un système radioélectrique, l'émetteur et le récepteur.

Le premier était constitué d'un générateur d'oscillations de haute fréquence, ou « *excitateur* », dans lequel des étincelles étaient produites par un éclateur à boules. Le second, dénommé alors « *résonateur* », éloigné de plusieurs mètres, permit à Hertz d'observer une étincelle témoignant de l'existence d'oscillations de haute fréquence induites à distance. Il en mesura diverses grandeurs, dont la longueur d'onde et la vitesse de propagation.

Ce fut sur cette base que de multiples éléments vinrent progressivement se greffer pour déboucher sur une utilisation pratique des ondes hertziennes. L'apport du physicien Édouard Branly fut fondamental en ce domaine. En 1890, il réalisa un tube *radioconducteur* à limaille métallique qu'il impressionna jusqu'à 30m avec les ondes produites par un appareillage de Hertz. Ainsi fut réalisé le premier détecteur d'ondes électromagnétiques.



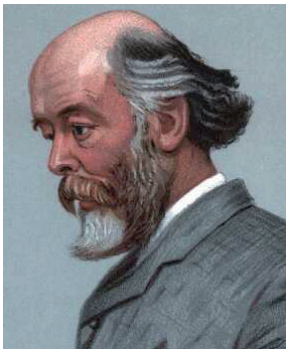
Le « *radioconducteur* » de Branly est constitué d'un tube de verre d'environ 3 mm de diamètre dans lequel sont introduits deux pistons métalliques distants d'environ 1 mm. L'espace disponible est rempli partiellement d'une limaille métallique (fer ou métal inoxydable).



Edouard Branly (assis)

Le dispositif est monté dans un circuit électrique alimenté par une pile de faible voltage. Sous l'effet d'un rayonnement électromagnétique le tube devient conducteur et laisse passer le courant dans le circuit.

Sir Oliver Lodge[41] eut aussi l'idée d'utiliser ce dispositif à l'étude des ondes hertziennes. Les Anglo-saxons disent que la limaille a été « cohérée ». Il faut pour la « décohérer » donner un petit choc sur le tube. De ce fait le tube portera le nom de « coherer » qui sera francisé en « *cohéreur* » malgré les protestations de Branly qui tenait au terme de radioconducteur.



Sir Oliver Lodge

Ce fut l'élément central de tout appareil récepteur de télégraphie sans fil pendant plusieurs années. Aux travaux de Hertz et de Branly, il conviendrait d'ajouter ceux de Nicolas Tesla[42] et d'Alexandre Popov. Ce dernier réalisa la première expérience attestée de « *télégraphie sans fil* », à Saint-Pétersbourg, le 7 mai 1895. Son

[41] Physicien britannique né à Penkhall près de Stoke on Trent (Staffordshire) en 1851, mort à Lake près de Salisbury en 1940. La grande contribution de Sir Oliver Lodge (anobli en 1902) au développement de la TSF est souvent largement passée sous silence. Bien qu'il fut très apprécié de ses pairs, à l'inverse d'un Marconi, il est resté, en pur scientifique qu'il était, éloigné des turbulences médiatiques et son absence de la grande presse fait qu'il est aujourd'hui quasi inconnu du grand public.

[42] Ingénieur américain, né à Smiljan en Croatie le 9/10 juillet 1856 et mort à New York City le 7 janvier 1943. Parmi les nombreuses inventions de Tesla, on peut citer les générateurs à haute fréquence (1890) et la bobine qui porte son nom (1891) et qui a eu des applications importantes dans le domaine des communications radio. Il est considéré comme l'un des principaux pionniers dans le domaine de l'énergie électrique. L'unité appelée Tesla est l'unité (Système international, symbole T). de l'intensité d'un champ magnétique.

apport fondamental à cette histoire du télégraphe fut l'ajout d'une antenne aux systèmes de réception et d'émission, ce qui lui permit des résultats extrêmement encourageants. Il transmit des messages en code Morse et démontra ainsi la portée pratique de l'utilisation des ondes hertziennes. On lui doit également la « *prise de terre* »

Guglielmo Marconi

Guglielmo Marconi, physicien et inventeur italien né à Mazabotta près de Bologne le 24 avril 1874 et mort à Rome le 20 juillet 1937. À l'été 1894, il apprend la mort de Hertz et imagine d'utiliser ses travaux comme moyen de communication sans l'aide de fils. Guglielmo MARCONI a juste 20 ans. Avec son frère Alphondo, il s'installe dans le grenier de la maison familiale et construit un appareillage qui permet de faire tinter une sonnette deux étages plus bas. Il associe bobine de Ruhmkorff, éclateurs, manipulateur télégraphique de Morse, cohéreur de Branly, antennes verticales de Popov pour concevoir un ensemble émetteur/récepteur complet.

Il avait organisé de manière plus rationnelle ces différents éléments, constatant alors le rôle essentiel joué par la prise de terre et révélant l'influence de la hauteur de l'antenne. À quelques mois d'écart, il obtint des résultats très sensiblement supérieurs à ceux de Popov, transmettant ainsi, à la fin de l'année 1895, un message en morse à une distance de 2 400m. L'année suivante, à 22 ans, il propose son invention au Ministère des Postes italien qui ne le prend pas au sérieux. Il faut dire qu'à cette époque, la télégraphie conventionnelle à fils est parfaitement au point en Europe et que des câbles sous-marins relient l'Europe aux États-Unis.

En 1897, il transmit des signaux de la côte jusqu'à un navire situé en mer, à 29 km de là. Le 16 juin 1897, suite à ses premiers succès, il est convié à faire une présentation devant la *Royal Society* sous couvert de son protecteur Sir William Preece. Sir Oliver Lodge assiste à cette présentation. Cette même année, le gouvernement italien informé des succès de Marconi revoit son attitude et l'invite, en juillet, à une démonstration à bord d'un navire militaire le *San Martino*. On peut dire que ce navire sera le premier bateau équipé d'une station de TSF.

Au mois de novembre, Marconi construit sa première station fixe de TSF à Needless sur l'île de Wight. Le 3 juin 1898, il transmet le premier message radio payant entre l'île de Wight et Bornmouth. Son premier client n'est autre que Lord Kelvin qui débourse un penny pour le service !

Il établit entre l'Angleterre et la France une communication commerciale, fonctionnant quel que soit le temps. Le 28 mars 1899, la première liaison télégraphique entre Douvres et Wimereux (50 km) franchissait la Manche avec ce texte : « MR MARCONI ENVOI(E)* A MR BRANLY SES RESPECTUEUX COMPLIMENTS PAR LE TELEGRAPHE SANS FIL A TRAVERS LA MANCHE − CE BEAU RESULTAT ETANT DU EN PARTIE AUX REMARQUABLES TRAVAUX DE MR BRANLY » * (le E n'était pas inscrit sur le message d'origine…)

Mais Marconi, homme de recherches ne s'en tint pas là. Le 12 décembre 1901, avec la collaboration de l'anglais J.A. Fleming[43], il réussit à envoyer un message d'une seule lettre à travers l'océan Atlantique, entre les Cornouailles (émetteur de 10 kW à Poldhu) et Terre-Neuve (Signal Hill) soit 3 400 km.

En France, Eugène Ducretet réalisa avec ses appareils la première émission télégraphique au dessus de la capitale. Le 5 novembre 1898, après quelques mois d'essais, ce fut, entre la tour Eiffel où l'assistait Ernest Roger, et le Panthéon, la première liaison. Ce fut le départ de la télégraphie sans fil en France. Des 4 km entre la tour Eiffel et le Panthéon, on passa vite à 7 km entre le Sacré Cœur et l'église sainte Anne (toujours en novembre 1898). Enfin, en septembre 1899, une liaison maritime de 42 km avait lieu en Bretagne, à cette occasion, Ducretet télégraphia à Tissot : « RETOUR VOYAGE – DITES A MINIS-

[43] En 1904, Sir John Fleming fait breveter une valve électronique qui sera le départ du développement des tubes électroniques utilisés dans les postes de TSF et les équipements de télégraphie militaire.

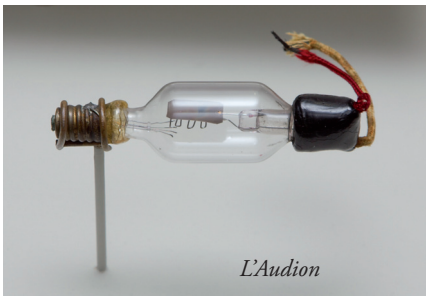
Première émission depuis la tour Eiffel par Ducretet

TRE QUE NOUS FERONS AUSSI BIEN QUE LES ANGLAIS – AVEC CREDITS… AMITIES – DUCRETET », car déjà, il y avait des problèmes de crédits…

À partir de 1902, des messages furent régulièrement envoyés à travers l'Atlantique et, dès 1905, de nombreux bateaux utilisaient la radio pour communiquer avec les stations côtières. Pour son travail de pionnier dans le domaine de la télégraphie sans fil, Marconi partagea, en 1909, le prix Nobel de physique avec le physicien allemand Karl Ferdinand Braun[44].

Pendant cette période, différentes améliorations techniques furent réalisées. Les circuits résonants, constitués d'une impédance et d'un condensateur, furent utilisés pour accorder les appareils. Les antennes furent améliorées, et leurs propriétés directionnelles furent découvertes et utilisées. On employa des transformateurs pour augmenter la tension transmise à l'antenne. D'autres détecteurs furent développés pour remplacer le cohéreur, peu pratique en raison de la nécessité de lui imposer une secousse pour libérer la limaille. On citera le détecteur magnétique, qui utilisait la capacité des ondes radio de démagnétiser les fils d'acier ; un *bolomètre*, mesurant l'augmentation de température d'un fil fin lorsqu'il est traversé par des ondes radio ; la valve de Fleming, le précurseur du tube thermoélectronique ou tube à vide.

Le développement du tube à vide remonte à la découverte par l'inventeur américain Thomas Edison qu'un courant passe entre le filament chaud d'une lampe à incandescence et une autre électrode de cette même lampe, et que ce courant passe dans une seule direction. La valve de Fleming n'était pas foncièrement différente du tube d'Edison. Développée par le physicien britannique John Ambrose Fleming en 1904, ce fut la première des diodes, ou tubes à deux électrodes, à être utilisée dans les matériels radio. Ce tube servit alors de détecteur, de redresseur et de limiteur.



L'Audion

Un progrès révolutionnaire, rendant possible l'avènement de l'électronique, fut réalisé en 1906, lorsque l'inventeur américain Lee De Forest monta un troisième élément, la grille, entre le filament et la cathode d'un tube à vide. Le tube de De Forest[45], qu'il nomma « *audion* » mais que l'on désigne de nos jours sous l'appellation de triode (tube à trois électrodes), ne fut d'abord utilisé que comme détecteur, mais ses possibilités comme amplificateur et comme oscillateur furent rapidement découvertes, et lui donnèrent un rôle décisif. Historiquement, les développements de la radio et de l'électronique furent toujours liés.

[44] Karl Ferdinand Braun (1850-1918) est né en 1850 à Fulda dans le centre de l'Allemagne. Il se lance en 1898 dans le bouillonnement en cours sur la transmission sans fil (TSF). À cette époque, les dispositifs radio de Guglielmo Marconi ont une portée limitée à 15 km, insuffisante pour des applications pratiques. Dans ces radios, sans amplificateur, l'antenne est une partie intégrante du circuit d'accord. Utilisant ses connaissances en physique, Braun sépare l'antenne du circuit d'accord en utilisant entre eux un couplage inductif. Il supprime ainsi l'étincelle des circuits limitant les pertes d'énergie et augmentant la sensibilité. Il brevette (en 1899) son système, qui lui permet de couvrir à Cuxhaven une distance de 62 km. En 1906, il utilisa sa connaissance des propriétés de conduction de la galène pour imaginer un redresseur, que l'on peut considérer comme l'ancêtre de la diode moderne, qui permit l'essor du poste à galène.

[45] Né à Council Bluffs (Iowa) le 26 août 1873, mort à Hollywood le 30 juin 1961. Il était le fils d'un ministre protestant flamboyant. Ingénieur américain, docteur es science en 1899. Il dirige le laboratoire de radio-électricité de la *Western Electric Co* à Chicago. L'invention de l'Audion resta à l'époque complètement inconnue et l'inventeur fut même mis un temps en prison pour dettes à la suite de nombreux procès qui lui coûtèrent beaucoup d'argent.

Reginald Fessenden, Inventeur et physicien canadien est né le 6 octobre 1866 à East Bolton - petit village aujourd'hui nommé Austin - dans une région rurale près de Sherbrooke au Québec et mort aux Bermudes le 22 juillet 1932. Il est convaincu que la voix ne pourra être transportée au travers de l'éther qu'à l'aide d'ondes entretenues et que les émetteurs de l'époque à ondes amorties de type Marconi ne sont pas adaptés pour cet usage. Il va donc chercher à mettre au point des appareils capables de générer des ondes entretenues de fréquence haute. Ancien collaborateur d'Edison, il a l'idée de superposer des ondes vibrant aux fréquences du son à une fréquence radio pour en moduler l'amplitude. Il invente un détecteur radio assez sensible pour être utilisé en radiotéléphonie. Il rencontre Georges Westinghouse et invente un émetteur à éclateur rotatif (*rotary spark gap*). En 1900, il imagine un système d'envoi de signaux télégraphiques à courant alternatif qui séduit le *Weather Bureau* de Washington. Il est embauché et nommé télégraphiste en chef à Cobb Island, au milieu du Potomac, près de Washington. C'est là qu'il réalisera ses plus géniales inventions. Le 23 décembre 1900, il fait un essai de modulation d'une onde à Haute Fréquence avec un micro et transmet depuis Cobb Island, le message suivant à son collaborateur : « *un, deux, trois, quatre ..... neige-t-il où vous êtes M. Thiessen ? S'il en est ainsi, rappelez-moi par téléphone* ». M. Thiessen ne tarda pas à confirmer qu'il avait bien reçu le message sur son récepteur radio. La radiophonie était née.

On peut ainsi dire que sa voix est sans doute la première voix qui a traversé l'éther pour être entendue par d'autres hommes.

Les propriétés de l'audion furent progressivement mises au jour dans les années précédant la Première Guerre mondiale. Ce fut l'Allemand Alexandre Meissner qui le premier déposa, en 1913, un brevet couvrant la production d'oscillations par un composant électronique. En 1912, les propriétés de redressement des cristaux découvertes par l'Américain Greenleaf Whittier et le circuit régénérateur mis au point par l'ingénieur électricien américain Edwin Howard Armstrong Pickard permirent d'améliorer encore les matériels commercialisés. Dès 1915, la téléphonie sans fil avait progressé à un point tel qu'une communication fut établie entre la Virginie et Hawaii et entre la Virginie et Paris.

La meilleure compréhension des modes de transmission des ondes constitua un autre élément décisif de progrès. En 1902, l'ingénieur électricien américain Arthur Edwin Kennelly et le physicien britannique Oliver Heaviside (de façon indépendante et presque simultanément) annoncèrent l'existence probable d'une couche de gaz ionisés à haute altitude dans l'atmosphère, affectant la propagation des ondes radioélectriques. Cette couche, autrefois nommée couche de Heaviside, ou de Kennelly-Heaviside, est l'une des nombreuses couches constituant l'ionosphère. Bien que l'ionosphère soit transparente aux longueurs d'ondes radio les plus courtes, elle réfracte ou réfléchit les longueurs d'onde plus importantes. Du fait de cette réflexion, les ondes radioélectriques peuvent se propager bien au-delà de l'horizon.

La propagation des ondes radio dans l'ionosphère varie fortement suivant l'heure, la saison et l'activité des taches solaires. De légères variations de la nature et de l'altitude de l'ionosphère peuvent survenir en un court laps de temps et affecter la qualité d'une réception à longue distance. L'ionosphère est également responsable du phénomène de rebond, qui se traduit par une réception à grande distance d'un signal alors que celui-ci ne peut être reçu à une distance moindre de l'émetteur. Ce phénomène se produit lorsque l'onde de sol est absorbée par les terrains de la zone intermédiaire, alors que l'onde de ciel, se propageant par réflexion sur l'ionosphère, n'est pas réfléchie selon un angle suffisamment aigu pour pouvoir être reçue à proximité de l'antenne.

Émission radio à ondes courtes.

Bien que certaines parties des différentes bandes de fréquences radio — grandes ondes, ondes moyennes, ondes courtes, très hautes fréquences et ultra hautes fréquences — soient affectées à divers usages, le terme émission radio à ondes courtes désigne en général les transmissions radio dans le domaine des

hautes fréquences (3 à 30 MHz) sur de longues distances, en particulier pour les communications internationales. Toutefois, la communication par micro-ondes, par l'intermédiaire de satellites de communication fournit désormais des signaux d'une fiabilité supérieure et exempts d'erreur.

Les radioamateurs se sont vus attribuer des fréquences dans la bande des ondes courtes, mais on leur en affecte également dans celles des ondes moyennes, des très hautes fréquences et des ultras hautes fréquences. Certaines de ces fréquences font l'objet de restrictions afin de les rendre disponibles au plus grand nombre d'utilisateurs.

Les radioamateurs ont réalisé des prouesses spectaculaires, comme le premier contact radio transatlantique (1921) sur ondes courtes, domaine délaissé par les professionnels, mais qui se révéla décisif pour le développement de la radiotéléphonie commerciale intercontinentale. Au fil des décennies, les associations jouèrent un rôle de plus en plus important au point de mettre en orbite un certain nombre de satellites, placés sur des lanceurs programmés pour des tirs officiels par les États-Unis, l'Union soviétique et l'Agence spatiale européenne. Ces satellites sont d'habitude appelés Oscar (*Orbiting Satellites Carrying Amateur Radio* : satellites en orbite porteurs de radio amateur). Le premier, Oscar 1, mis en orbite en 1961, fut également le premier satellite non étatique. Le quatrième fut lancé en 1965 et assura les premières communications directes par satellite entre les États-Unis et l'Union soviétique. Au début des années 1980, il y avait plus de 1,5 million de radioamateurs licenciés dans le monde, y compris les opérateurs radio de la *citizen band*[46].

La radio d'aujourd'hui.

Des progrès immenses dans la technologie de la radiocommunication furent réalisés après la Seconde Guerre mondiale et contribuèrent à rendre possible l'exploration de l'espace, dont la plus formidable démonstration fut sans doute donnée lors des missions d'alunissage Apollo (1969-1972). Des équipements sophistiqués de transmission et de réception furent intégrés dans le système de communication compact, à très haute fréquence, embarqué sur les modules de commande et les modules lunaires. Le système exécutait simultanément les fonctions de transmission de la voix et de télémétrie, en calculant la distance entre les deux véhicules par mesure du laps de temps entre l'émission de tonalités et la réception des signaux de retour. Les signaux vocaux des astronautes étaient également transmis simultanément dans le monde entier par un réseau de communications. Le système récent de radio cellulaire est une version miniature des grands réseaux radio.

Chez un « radio-amateur » dans les années 1930. Musée Européen de la Communication, Pignerolle - 49)

[46] La *citizen band* ou CB (de l'anglais, bande des citoyens) est une bande de fréquence allouée au trafic radio et ouverte à tous. En français, le sigle CB, qui a parfois été traduit par canaux banalisés, se prononce toujours « *cibi* », à l'anglaise. Par extension, le mot CB désigne également les émetteurs radio émettant sur la bande CB, et l'on appelle les utilisateurs les *cibistes*.

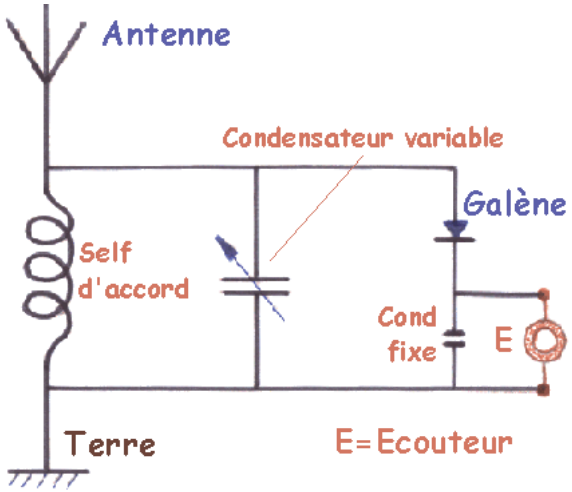


Schéma d'un poste à galène

Poste à galène Duvivier

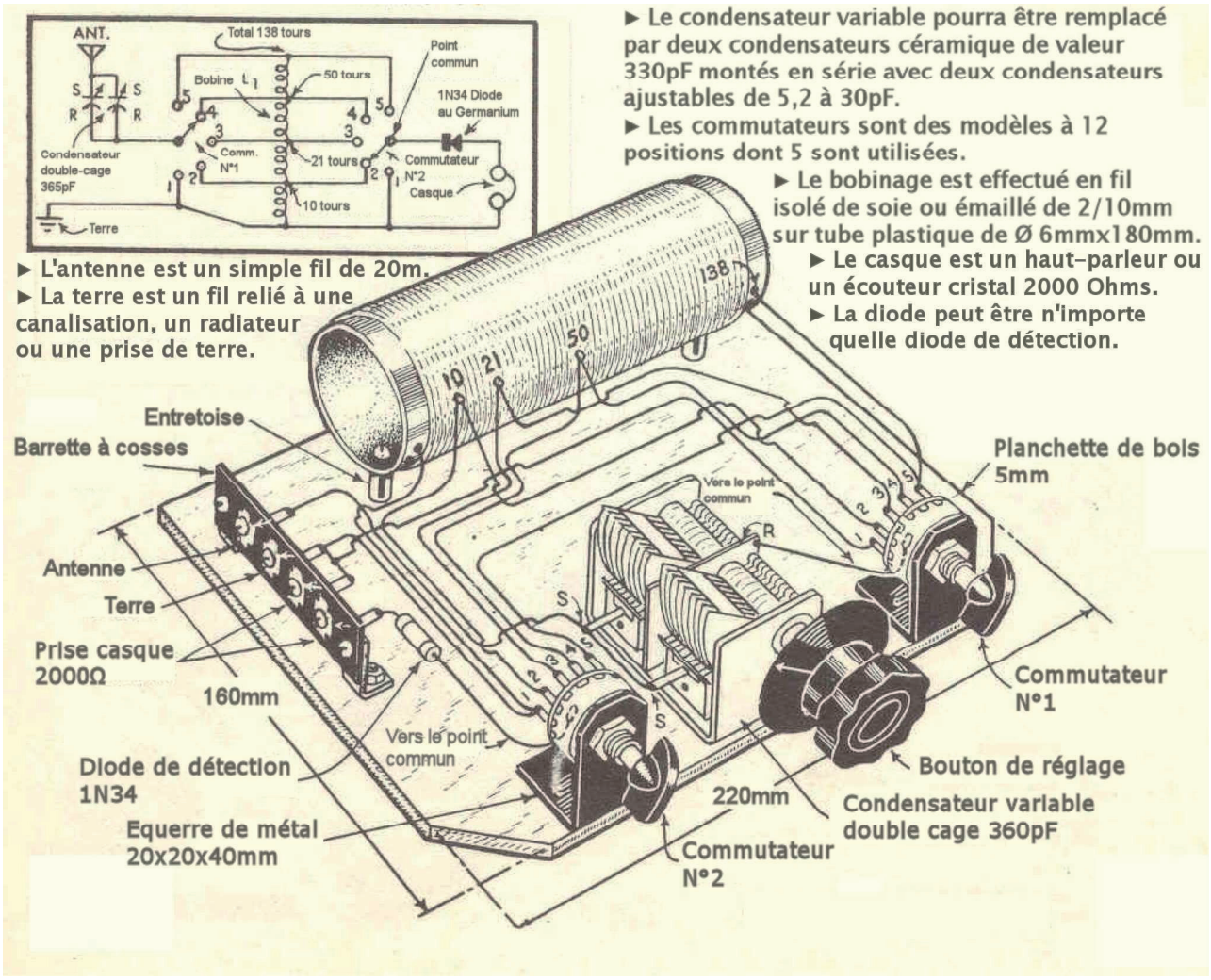


Schéma d'un récepteur simple à une diode de détection (fonctionne sans courant !)

La révolution numérique

En France, à partir de 1970, la technique dite numérique a été introduite dans les centraux téléphoniques et les systèmes de transmission sur câbles puis sur faisceaux hertziens (liaisons radioélectriques à très hautes fréquences) pour remplacer progressivement la technique analogique. Dans cette nouvelle technique, le signal à transmettre est d'abord converti en une succession de nombres binaires (composés de 0 et de 1) qui représentent les variations d'amplitude du signal dans le temps (en fractions de volts, par exemple). Ces nombres sont à leur tour symbolisés par des signaux électriques à nombre fini d'états possibles (bits), qui s'enchaînent suffisamment rapidement (8 000 nombres par seconde dans le cas de la liaison téléphonique) pour permettre une reconstitution satisfaisante (décodage) à l'extrémité réceptrice.

Les signaux ainsi transmis par ce système sont beaucoup plus résistants aux dégradations éventuelles provenant des bruits de circuit, des parasites électriques, des distorsions de non-linéarité ou des variations de l'affaiblissement en fonction de la fréquence. En pratique, les imperfections de transmission se traduisent par un taux d'erreurs généralement très faible sur les éléments binaires. Les signaux téléphoniques sont alors restitués sans dégradation notable, le délai de propagation demeurant le seul inconvénient éventuel. L'avantage provient aussi de ce qu'il devient possible de tirer le meilleur parti des ressources de la microélectronique dans les équipements.

Le Réseau numérique à intégration de services (*R.N.I.S. de France Télécom*), appelé depuis 1987 réseau Numéris et dont nous avons déjà parlé plus haut, est à la fois un prolongement du réseau téléphonique commuté public et une amélioration de sa nature et de l'étendue de ses services. Ses concepts, son architecture fonctionnelle ainsi que ses caractéristiques techniques ont fait l'objet d'une concertation internationale, notamment en Europe, afin d'assurer la meilleure cohérence possible dans le but de constituer un réseau mondial.

Avant l'existence du R.N.I.S. et sauf exceptions, la méthode numérique était uniquement réservée aux centraux téléphoniques appelés commutateurs et à leurs interconnexions. La proportion d'équipements numériques en France (tant en ce qui concerne les commutations interurbaines et locales que les circuits de transmission pour les liaisons interurbaines et locales), supérieure à 50 % avant 1985, dépassait 80 % en 1990 et a presque atteint 100 % peu après 1995. Les commutateurs privés existant dans le milieu professionnel ont également bénéficié de cette numérisation.

Les deux dernières décennies du XX^{e} siècle ont donc été marquées par un bouleversement profond de l'ensemble des moyens de communiquer à distance, dont il n'est pas inutile de rappeler les principales étapes, avant de présenter la nouvelle panoplie des services qui sont offerts à l'utilisateur, privé ou professionnel, et d'anticiper quelques évolutions vraisemblables.

Rappel historique

En 1980, la France, qui avait, en ce qui concerne les équipements téléphoniques, presque rattrapé son retard sur les autres pays industriels, avait su prendre une avance technologique en matière de réseaux : les centraux téléphoniques neufs étaient tous à commutation électronique, les circuits de transmission étaient en voie d'être pour la plupart réalisés selon les techniques numériques, plus propices à la miniaturisation et à une protection des signaux à l'égard des dégradations jusqu'alors inévitables : bruit de fond, diaphonie, distorsions, limitations de la bande de fréquences transmises, échos, etc.

Pour l'« *abonné au téléphone* », catégorie fortement majoritaire d'utilisateurs des moyens de télécommunication, les bénéfices sont sensibles : la qualité du service s'améliore et, surtout, sa disponibilité n'est plus aléatoire.

Le réseau Transpac (réseau à commutation de paquets de données, en d'autres termes le « *téléphone des ordinateurs* »), réalisation d'avant-garde, est lancé, mais encore peu développé. Le réseau et le service

télex de transmission de données alphanumériques à basse vitesse sont largement utilisés dans l'activité économique, notamment pour les échanges internationaux. Le télécopieur, ou fax, qui vient d'être inventé, est cependant encore inconnu du public, d'autant que le prix des premières machines est élevé et que leur fiabilité est médiocre. Le Minitel sort des laboratoires et n'a pas même abordé sa phase critique d'« *accouchement sociologique* » : la controverse avec les autres médias, en premier lieu avec la presse.

On est encore en pleine phase technologique, dont l'apogée sera marqué par le lancement de satellites français de télécommunication (*Télécom-1A* et *Télécom-1B* sont mis sur orbite en août 1984 et en mai 1985, respectivement) et la gestation d'un vaste projet global, dans ses intentions au moins : le Réseau numérique à intégration de services (R.N.I.S.) ; en témoigne notamment un ouvrage collectif réalisé alors par la Direction générale des télécommunications du ministère des P.T.T. : *Les Télécommunications françaises* (1982), consacré aux télécommunications, où les propos traitant d'autres services que le téléphone représentent moins de 4% du total des pages !

Dans les autres pays industriels, l'évolution est comparable, voire un peu plus lente, mis à part les satellites et le radiotéléphone, plus rapidement apparu et, surtout, diffusé dans les pays nordiques et anglo-saxons.

Alors que la technologie est en évolution constante, les années 1980 vont connaître une série de mutations d'importance :

– diversification des modes de télécommunication possible, étant entendu que l'on donne au vocable « télécommunication » le sens d'une transmission (quasi) immédiate du message de l'émetteur vers le destinataire, avec ou sans mise en relation « conversationnelle », et sans transport physique (de type postal, par exemple) du support matériel du message en question ;

– émergence des réseaux multiservices ;

– apparition et spécialisation des moyens de télécommunication à l'usage des professionnels (entreprises, organisations de toutes sortes) ;

– mondialisation des possibilités offertes.

Ces mutations, alliées à une interpénétration progressive avec le monde de l'informatique et à un abaissement constant des coûts d'usage induit par les progrès technologiques, ont façonné un domaine désormais très diversifié, de haute technicité, où il devient parfois délicat de se repérer, d'exprimer et de faire comprendre en termes simples les possibilités réellement offertes à l'utilisateur courant, au-delà du discours des professionnels.

Au milieu des années 1990, le taux d'équipement téléphonique dépassait cinquante lignes pour cent habitants en France, où plus de 95% des foyers en étaient équipés (notons que ce taux est pratiquement égal à celui des États-Unis). Mais le service téléphonique est également devenu accessible dans les lieux publics, et sur la voie publique, où l'emploi de la télécarte de paiement a permis de prévenir efficacement les actes de malveillance à l'encontre des appareils publics.

Le téléphone est aussi devenu couramment accessible dans les moyens de transport particuliers (radiotéléphone de voiture) et de transport en commun : trains, avions commerciaux (la liaison radioélectrique étant dans ce dernier cas assurée par satellite et non pas par un réseau terrestre).

En Europe, l'adoption d'une norme commune de radiocommunications mobiles numériques (G.S.M., *global system for mobiles*) autorise l'emploi du même équipement dans des pays différents. De plus, comme pour le téléphone fixe, les appareils modernes offrent des ressources supplémentaires : accès aux services télématiques – avec un terminal Minitel portable –, à la télécopie et à la communication de données.

Dernière en date des variantes d'accès : le téléphone portable personnel de type *Bi-Bop*. Techniquement, il s'agit d'un radiotéléphone, mais il ne peut fonctionner que dans le voisinage immédiat (quelques dizaines de mètres) de radioémetteurs (« bornes ») de faibles puissances reliés au réseau téléphonique

général. Un premier avantage réside dans le faible encombrement de l'appareil individuel (format de poche), qui se prête ainsi à un usage polyvalent :

– en fournissant le moyen de téléphoner au cours de déplacements (au lieu d'utiliser des appareils publics ou les radiotéléphones de voiture) ; mais on ne peut être appelé que sous certaines conditions ;

– en servant de terminal téléphonique personnel dans les locaux d'une entreprise, une fois ceux-ci équipés d'un radioémetteur du type évoqué ci-dessus, relié au réseau téléphonique interne de celle-ci ; ce système de communication personnel est plus efficace que les systèmes antérieurs d'appel de personnes ou de radiomessagerie.

Autres modes de communication utilisant l'infrastructure du réseau téléphonique

S'il comporte des limitations pour la transmission des signaux (bande de fréquences transmises limitée à 3 000 hertz environ, bruit de fond, distorsions, etc.), le réseau téléphonique présente l'avantage de sa facilité d'accès et d'utilisation pour les procédés pouvant s'accommoder de ses caractéristiques. Trois d'entre eux sont devenus d'usage courant – la télécopie, le vidéotex et la télématique vocale –, mais certains sont encore peu connus.

La télécopie

En quelques années, la diffusion de la télécopie a dépassé celle du télex (le parc français de télécopieurs, inférieur à 40 000 exemplaires en 1985, en comptait plus d'un million en 1993), en raison d'avantages propres : facilité d'emploi par des personnes non spécialisées, faible coût de transmission d'un document (même coût que celui d'une conversation téléphonique de durée identique), reproduction de l'écriture manuscrite et des dessins, voire des photographies. La qualité de reproduction des documents est en effet en amélioration constante et permet notamment la consultation à distance de services documentaires comportant des images dont la précision est essentielle. La définition obtenue peut atteindre alors un seizième de millimètre, au lieu d'un quart de millimètre ordinairement.

La modulation des signaux nécessaires à la télécopie est de type numérique. Or la vitesse de transmission des données sur le réseau téléphonique a progressé de manière sensible, atteignant couramment 9 600 bits par seconde, au lieu de 2 400 quelques années auparavant. La limite théorique se situant au-delà de 20 000 bits par seconde, les améliorations de la qualité des documents transmis par télécopie ne se traduiront pas nécessairement par un allongement des durées de transmission, typiquement inférieures à une minute par page de format courant (A4). C'est a fortiori le cas si l'on utilise un R.N.I.S., dont chaque canal numérique offre un débit de 64 000 bits par seconde.

Le vidéotex

Le terminal à écran et clavier Minitel est bien connu en France, en 1992, le réseau desservait 6 millions de terminaux, pour un trafic annuel de 105 millions d'heures, vers 17 200 codes d'accès ; certains pays étrangers ont progressivement adopté des équivalents du Minitel.

L'annuaire électronique public est le plus consulté des services auxquels il permet l'accès, et dont il est devenu impossible de donner une énumération, leur nombre s'exprimant en dizaines de milliers. On peut toutefois les classer en quelques catégories types :

– les services d'information, y compris de type « presse », accessibles au public, ou de type privé (accès conditionnels par abonnement, codes d'accès, etc.) ;

– les services de messagerie selon divers modes (échanges de messages de personne à personne, diffusion simultanée à des destinataires multiples, ou recueil d'informations ou d'avis émanant d'un grand nombre de personnes, etc.) ;

– les services transactionnels (réservations de titres de transport, de billets de spectacles, etc. ; commandes sur catalogues ; opérations de type « banque à domicile », y compris des virements et des versements, etc.) ;

– des combinaisons des types précédents ; au cours de la même communication, par exemple, une transaction peut succéder à une recherche d'informations (commande après demande de prix ; réservation après obtention de renseignements sur les horaires de transports, etc.) ;

– des jeux.

La lenteur de la modulation initiale – 1 200 bits par seconde – des signaux du système télétel, réseau du vidéotex de *France Télécom*, est impropre à la transmission d'images photographiques, sauf si des temps de transmission élevés sont acceptables. L'augmentation de cette vitesse, déjà signalée, conduit cependant à des services vidéotex plus riches et d'un accès plus rapide, grâce à la nouvelle gamme de possibilités fondée sur les performances du R.N.I.S.

La télématique vocale

Au lieu d'accéder à un service par le clavier d'un Minitel, les informations en retour s'affichant sur l'écran, les touches de l'appareil téléphonique permettent la connexion à l'ordinateur contenant les informations recherchées. Celui-ci interprète les demandes préalablement codées par pression sur les touches en question, puis fournit des réponses vocales intelligibles pour le demandeur, par imitation de l'élocution d'une personne.

Dans certaines variantes, les questions peuvent même être formulées verbalement, l'ordinateur étant doté d'une certaine capacité de reconnaissance de la parole humaine.

La téléaction

Pour identifier ou modifier à distance une situation type, parmi un ensemble limité de possibilités, ou détecter l'occurrence d'un événement caractérisable et prévisible, il peut suffire de transmettre très momentanément une quantité relativement faible de signaux. Mais les conséquences éventuelles d'un dysfonctionnement exigent en contrepartie une grande sécurité de la liaison, sa quasi-permanence, et la rapidité de la transmission.

Pour répondre économiquement à ce type de besoin, des équipements permettent aussi d'utiliser les infrastructures du réseau téléphonique sans pour autant nécessiter une liaison téléphonique permanente, ni même perturber les communications téléphoniques sur le trajet qu'elles empruntent, ni mettre en œuvre des liaisons louées fixes. France Télécom a ouvert commercialement un service de ce type en 1990, sous l'appellation *Transveil*. Ce service permet la surveillance éloignée d'installations à haut risque ou de systèmes dont les défaillances doivent être immédiatement détectées et éliminées, ou encore la commande à distance d'organes mécaniques, en des lieux non pourvus de personnel permanent, etc.

Échanges électroniques de documents. Courrier électronique

Les types de symboles auxquels il est fait appel dans les processus de communication humains sont en nombre restreint, cinq au plus : les symboles sonores (parole), les textes au sens large (ensembles ordonnés de caractères alphanumériques), les images fixes, les images animées (documents de type cinématographique) et les symboles monétaires.

Le texte présente des caractéristiques qui en ont fait un mode privilégié de support des messages : précision de l'expression, permanence, asynchronisme de l'émetteur et du récepteur, facilité de reproduction, économie de moyens techniques, le codage et la transmission se réduisant à ceux d'un nombre restreint de caractères. Il a constitué pendant des siècles, grâce au service postal, le principal moyen de communiquer à distance.

Il demeure essentiel. Mais le support traditionnel en papier présente plusieurs inconvénients ; en particulier, il entraîne une difficulté d'accès, du fait de la grande masse de documents disponibles ou créés, et il requiert un transport matériel dont la durée conditionne le rythme des échanges.

En substituant un support électronique au papier, ces inconvénients sont levés, au prix de la nécessité de dispositifs de présentation (imprimante ou écran). La durée du « transport » devient négligeable, l'accès à une masse de documents est facilité. Avantage supplémentaire quand les textes sont enregistrés dans des mémoires électroniques modifiables : si une partie d'un texte doit être modifiée, nul besoin de le récrire entièrement ; seuls les éléments à modifier doivent être traités, d'où une meilleure productivité des personnes intervenant pour ces modifications. D'où également le succès croissant du courrier électronique, aux variantes multiples.

Le *télex*, forme la plus ancienne encore utilisée, présente désormais des inconvénients provoquant un ralentissement de son utilisation : lenteur de la transmission et, surtout, forte limitation dans la variété des caractères utilisables. Répondant néanmoins à une norme mondiale unique, il reste largement utilisé pour les télécommunications internationales.

Le *télétex*, développé en France et en Allemagne, tendait à supprimer les inconvénients du télex, par un alphabet beaucoup plus riche (308 caractères, soit six fois plus que celui du télex) et une cadence de transmission considérablement accrue (d'un facteur cinquante environ : 2 400 bits au lieu de 50). En contrepartie, il nécessitait un poste de travail réservé à cet usage – une machine à écrire de type particulier –, ce qui en a limité l'intérêt et la diffusion, compte tenu de l'apparition de la micro-informatique à usages polyvalents. En France, le service télétex a été interrompu à la fin de 1992.

Ce procédé n'en offrait pas moins de puissantes ressources de communication pour l'échange de correspondance de type texte : facilité de mise en œuvre, utilisation indifférente du réseau téléphonique ou des réseaux informatiques conformes à la norme X25 du Comité consultatif international télégraphique et téléphonique (C.C.I.T.T.), normalisation internationale, qualité, sécurité, rapidité et faible coût de la transmission.

Avec le télex, la télécopie, le télétex, les messages parviennent à l'équipement terminal du destinataire au moment même de leur émission par celui de l'expéditeur, c'est-à-dire de manière pratiquement instantanée. Une messagerie électronique introduit en revanche un dispositif intermédiaire, dit boîte à lettres, où le message est enregistré et tenu à la disposition du destinataire jusqu'à ce qu'il en prenne connaissance, à l'aide d'un code d'accès assurant qu'il est seul à pouvoir le faire.

Cette organisation présente de nombreux avantages, en particulier la désynchronisation de l'émission et de la réception des messages – l'émetteur peut transmettre des messages au(x) destinataire(s) en l'absence de celui(ceux)-ci –, ainsi que la possibilité d'introduire une « valeur ajoutée » par le système de messagerie, par exemple la transmission d'un même message à plusieurs destinataires désignés par l'émetteur, l'authentification de l'origine du message, la conversion d'un message provenant d'un type d'équipement d'émission pour en permettre la réception sur un équipement d'un type différent (ainsi, d'un Minitel vers un télex, ou d'un télétex vers un télécopieur).

Une norme a été adoptée internationalement pour les messageries (elle porte la référence X400 du C.C.I.T.T.). La conformité à celle-ci assure la possibilité d'effectuer les conversions de codes nécessaires pour permettre les échanges entre terminaux de types différents, et pour interconnecter les messageries entre elles, en vue d'acheminer les messages entre abonnés de messageries différentes, ou raccordés à des réseaux de communication différents, par exemple d'un pays à un autre.

Une messagerie publique de ce type existe en France ; elle est commercialisée par la filiale Transpac du groupe France Télécom, sous l'appellation *Atlas 400.*

Informatique et télécommunications

Du point de vue fonctionnel, un ordinateur n'est pas autre chose qu'un outil capable de traiter des symboles créés par l'homme, selon des règles, variables, définies par l'utilisateur et représentatives de sa propre démarche mentale. Il s'agit donc bien d'une machine à communiquer, en particulier quand les personnes qui entrent les données ne sont pas les mêmes que celles qui exploitent les résultats.

Les ressources de télécommunication répondent aux besoins les plus variés d'échanges de données vers, en provenance, ou entre des ordinateurs. Des techniques spécifiques ont été développées, permettant d'atteindre des vitesses de transmission de plusieurs millions de caractères (octets) par seconde, la plupart des besoins se situant toutefois en deçà de 250 000 caractères par seconde.

Une partie des échanges emprunte des liaisons fixes terrestres, louées aux exploitants de télécommunication, reliant par exemple des établissements éloignés d'une même entreprise. Le coût en étant élevé pour les faibles trafics, il est possible de faire appel aux réseaux publics à commutation Transpac (purement téléinformatique) ou Numéris, selon les types d'usage.

Bien que la radiotéléphonie soit en principe utilisable pour la téléinformatique, l'emploi optimal de ce type de liaison a conduit à constituer des réseaux radioélectriques réservés aux échanges de données (3RD), en particulier pour des utilisateurs en déplacement.

De ce fait, le choix du moyen de transmission est pour l'utilisateur essentiellement dépendant du coût, car l'informatique possède, à la différence du téléphone, une grande flexibilité à l'égard de la cadence de transmission et du non-synchronisme entre l'émission et la réception.

Micro-ordinateurs et communication

Le micro-ordinateur rassemble les ressources :

– d'un ordinateur proprement dit, avec sa puissance de calcul et de traitement de symboles, sa capacité d'enregistrer des volumes importants de signes (plusieurs dizaines de millions, le plus fréquemment), ses accessoires (matériels et logiciels) nécessaires à la connexion à un réseau de télécommunication ;

– d'un terminal informatique connectable à un gros ordinateur, doté de surcroît de mémoire et d'une certaine « intelligence » ;

– d'une « super »-machine à écrire, offrant des possibilités de composer, de consulter ou de modifier des documents non seulement textuels alphanumériques, mais également des dessins, des diagrammes, et même des images de type photographique.

Il ne nécessite pas impérativement une imprimante, puisqu'il peut opérer à partir de supports magnétiques, où la densité d'information est très supérieure à celle des supports de papier.

De plus, des techniques permettent de compléter ces ressources par des possibilités audiovisuelles :

– enregistrement et reproduction de brèves séquences sonores (paroles ou toute autre forme de sons) et vidéographiques (images animées) ;

– codage et décodage pour l'échange instantané de ces types de documents à travers un réseau (numérique) de télécommunication, faisant alors de la machine un terminal téléphonique ou visiophonique.

Cet appareil devient ainsi un terminal universel de communication, soit en temps réel (conversation téléphonique), soit en temps différé (messagerie), soit avec traitement de l'information elle-même (informatique). L'usage des micro-ordinateurs connaît ainsi un fort développement, d'autant que leur prix décroît constamment et que leur commodité est sans cesse améliorée, réduisant l'initiation nécessaire à leur maîtrise et facilitant leur emploi par une population étendue.

Un mode de communication consiste à transporter les supports des documents (par exemple, sous la forme de disquettes) d'une machine vers une ou plusieurs autres.

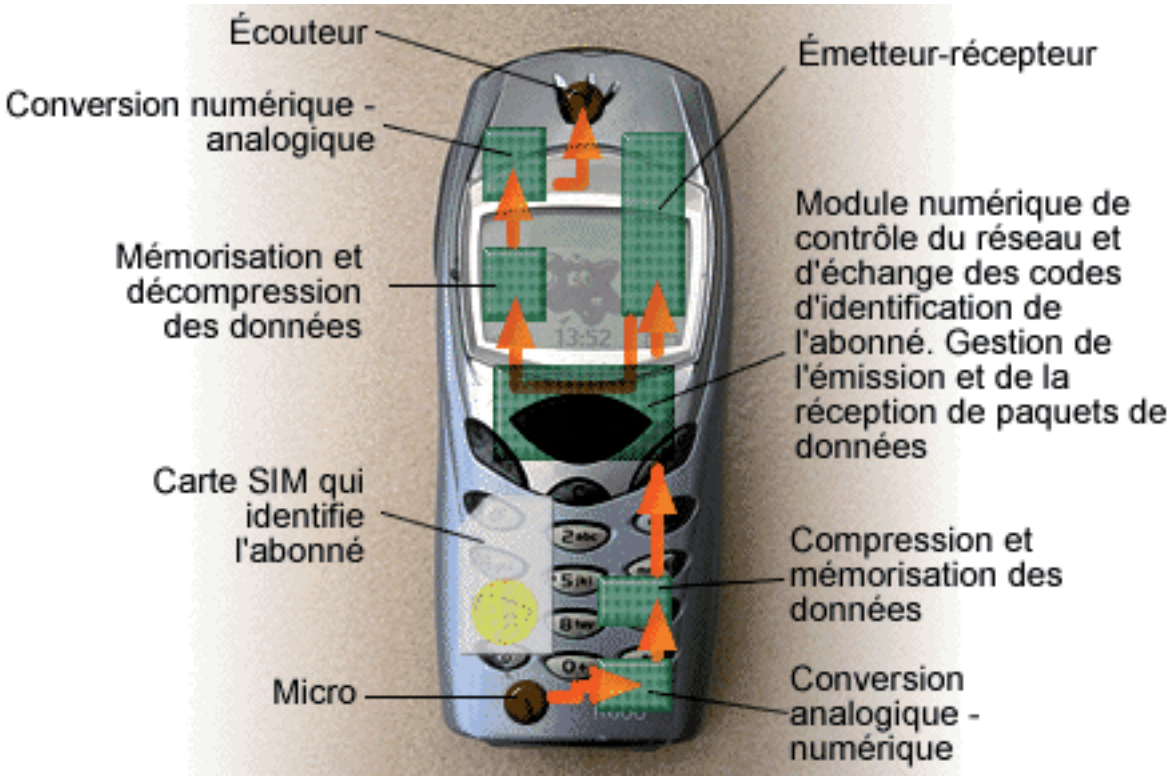
Depuis le début des années 1980, des réseaux locaux de micro-ordinateurs ont été mis en œuvre, qui permettent la communication entre les machines situées dans un même bâtiment ou établissement, sur des distances maximales de l'ordre d'une centaine de mètres.

La communication à des distances quelconques est aussi devenue possible, y compris entre des pays différents, en empruntant les ressources des réseaux publics et internationaux (liaisons louées, réseaux à commutation de circuits ou de « paquets » de données), dont le choix dépend du type de besoin et du coût.

Des difficultés subsistent encore néanmoins pour l'établissement de communications entre micro-ordinateurs : il s'agit de la non-compatibilité entre machines de conceptions différentes ou entre logiciels d'application ou de communication. Les machines ne « parlent » alors pas la même langue, et la difficulté est multiple : différences de syntaxe, de vocabulaire, de concepts et même d'alphabet.

Des choix d'équipements compatibles permettent cependant la réalisation de vastes ensembles communicants. Par ailleurs, des normes communes se dégagent progressivement, de même que des ressources de « traduction » deviennent disponibles et autorisent des intercommunications de plus en plus aisées entre domaines homogènes différents. La condition pour qu'il y soit fait massivement appel reste la simplicité de mise en œuvre par les utilisateurs, l'idéal étant non seulement qu'il ne soit pas nécessaire pour eux d'être rompus aux techniques de la micro-informatique, mais que ces opérations s'effectuent automatiquement et à leur insu.

Antennes relais GSM



Intérieur d'un téléphone mobile

L'histoire du téléphone portable

La création du téléphone « mobile »

Contrairement au téléphone filaire, son aîné, on ne peut pas conférer au téléphone mobile le statut d'invention. En effet, même si la paternité est généralement attribuée à Motorola, il s'agit plus de l'association de plusieurs techniques que d'une réelle invention.

Depuis longtemps, les communications vocales par ondes radioélectriques étaient possibles grâce aux découvertes de Maxwell, aux techniques de Marconi, et à l'invention du tube électronique par Lee de Forest. Cependant, l'une des différences majeures par rapport au téléphone était le mode de fonctionnement : chaque interlocuteur devait attendre son tour pour parler (fonctionnement type *talkie walkie*). Ce mode, appelé alternat, rendait les communications austères. Il fallut attendre l'arrivée d'un composant spécial, un filtre dit duplexeur pour rendre possible l'émission et la réception simultanée dans une bande de fréquence identique. Dès lors, il était possible de concevoir des équipements « transportables », libérant ainsi le téléphone de son fil historique.

Cependant, deux problèmes restèrent insolubles jusqu'à assez récemment. L'énergie nécessaire pour émettre était importante, et donc rendait illusoire l'utilisation sur piles. De plus, l'antenne devait mesurer plus d'un mètre. Difficile d'imaginer loger une batterie de véhicule et l'antenne dans une mallette... Ces raisons ont contraint le téléphone mobile à trouver refuge dans les véhicules, seuls capables d'héberger le système radio, de fournir l'énergie et la base de l'imposante antenne « fouet ». Le téléphone de voiture était né...

Le téléphone de voiture en France.

Le premier réseau commercial en France voit le jour en 1956. Il s'agit d'un réseau manuel, nécessitant l'intervention d'une opératrice. Le téléphone est très dépouillé : un combiné de type U43 repose sur une base, laquelle comprend un interrupteur de mise en service, et deux voyants, un vert, et un rouge. Le réseau fonctionne dans la bande des 150 MHz sur une fréquence unique. Lorsqu'un abonné « prend la ligne », tous les autres postes voient leur voyant rouge s'allumer : passer un appel leur est alors impossible. L'abonné ayant pris la ligne demande le N° de son correspondant à l'opératrice, laquelle s'occupe d'appeler le destinataire, et de mettre en relation les deux interlocuteurs. À la fin de l'appel, raccrocher libère le canal radio, et tous les abonnés au service voient le voyant vert s'allumer : il est alors possible de passer un appel. Le prix, la complexité, la limite de portée réservent ce service à un très petit nombre : lorsque le service manuel est arrêté en 1973, il ne compte que 500 abonnés...

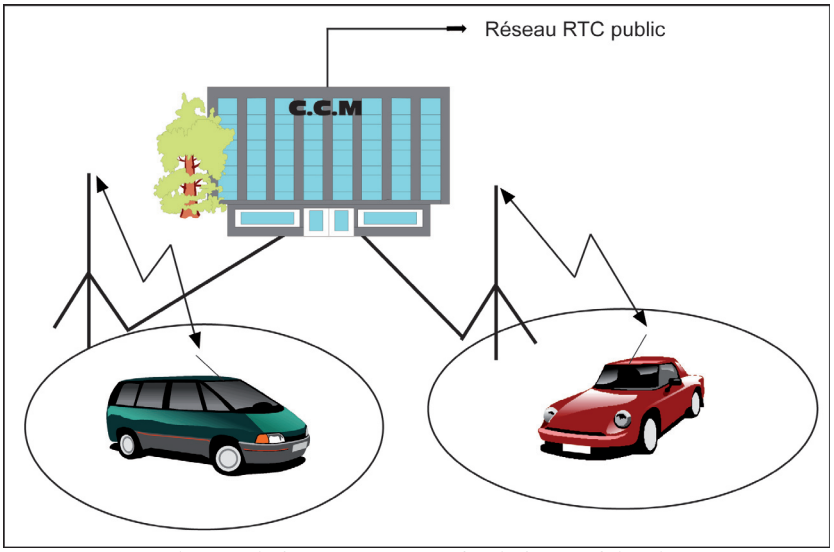
Poste U43

Pour remplacer le premier réseau manuel, un second système est développé. Il utilise la même bande de fréquence, mais les capacités augmentent : il est désormais possible à plusieurs utilisateurs de converser en même temps, grâce à l'adoption d'un système de gestion de plusieurs canaux simultanés. De même, le réseau devient automatique.

Les appareils utilisés sont dérivés d'une radio de type professionnelle, le *copilote* de Thomson CSF. Même si les platines radio sont identiques, on leur associe une carte de gestion à microprocesseur 4 bits, ainsi qu'une série de quartz (2 par fréquence), permettant de changer le canal de transmission. Le combiné est identique au S63 filaire.

Dans les années 80, la France accuse un retard important dans les technologies de téléphonie mobile. Le seul réseau en place ne permet qu'un nombre limité d'utilisateurs, il est uniquement disponible dans les grandes agglomérations, et ne permet en aucun cas une intégration dans un volume portable. Pour ces raisons, le ministère des Télécommunications décide de lancer le programme *Radiocom 2000*.

Le réseau « Correspondance Publique » fonctionnera jusqu'à la fin des années 80, c'est à dire jusqu'au déploiement complet du Radiocom 2000. Les abonnés reçoivent alors une proposition personnalisée de changement de système.



La liaison téléphonique entre un radiotéléphone mobile et le réseau commuté est assuré par l'intermédiaire d'un relais et d'un centre de commutation des radiotéléphones mobiles (C.C.M.)

Le Radiocom 2000

Lancé en 1986, il s'agit d'un réseau fonctionnant dans la bande des 400 MHz, utilisant la technologie numérique pour la signalisation (gestion des appels, des connexions). La modulation est cependant standard (analogique pour la voix). Les fréquences sont attribuées dynamiquement en fonction des besoins. Contrairement au réseau précédent, le Radiocom utilise un synthétiseur de fréquence, supprimant ainsi les nombreux quartz tout en augmentant le nombre de canaux utilisables

L'autre grande nouveauté est la notion de téléphone cellulaire : les fréquences sont attribuées au sein d'une « *cellule* », c'est-à-dire une zone géographique délimitée par la portée de l'émission radio. Lorsqu'un mobile sort de la zone de couverture radio, il peut « s'inscrire » sur la zone de couverture adjacente. Alors que lors de son lancement la communication était perdue lorsque le mobile sortait de la cellule d'inscription précédant l'appel, l'ajout de la fonction de « *hand over* » permet de continuer la communication en changeant de zone de couverture. Cette dernière évolution technique a coûté le rapatriement de tous les mobiles pour mettre à jour le logiciel de gestion du mobile.

Enfin, ce réseau a pour vocation de couvrir la totalité du territoire français, y compris les zones à faible population.

Toutes ces évolutions techniques permettent de créer assez rapidement le premier téléphone portable, c'est à dire libéré de la voiture : le *Poctel*. Dès ses débuts, ce téléphone est un objet de luxe. D'abord par le coût de l'abonnement, mais aussi pour son prix d'acquisition (25 000 F en 1991). L'énergie est assurée par une batterie rechargeable de type Nickel Cadmium, et l'antenne est raccourcie au minimum possible. L'objet remporte un grand succès en regard de son prix.

Le réseau NMT-F

En 1989, l'État français décide de déréguler le marché des télécommunications mobiles. Un appel d'offres est lancé pour compléter le Radiocom. La société SFR répond à cet appel d'offres avec un réseau basé sur le standard NMT (*Nordic Mobile Telephone*). Il sera adapté au marché français, d'où son nom, le NMT-F. Le fonctionnement est très similaire au Radiocom 2000 (modulation analogique pour la voix, et signalisation numérique, bande de fréquence en 400 MHz). Les terminaux mobiles sont très proches des versions Radiocom. Extérieurement, la seule différence visible sera la couleur adoptée pour chaque terminal...

De l'analogique au numérique : le GSM.

En 1982, un consortium d'opérateurs européens décide de lancer les études d'un système de télécommunication mobile universel. Le Groupe Spécial Mobile, ou GSM, voit officiellement le jour en 1987, date à laquelle ses spécifications sont adoptées. Le cahier des charges précise que ce système devra être compatible quel que soit le pays, les terminaux étant reconnus à l'aide d'une carte d'identification (la carte SIM pour *Subscriber Identification Module*). Le mode de transmission adopté est très novateur : entièrement numérique pour la voix et la signalisation, mode TDMA (*Time Division Multiple Access*), compression des données vocales, large utilisation d'algorithmes de traitement du son, capacité à transmettre des données numériques, fax, ou messages courts de 160 caractères (SMS, *Short Message Service*)... Toutes ces évolutions font de ce système un véritable défi lancé aux centres de recherche. Comment intégrer toutes ces technologies dans un volume aussi réduit qu'un paquet de cigarettes ?

Finalement, les technologies de l'électronique évoluant suffisamment, les industriels utilisent des composants de toute dernière génération (microprocesseurs 16 ou 32 bits, DSP, ...). Ces postes n'ont plus aucun réglage par potentiomètre, aidant ainsi à la fiabilité de l'ensemble. La bande de fréquence à 900 MHz est également nouvelle dans le monde civil. Les premiers terminaux sont encore des versions « téléphone de voiture », en forme de petite mallette. Ils seront très rapidement remplacés par des versions portables. Le service commercial GSM démarre en 1991 dans les grandes agglomérations françaises.

Une tentative avortée : le Bi Bop

Alors que le réseau GSM poursuit sa croissance, lentement mais sûrement, un réseau alternatif est proposé en 1993, le *Pointel*. Ce réseau, contrairement au GSM, n'est pas à proprement parler un téléphone mobile. Il ne permet pas de recevoir d'appel, seulement d'en émettre lorsque l'usager se trouve à proximité immédiate d'une borne. Il est à ce titre qualifié de « cabine téléphone de poche ».

Le succès de ce réseau n'aura pas lieu. Le développement rapide du GSM, la réduction de taille des téléphones devenant réellement portables annihilent tout espoir et avantage du Pointel. France Télécom tentera un ultime rattrapage en lui associant la compatibilité avec les téléphones portables domestiques (avec une base chez un particulier). Le réseau fut abandonné en 1997, n'ayant convaincu qu'une centaine de milliers d'usagers.

Le GSM : un développement continu

L'un des développements les plus remarquables du GSM est son usage international. Le réseau en lui-même n'est pas visible par l'usager (antennes relais mises à part). Il permet cependant de communiquer avec le même téléphone quel que soit le pays, pourvu que ce dernier ait adopté le standard. Victime de son succès, le GSM se voit rapidement attribuer d'autres bandes de fréquences. On retiendra la bande des 1800 MHz pour le DCS, et 800/1900 pour la version américaine. Ces évolutions imposent aux fabricants des modèles « multibandes » pour assurer la compatibilité avec l'ensemble des réseaux.

Architecture réseau et protocole

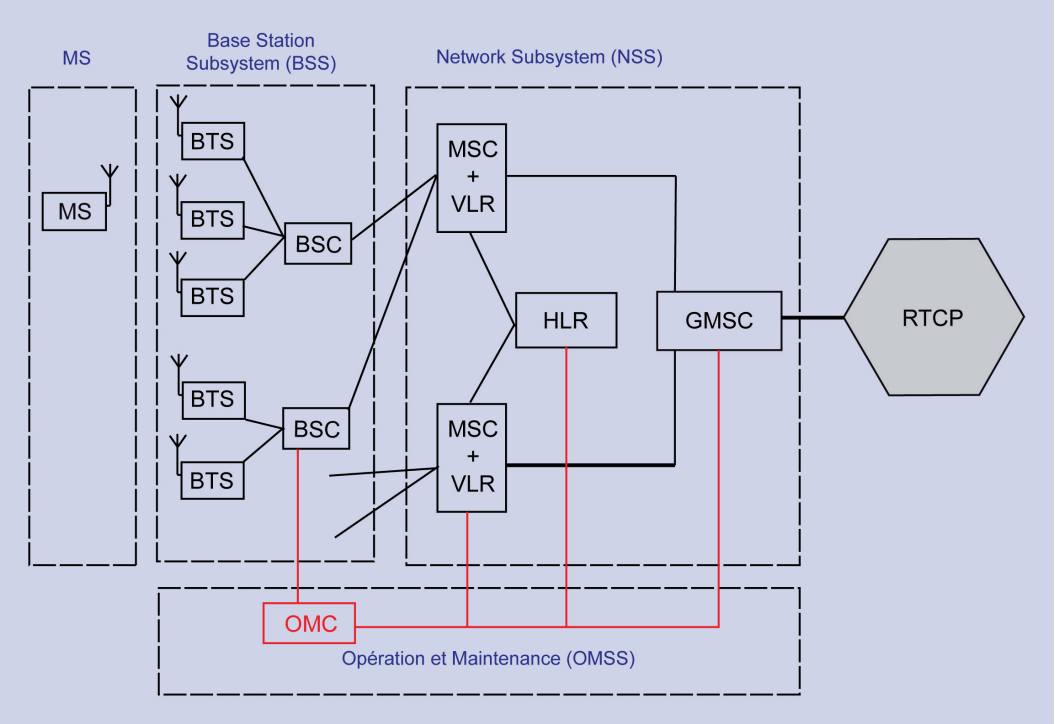
Le réseau spécifique pour le GSM s'appelle PLMN (*Public Land Mobile Network*), chaque opérateur ayant le sien propre. Il est relié au Réseau Téléphonique Commuté Public (RTCP).

En ne tenant pas compte des extensions GPRS, un tel réseau est composé de 4 grandes entités :

— une station Mobile appelée Mobile Station (MS): c'est habituellement un téléphone mobile, mais de manière générale, cela peut être n'importe quel appareil disposant d'un transmetteur adéquat et d'une carte SIM.

— la partie radio du réseau, appelée Base Station Subsystem (BSS): elle est composée d'un maillage de stations de base (BTS) et de leurs stations de contrôle (BSC). À cela se rajoute le Transcoder (*Transcoder and Rate Adaptation Unit, TRAU*) qui se charge de la compression/décompression de la voix.

— la partie routage, appelée Network Subsystem (NSS) ou Core Network Subsystem, chargée d'acheminer la communication entre deux utilisateurs du réseau ou vers l'extérieur (réseau fixe par exemple) : elle est composée de Mobile Switching Centers (MSC) reliés entre eux qui effectuent le routage des communications. À chaque MSC est rattaché un Visitor Location Register (VLR) qui gère les informations des abonnés se trouvant dans la zone gérée par le MSC. Une base de données unique, le Home Location Register (HLR) gère la liste des abonnés de l'opérateur du réseau. Pour se connecter à d'autres réseaux extérieurs, il y a une passerelle dédiée, le commutateur réseau Gateway Mobile Switching Center (GMSC). L'AuC (*Authentication Center*) se charge de l'authentification des usagers.



— la partie Opération et Maintenance, gérée par l'Operation and Maintenance Center (OMC), qui est chargé de mettre en place et de veiller au bon fonctionnement des différents éléments du réseau.

Le réseau de téléphonie mobile a une structure « *cellulaire* » qui permet de réutiliser de nombreuses fois les mêmes fréquences. En France, aux heures d'affluence, près d'un million d'appareils sont en service avec seulement 500 canaux disponibles. Comment fait-on alors ?

Pourquoi, en France, 500 canaux ?

Le réseau de téléphonie mobile utilise des ondes électromagnétiques, tout comme le réseau pour la radio, la télévision, les satellites et les autres réseaux de communication tel que ceux dédiés aux gendarmes, ambulanciers et autres. En général, pour transmettre une information (binaire ou analogique) on utilise un canal. Ce canal est une fréquence spécifique à laquelle l'onde est modulée. On préfère garder un certain espace entre les canaux, car si leurs fréquences sont trop proches, ils finissent par empiéter les uns sur les autres.

On a donné à chaque application (radio, télévision, téléphones, etc.) des groupes de fréquences, qui varient de continent à continent, voire parfois de pays à pays. En Europe, la téléphonie mobile a reçu deux groupes : autour de 900 et autour de 1800 mégahertz (MHz).

Il a tout d'abord fallu scinder chacun de ces groupes en deux : une fourchette de fréquences pour envoyer des données vers les téléphones mobiles, l'autre pour leurs émissions. L'un donc pour être appelé et entendre, l'autre pour appeler et parler.

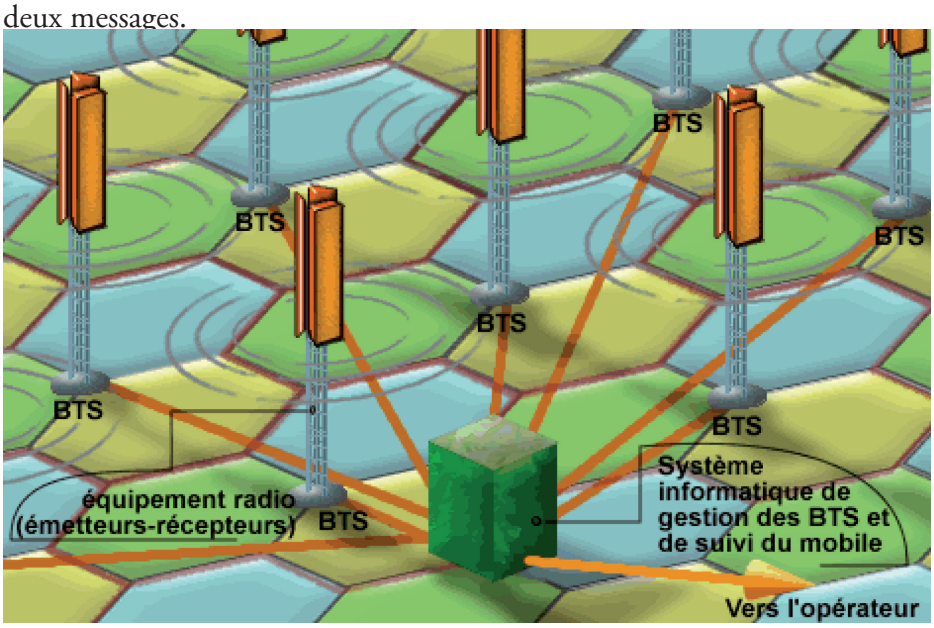
	Émission (en MHz)	Réception (en MHZ)
Groupe 1	890-915	935-960
Groupe 2	1710-1785	1805-1880

Vient alors la subdivision en canaux. En GSM (pour *Global System for Mobiles*), l'écart de fréquence entre deux canaux adjacents a été fixé à 200 kHz, soit 0,2 MHz. Le groupe 1 a donc 125 canaux et le groupe 2 en a 375, ce qui fait 500 au total. S'il n'y avait qu'un émetteur pour toute l'Europe, on ne saurait effectuer que 500 communications à la fois.

Première solution : des milliers d'émetteurs

On a donc installé un grand nombre d'émetteurs à courte portée ne couvrant qu'un domaine bien délimité, une *cellule*. De là le terme « *téléphone cellulaire* ». La portée moyenne est de 1 km. Ainsi, les téléphones reçoivent les ondes d'un mât et lui répondent pour faire savoir s'ils souhaitent en dépendre. Si celui-ci accepte, il retient le numéro d'identité de l'appareil, lui réserve un canal et reprend le contact si un appel pour ce téléphone lui parvient ou si le téléphone en effectue un.

Cette solution pose néanmoins un problème : les antennes adjacentes utilisent la même fréquence pour chaque utilisateur. Si l'un d'eux se situe à la frontière entre les deux zones de portée, il reçoit les deux messages.



Amélioration : le damier hexagonal

On a alors divisé les émetteurs eux-mêmes. Souvent, les antennes relais (BTS pour *Base Transceiver Station*) sont regroupées par trois sur un pylône ou suivant une configuration équivalente. Chacun supporte donc un tiers des canaux. Sur ce schéma, chaque couleur (vert, bleu, jaune) figure un groupe de fréquences. Elles créent ainsi un « damier hexagonal » de cellules. Ce damier est avant tout une vue de l'esprit, les zones se recouvrant les unes avec les autres et variant avec la météo, le nombre d'utilisateurs, etc.

Mais cela pose un problème pour la localisation du destinataire d'un appel. Lorsque le téléphone (MS) décide de changer de cellule, il informe le VLR (*Visitor Location Register*) dont dépend la nouvelle cellule. Si l'on a changé de MSC (*Mobile service Switching Center*), le HLR (*Home Location Register*) est contacté, ce dernier contactant le précédent MSC. L'utilisateur s'identifie soit avec l'IMSI (*International Mobile Suscriber Identity*) ou le TMSI (*Temporary Mobile Suscriber Identity*), ce dernier étant préféré pour des raisons de sécurité.

Pour augmenter le nombre d'utilisateurs d'une zone donnée, on réduit la taille des cellules.

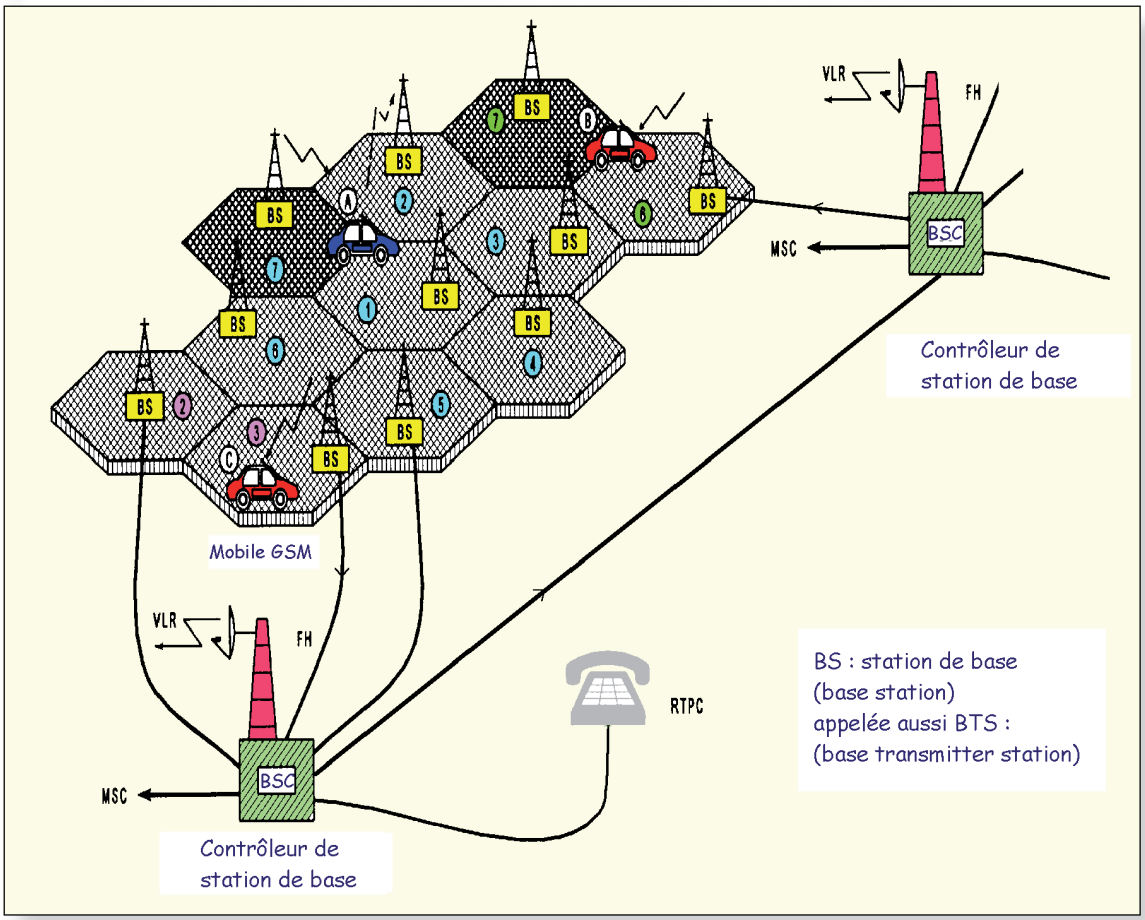
Solution supplémentaire : le multiplexage temporel

Contrairement à ce que peut faire croire le nom de cette technique, le multiplexage temporel est assez simple à effectuer en numérique. Dans le combiné, la voix est numérisée et donne donc un code binaire. Celui-ci a la particularité de pouvoir être compressé. Or sur une bande de 200 kHz, on peut faire passer plusieurs paquets de telles données compressées. Du coup, le téléphone numérise, puis compresse le son

La structure du réseau GSM

Lorsqu'on téléphone à partir d'un mobile GSM :

- le mobile transmet par radio la communication vers la station de base de sa cellule.
- la conversation est ensuite acheminée de façon plus classique (câble, fibre optique ...) vers le correspondant s'il est raccordé au réseau téléphonique filaire, ou à sa station de base s'il est équipé d'un mobile.
- cette station de base transmet finalement la conversation par radio au correspondant.



Même si deux personnes se trouvent dans la même cellule et se téléphonent, la conversation ne passe jamais directement d'un GSM à l'autre.

Au cours d'un déplacement, il est possible qu'on sorte d'une cellule. Il est nécessaire alors de changer da station de base tout en maintenant la communication : c'est le transfert intercellulaire ou handover .

Pour gérer ce transfert :

- le téléphone GSM mesure en permanence la force du signal radio reçu de la station de base et écoute aussi régulièrement les stations de base des cellules voisines
- lorsqu'il constate qu'il reçoit mieux une autre station de base que celle avec laquelle il échange les signaux, il en informe sa station de base
- la station de base décide alors de passer le relais à la station de base voisine et met en œuvre la procédure de handover

Ce processus oblige tous les mobiles GSM à écouter les stations de base des cellules voisines en plus de la station de base de la cellule dans laquelle il se trouve.

et n'envoie cela que par « paquets » toutes les 20 millisecondes. Ainsi, on peut imbriquer huit émissions (7 communications + 1 canal de contrôle) par canal.

Évolutions futures

Localisation automatique (ou géolocalisation) : comme la couverture des antennes de relais est réduite et que celles-ci se recoupent (il y en a environ 35 000 en France), il est facile, par triangulation, de localiser assez précisément la position du téléphone mobile. Les opérateurs vont mettre cela à profit pour offrir des services de guidage automatique pour piétons ou des informations locales. En France, ce service est disponible pour les mobiles équipés d'*i-mode* d'un certain opérateur depuis novembre 2003.

Augmentation de l'aptitude des GSM à transmettre des données numériques. Maintenant qu'on est passé à la norme GPRS, pour aller encore plus loin, il faudra installer un nouveau réseau radio. On passerait alors à la norme UMTS (dite de 3e génération). Cela donnerait un débit de l'ordre de 384 kbits/s (pouvant aller théoriquement jusqu'à 1,9 Mbits/s) alors que le GPRS ne permet qu'un débit théorique de 110 kbits/s (en pratique 30/40 kbits/s) et le mode GSM de base 9,6 kbits/s.

Le téléphone mobile semble réussir là où ont échoué des technologies antérieures : devenir un couteau suisse numérique. Comme ce dernier, le téléphone mobile tient dans la poche, est relativement simple à utiliser et recouvre une multitude de fonctions liées au nomadisme : de simple téléphone à l'origine, il permet désormais d'envoyer des messages textuels (SMS, MMS, courriel), il sert de montre/chronomètre/minuteur, de télécommande (s'il est équipé de Bluetooth[47]) et il remplace de plus en plus les PDA (c'est alors un smartphone) ou même l'appareil-photo (c'est alors un photophone). Des modèles faisant office de caméscopes numériques ou de puissantes consoles de jeu 3D portable seront également disponibles courant 2006.

Le téléphone mobile est également amené à évoluer vers les systèmes de paiement : porte-monnaie électronique. Par exemple, au Japon, l'opérateur de téléphonie mobile japonais NTT DoCoMo et l'établissement de crédit JCB déploient en 2005 un téléphone mobile équipé du système de paiement QuicPay qui communique par radio, sans contact, avec le terminal du commerçant (opération pilote en 2005 avec les taxis de Yokohama près de Tokyo).

Distribution et vente de contenu sous forme numérique, comme la musique, en France les principaux opérateurs disposent d'une offre dans ce domaine. Les MVNO, NRJ Mobile et M6 Mobile en font même leur principal produit d'appel. Il s'agit en fait d'un système de radio personnalisée, qui après inscription et définition des goûts n'envoie que les morceaux qui sont le plus susceptibles de plaire à l'utilisateur. Le gros avantage de cette innovation serait la possibilité de découvrir de nouveaux groupes/artistes. Cette technologie fonctionnerait sur le même principe que les PodCasts, avec des morceaux téléchargés précédemment et que l'on peut écouter à son gré.

Il semble que la voie tracée par la plupart des producteurs, mais aussi ce que demande le public soit une convergence des technologies et des concepts vers un seul appareil multimédia. Ainsi, les téléphones mobiles se sont vu ajouter, ces dernières années, des fonctions agenda, lecteur multimédia, appareil photo numérique et autre chronomètre ou dictaphone...

La téléphonie mobile 4G (4e génération) se profile. L'industrie des télécommunications y travaille et son lancement est prévu à l'horizon 2008-2010 au Japon, puis après en Europe. Les débits de ces appareils pourraient atteindre des valeurs de l'ordre de 300Mpbs, ouvrant la voie à la télévision sur mobile...

[47] *Bluetooth* est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les claviers, les souris, les téléphones portables, les PDAs et les appareils photo numériques.

Les satellites de télécommunication

Les satellites de télécommunications représentent pour le moment la pointe du progrès en matière de communication. Avant l'ère spatiale, aucune transmission de télévision n'était possible entre les continents, et les quelques câbles transocéaniques qui existaient ne pouvaient acheminer que quelques dizaines de conversations téléphoniques. En quelques années, le satellite a changé totalement la donne pour la télévision, le téléphone ou même Internet.

Fonctionnement général

Le satellite de communication reçoit le signal de la station terrestre. Il l'amplifie et le transmet à une station réceptrice en utilisant une autre longueur d'onde. Les programmes de télévision, les communications téléphoniques, les données numériques peuvent être ainsi relayés à l'échelle planétaire.

Avantages d'un satellite par rapport aux communications terrestres.

Les satellites de télécommunications sont à l'heure actuelle très nombreux, car ils sont venus compléter et améliorer les possibilités des moyens de télécommunications terrestres par fil ou par ondes qui souffrent des limitations suivantes :

— Coût d'installation, de maintenance et des matières premières très élevé et augmentant fortement avec la longueur du réseau.

— Problème physique : plus la quantité d'information qu'il est possible de confier à une onde est grande, plus la longueur de cette onde est petite et moins bien celle-ci se propage à la surface de la Terre. Si elle est de quelques mètres, chaque obstacle susceptible d'arrêter la lumière l'arrête également (montagnes,…)

— Exposition aux tremblements de terre, inondations, tempêtes et autres risques majeurs qui peuvent détruire la ligne.

Avant l'arrivée des satellites, les images venant d'autres continents ne nous parvenaient que par avion, plusieurs jours après avoir été filmées. Quand le satellite arriva, celui-ci résolut, dans son principe même, les 3 contraintes citées ci-dessus. Primo, il est un moyen idéal pour la transmission d'informations sur des aires géographiques très vastes. Il possède donc a priori une vocation mondiale puisqu'il ne nécessite pas une lourde infrastructure au sol, ce qui paraît particulièrement bien adapté pour un pays dont le peuplement est discontinu. Secundo, les satellites de télécommunications offrent la possibilité de communiquer entre deux points éloignés sans être gênés ni par le relief, ni par la courbure de la terre, à condition de rester dans l'aire de visibilité du satellite assurant la transmission. Tertio, le satellite ne risque rien dans le cas d'un tremblement de terre ou d'une inondation et les infrastructures au sol occupent une si petite surface que le risque de dégâts en est fortement réduit.

Les différents types de satellites de télécommunication

Tous ces avantages, plus le fait qu'ils soient une des seules applications spatiales rentables, expliquent certainement l'expansion des satellites de télécommunications (on estime à un millier aujourd'hui le nombre de satellites de télécommunications). Le premier d'entre eux fut Echo 1. Il s'agissait d'un satellite passif puisqu'il réfléchissait seulement l'énergie qu'il recevait. Le signal était fortement diminué et ce fut le premier et le dernier des satellites de télécommunications passif. À partir de 1962 et de Telstar, les satellites sont tous devenus « actifs » : ils reçoivent les signaux, les amplifient et les réémettent à partir de répéteurs. Leur charge utile se compose de panneaux solaires fournissant l'énergie nécessaire à l'amplification du signal et des antennes plus ou moins directionnelles qu'il faut orienter avec une grande précision vers la terre. Les antennes terrestres doivent par ailleurs impérativement être pointées avec précision

en direction du satellite pour la réception comme pour l'émission. Les premiers satellites télécoms étaient des satellites à défilement, c'est-à-dire qu'ils n'étaient visibles que quelques minutes. Cette orbite basse a été rapidement abandonnée et maintenant la plupart des satellites de télécommunications (le premier fut Early Bird en 1965) sont logiquement placés sur une orbite géostationnaire pour que les antennes soient constamment reliées entre elles, sans coupures. Pourtant aujourd'hui, on en revient aux satellites à défilement (et même à une constellation de satellites à défilement) pour répondre à la croissance de l'utilisation des téléphonies mobiles.

Affaiblissement possible du signal

Certains phénomènes météorologiques et astronomiques peuvent affaiblir un signal (la pluie ou des vents solaires). Le signal est aussi plus facilement arrêté par le relief en région de haute latitude (l'angle sol-satellite est plus faible et l'ombre est donc plus grande).

Deux ressources fondamentales

Un satellite de télécommunications utilise deux ressources limitées : l'orbite géostationnaire et une bande de fréquence radio réservée. À quelques rares exceptions près (utilisations du laser pour les communications sous-marins – satellites, par exemple), toutes les communications par satellites exploitent les ondes radio. Avec l'augmentation continue du nombre de satellites, le problème de l'allocation des fréquences est devenu extrêmement complexe. Le spectre des fréquences utilisables apparaît déjà très exploité. Cependant, les progrès des techniques de transmission de données ont permis de décupler la capacité des installations et de réduire la taille des stations terrestres. Les méthodes numériques de codage à la source ont ainsi entraîné une division par dix du débit nécessaire pour transmettre une communication téléphonique ou une émission de télévision.

Modulation du signal

Pour faire en sorte que l'onde « porte » un message, on utilise la modulation. Le procédé consiste à modifier une ou plusieurs caractéristiques de l'onde radio (porteuse) selon le type d'informations que l'on souhaite envoyer. Le procédé inverse, la « démodulation », sert à reconstruire l'information d'origine (discours, données informatiques ou programme TV) dans le récepteur. En pratique, la méthode de modulation, généralement assez complexe, est choisie afin d'optimiser les performances d'une liaison satellite selon le type d'information à transporter. L'information est souvent codée à l'émetteur afin de pouvoir détecter et corriger les éventuelles erreurs dues à une mauvaise interprétation dans le récepteur. Des techniques semblables, tout aussi élaborées, sont utilisées par exemple pour protéger les disques laser audio contre les rayures et les mauvaises manipulations.

Types de couvertures d'un satellite géostationnaire

Un satellite de télécommunications n'utilisera jamais toute la surface qu'il peut couvrir, car sur la périphérie de cette zone maximale couverte, l'angle formé entre le sol et le satellite est trop faible pour pouvoir recevoir les ondes émises par le satellite. Par contre, des couvertures restreintes — semi-globale (échelle d'un continent), régionale (échelle de l'Europe) et étroite (2 à 3 pays moyens) - présentent l'avantage de concentrer l'énergie sur de plus petites surfaces et donc de fournir un signal plus fort.

Services commerciaux

Les télécommunications ont très vite représenté un marché important (50 milliards de dollars en 2000). Plusieurs services commerciaux se sont donc développés, tant au niveau mondial que national :

Services internationaux

Intelsat

Intelsat est l'Organisation internationale des satellites de télécommunications qui réunit plus de 120 pays. Le premier satellite d'Intelsat fut « *Early Bird* », qui assurait des retransmissions télé entre l'Europe et les États-Unis. Les générations de satellites suivantes possédaient des capacités de transmission et d'émission déjà plus élevées, grâce à la concentration de la puissance en direction de la terre, et à la division du spectre de transmission en bandes de fréquence plus étroites. Ainsi, le premier des satellites Intelsat de quatrième génération, lancé en 1971, était doté d'une capacité de 4 000 circuits vocaux.

En 1980, les satellites Intelsat de 5e génération avaient une capacité de 12 000 circuits vocaux. On a par ailleurs commencé à concentrer la puissance du satellite sur de petites régions de la terre, ce qui a fait chuter les prix des antennes de réceptions (taille et diamètre plus petit). Mis en service à partir de 1989, les satellites de sixième génération ont pu établir 24 000 circuits simultanés. Au début des années 1990, Intelsat, avec 15 satellites en orbite, offrait ainsi le système de communications le plus étendu du monde, relayant 100 000 circuits téléphoniques. Cependant, d'autres systèmes proposent également un service international du même type, concurrençant ainsi celui d'Intelsat qui a été privatisé en 2001…

Inmarsat

Organisation internationale des satellites maritimes, Inmarsat (*International Maritime Satellite*), fondée en 1979 et transformée en société privée depuis 1999, couvre un réseau mobile de télécommunications qui assure des liaisons de données numériques, des liaisons téléphoniques et un service de transmission par télécopie entre des bateaux, des installations en mer et des stations terrestres à travers le monde. En outre, ce réseau prolonge maintenant le système de liaisons par satellites utilisé par les avions des lignes internationales. Les téléphones Inmarsat sont devenus indispensables dans les courses transatlantiques, les rallyes, etc. Ce sont également des outils formidables pour les journalistes, et pour toutes les équipes de secours en cas de catastrophe naturelle : ainsi, lors du grand tremblement de terre de Kobé, les liaisons avec le monde extérieur ont pu être rétablies grâce à des téléphones Inmarsat. Il en est de même en cas de raz de marée, d'éruption volcanique, d'inondation… Inmarsat va désormais être concurrencé par les nouvelles constellations de satellites pour les « mobiles » (*Globalstar*) voir même par des satellites géostationnaires qui offriront des liaisons à plus bas prix pour les pays en voie de développement (ACES en Asie et EAST pour l'Afrique).

Les services régionaux

L'expansion des systèmes internationaux s'est faite parallèlement au développement de systèmes à l'échelle régionale.

En Europe :

L'importance des satellites de télécommunications est apparue très tôt aux pays européens, mais il faudra attendre une véritable cohésion spatiale européenne pour établir, en 1977, Eutelsat qui permettra l'obtention d'un véritable service de télécommunication européen indépendant de la tutelle mondiale. Ainsi, Eutelsat fait partie des réalisations qui ont permis une plus grande cohésion régionale entre États membres de l'ex-CEE. Le service se base principalement sur une offre télévision avec un service européen de téléphonie qui a permis de compléter le réseau terrestre européen sans enfreindre les conditions d'Intelsat (toujours utilisé pour les communications hors Europe). Il faut également mentionner le réseau européen de satellites de communication ECS (*European Communication Satellite*), développé par l'Agence spatiale européenne (ESA) ; chacun de ses satellites peut établir 12 600 circuits.

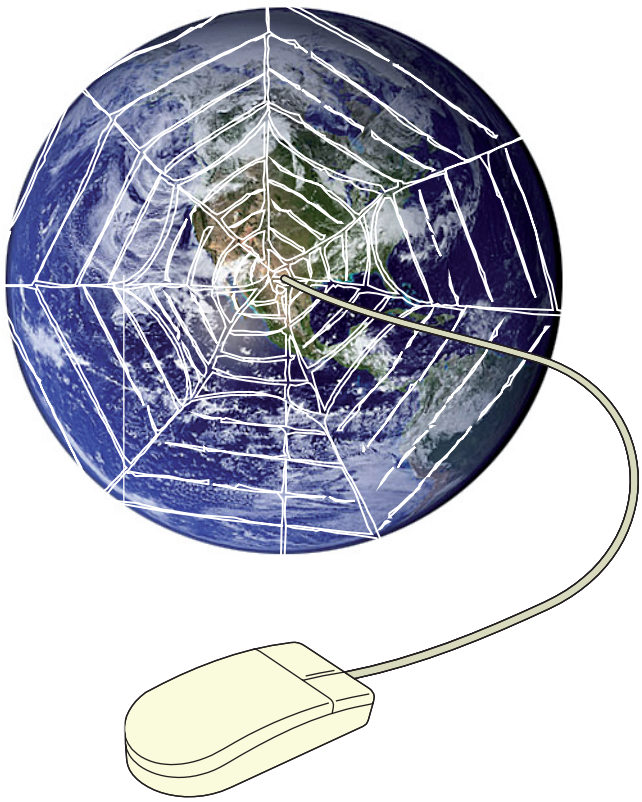
Arabsat :

La création de l'Organisation Arabe des Télécommunications en 1976 correspond à une volonté politique de développement des liens régionaux mais dans un contexte différent puisqu'il s'agissait ici d'un programme de renforcement de l'identité culturelle arabe. Ces dernières années, la volonté commerciale semble cependant l'avoir emporté sur la volonté culturelle.

Palapa :

Au début uniquement basé sur les Philippines, le système Palapa s'est progressivement étendu au reste des pays de l'ASEAN (Association des pays du Sud-est asiatique) jusqu'à être reconnu système régional par Intelsat.

Internet



...Et l'Homme créa l'Internet

L'Internet, avec un grand « I », tel que nous le connaissons maintenant est une infrastructure de communication à l'échelle planétaire issue de l'interconnexion de réseaux informatiques publics et privés. Mais à l'origine le concept d'Internet s'écrivait avec un petit « i », et désignait simplement l'idée d'« *interconnected network* » ou d'« inter-networking » puis « internetting » c'est à dire la possibilité de faire dialoguer plusieurs réseaux ensemble et non pas l'« International Network » comme on peut le lire parfois. Il est né de croisements entre plusieurs courants de recherche et son succès d'une ampleur imprévue ne cesse d'étonner tous ceux qui s'y intéressent. Ses retombées ont depuis longtemps dépassé le cadre technique pour s'étendre au commerce, à l'économie, et à tous les aspects de notre société qui directement ou indirectement sont liés à l'information et la communication. La surabondance de livres à propos d'Internet montre l'étendue de l'intérêt que lui porte maintenant le public, cependant la vision de l'histoire d'Internet que ces ouvrages donnent souvent en première partie est en générale succincte, romancée et parfois même erronée. Cette histoire, comme nous allons le voir, est une succession de croisements entre plusieurs domaines d'activité. Citons par exemple :

— Les mathématiques, les télécommunications, traitement du signal, codage, cryptographie…
— L'électronique, la microélectronique, l'ordinateur, l'informatique, le PC et ses périphériques, la micro-informatique…
— Les logiciels, la bureautique, la gestion documentaire, l'hypertexte, jeux, la programmation…
— La recherche militaire, la recherche académique,…

• 1945 : Vannevar Bush conseiller scientifique du président Roosevelt pendant la Seconde Guerre mondiale propose *Memex*, une machine conceptuelle dont la description contient les germes des systèmes hypertextuels. Il critique les systèmes d'indexation des documents et remarque que l'esprit humain travaille souvent par associations d'idées. Son système, décrit en termes techniques limités de l'époque, devait pouvoir enregistrer une grande quantité d'informations, et serait pour l'homme une mémoire augmentée. Il permettrait à l'utilisateur de créer des rails ou des pistes de navigation, des liens d'association entre des textes et/ou des illustrations stockés, des mécanismes d'annotation et d'historique…

Memex :

« Imaginons un appareil de l'avenir à usage individuel, une sorte de classeur et de bibliothèque personnels et mécaniques. Il lui faut un nom et créons-en un au hasard. « Memex » fera l'affaire. Un memex, c'est un appareil dans lequel une personne stocke tous ses livres, ses archives et sa correspondance, et qui est mécanisé de façon à permettre la consultation à une vitesse énorme et avec une grande souplesse. Il s'agit d'un supplément agrandi et intime de sa mémoire.

Cet appareil se compose d'un bureau et bien que l'on puisse présumer le faire fonctionner à distance, c'est surtout le meuble où l'on travaille. Sur le dessus, on trouve des écrans translucides inclinés sur lesquels des documents peuvent être projetés pour une lecture confortable. On y trouve un clavier et plusieurs ensembles de boutons et de leviers. Autrement, on dirait un bureau ordinaire.

À une extrémité se trouve le stock de documents. La question du volume est aisément prise en charge par des microfilms améliorés. Une petite partie de l'intérieur du memex seulement est consacrée au stockage, le reste est utilisé par le mécanisme. Pourtant si l'utilisateur entrait 5 000 pages de documents par jour, il lui faudrait des siècles pour remplir cet entrepôt. Il peut donc utiliser l'espace sans parcimonie et ajouter des documents en toute liberté.

La plus grande partie des contenus du memex sont achetés sur microfilm prêt à l'emploi. Livres en tout genre, images, numéros récents de revues, journaux, tout peut être acquis et disposé au bon endroit. La correspondance d'affaires prend le même chemin. Et il est prévu de pouvoir ajouter directement de l'information. Dans la partie supérieure du memex, un plateau transparent accueille les notes, les photos et les éléments les plus divers. Une fois le document en place, on actionne un levier pour le photographier et l'intégrer à l'espace disponible le plus proche sur une section du film memex, en utilisant le procédé de la photographie à sec.

Il serait possible, bien sûr, de consulter les dossiers par le système de classement habituel. Pour feuilleter un livre précis, l'utilisateur tape le code de l'ouvrage sur son clavier et la page de titre apparaît aussitôt devant lui, projetée sur l'un de ses écrans de lecture. Les codes les plus utilisés sont mémorisés par un moyen mnémotechnique, pour que l'utilisateur n'ait pas à consulter trop souvent le manuel des codes, qui peut cependant apparaître par simple pression d'une touche. D'autres leviers sont à sa disposition. En inclinant l'un d'eux à droite, le livre défile devant lui, les pages apparaissent les unes après les autres à une vitesse qui permet un rapide coup d'œil. En poussant le levier encore plus à droite, tout le livre défile dix pages par dix pages ; encore plus à droite, cent pages par cent pages. Vers la gauche, le levier opère les mêmes opérations en arrière.

Un bouton spécial le ramène instantanément à la première page de l'index. Il peut ainsi appeler et consulter n'importe quel ouvrage de sa bibliothèque avec beaucoup plus de facilité que sur de vrais rayonnages. Comme il dispose de plusieurs postes de projection, il peut laisser un document en position pendant qu'il en appelle un autre. Il peut également ajouter des notes et des commentaires, utilisant pour cela un système de photographie à sec. Il se pourrait même qu'il puisse le faire avec un système de pointe de lecture comme sur les télautographes[48] *que l'on peut voir dans les salles d'attente des gares, exactement comme s'il avait une page réelle devant lui.*

Tout cela n'est que supposition, excepté en ce qui concerne la projection des mécanismes actuels et de tous les gadgets que nous connaissons déjà. Une étape s'avère indispensable au classement par association, dont le principe reposerait sur un système permettant à tout article d'en sélectionner immédiatement et automatiquement un autre. C'est ce processus reliant deux articles l'un à l'autre qui caractérise le memex.

Quand l'utilisateur construit une piste, il lui donne d'abord un nom, qu'il note dans son manuel des codes avant de le composer sur son clavier. Devant lui, les deux documents à assembler sont projetés sur des écrans voisins. En bas de chacun, on peut voir un certain nombre d'espaces destinés à recevoir le code, et un curseur est prêt à indiquer l'un d'eux sur chaque document. L'utilisateur n'a plus qu'à appuyer sur une touche pour que les articles se trouvent définitivement rassemblés. Le mot de code apparaît sur chaque espace prévu à cet effet. Invisibles, mais également dans l'espace destiné aux codes, des pointillés sont insérés pour la visualisation de cellules photographiques et, sur chaque document, ces tirets indiquent, par leur position, le numéro de classement des autres documents.

Ainsi, à tout moment, quand l'un de ces documents est visible, l'autre peut être rappelé instantanément en pressant une touche sous l'espace du code correspondant. En outre, il est possible de les consulter tour à tour, plus ou moins rapidement, en actionnant un levier tout comme celui qui permet de faire défiler les pages d'un livre. C'est exactement comme si on avait rassemblé les documents réels pour faire un nouveau livre, en mieux, car chaque article est relié à une multitude de pistes.

Supposons que le propriétaire du memex s'intéresse aux origines et aux caractéristiques de l'arc et de la flèche et qu'il étudie plus particulièrement les raisons de la supériorité apparente du petit arc turc sur l'arc long des

[48] Appareil reproduisant au poste d'arrivée, sur une feuille de papier spécial, les caractères d'un message ou les traits d'un dessin, au fur et à mesure qu'ils sont formés par la main même de l'expéditeur au poste de départ, ce qui donne au télégramme une authenticité indiscutable. Inventé par le physicien anglais Backwell.

croisés. Après avoir entreposé des dizaines de livres et d'articles sur le sujet dans son memex, il commence par parcourir une encyclopédie où il trouve un document intéressant, mais trop général ; il le garde en projection.

Dans un livre d'histoire, il découvre un autre élément pertinent qu'il joint au premier. Il avance ainsi, traçant une piste constituée de nombreux éléments. Il ajoute parfois ses propres commentaires, soit en les reliant directement à la piste principale, soit en les rattachant par une piste secondaire à un document précis. Quand il apparaît évident, que les propriétés élastiques des matériaux disponibles sont inhérentes à la qualité de l'arc, il bifurque sur une piste latérale qui l'amène à étudier les ouvrages sur l'élasticité et les constantes physiques. Il intègre une page manuscrite de ses propres analyses. Il construit ainsi une piste déterminée par son sujet à travers le labyrinthe des documents dont il dispose.

Et sa piste ne disparaît pas. Quelques années plus tard, il discute avec un ami de l'étonnante résistance des gens à la nouveauté, fut-elle d'un intérêt vital. Il a un exemple dans le fait que les Européens, vaincus, ne parvinrent pas à adopter l'arc des Turcs, il a même une piste sur ce sujet. En appuyant sur une touche, il fait apparaître le manuel des codes puis, à l'aide de quelques touches supplémentaires, il projette le début de la piste. Un levier lui permet de la parcourir, de s'arrêter aux sujets qui l'intéressent et d'explorer d'autres articles complétant la discussion. Il met alors en route un reproducteur qui photographie l'intégralité de la piste. Son ami peut ensuite l'intégrer à son propre memex, où il la reliera à la piste générale.

Des formes entièrement nouvelles d'encyclopédies vont apparaître, prêtes à l'emploi avec un réseau de pistes fonctionnant par association les traversant, prêtes à être insérées et amplifiées dans le memex. Ainsi, l'avocat aura sous les doigts les opinions et les décisions accumulées au cours de son expérience professionnelle, ainsi que de celles de ses amis et des pouvoirs publics. Le bureau des brevets disposera sur un simple appel des millions de brevets d'invention, avec des pistes réparties selon les spécialités de chacun. Le médecin, perplexe face à la réaction d'un patient, pourra suivre la piste établie lors de l'étude antérieure d'un cas similaire et consulter rapidement l'histoire de cas analogue, avec la possibilité de consulter ses ouvrages de référence en matière d'anatomie et d'histologie. Le chimiste, se débattant avec la synthèse d'un composé organique, aura à sa disposition toutes les publications traitant de son sujet ainsi que des pistes secondaires concernant leurs caractéristiques physiques et chimiques.

[...] Ainsi la science peut-elle améliorer la manière dont les hommes produisent, stockent et consultent les dossiers de l'espèce humaine. Il serait peut-être plus efficace de décrire de manière spectaculaire les instruments de l'avenir, au lieu de respecter scrupuleusement les méthodes et les éléments non encore élaborés qui subissent une évolution rapide, comme nous l'avons fait ici. Sans aucun doute, des difficultés techniques de toutes sortes n'ont pas été prises en considération, de même que l'on ignore les nouveautés qui peuvent surgir d'un jour à l'autre et accélérer le progrès technique de manière aussi brutale que la découverte du tube thermoionique. Pour que notre présentation ne soit pas trop ennuyeuse, car trop proche des modèles contemporains, il peut être utile de mentionner une telle possibilité, non pour jouer les prophètes, mais simplement pour suggérer, car toute prophétie qui repose sur l'extrapolation de ce que l'on connaît a une certaine consistance tandis que celle qui est fondée sur l'inconnu n'est qu'une double supposition. »

L'idée de Vannevar Bush était, non pas de faire de nouveaux documents avec des bribes de documents, mais de tracer un chemin entre les différentes bribes de documents. Ainsi, nous n'aurions plus besoin de lire tout un livre pour atteindre une partie qui nous intéresse, ni de rechercher dans d'autres livres les parties qui peuvent compléter l'information que nous avons déjà lue. Pour que ce chemin existe, il faut bien sûr le baliser. Pour être utiles il faut que ces balises permettent d'aller rapidement d'une bribe d'information à une autre.

Le Memex n'a jamais été construit, mais pour la première fois l'idée de se déplacer dans l'information, non pas de manière séquentielle, mais de manière associative, était décrite. Avec la manière séquentielle, nous sommes obligés de passer par un index pour trouver une page sur un sujet. Si nous voulons trouver

une page sur un sujet similaire, nous sommes obligés de revenir à l'index. Avec la manière séquentielle, les pages d'un sujet sont lues les unes à la suite des autres sans qu'à aucun moment nous puissions aller vers une page qui aborde un sujet similaire. Aujourd'hui, nous trouvons des sites, dit Internet, qui fonctionnent exclusivement suivant cette logique. Leurs constructeurs n'ont pas compris qu'il existait aujourd'hui une manière infiniment plus riche de se déplacer dans l'information : la manière associative.

La manière associative permet de relier des documents divers grâce à des associations d'idées. Si dans un livre vous trouvez à la page 10 un renvoi à la page 30 pour compléter une idée. Il s'agit là, bien sûr, d'un lien associatif. Mais si tous les liens associatifs renvoient au sein d'un même livre, il n'était nul besoin de songer à inventer une machine pour se déplacer d'un lien associatif à un autre. Il n'en va pas de même si la page 10 renvoie à une page 50 d'un autre livre et indique son titre et son auteur. Il va falloir savoir où se trouve cet autre livre parmi des milliers ou des millions d'autres livres.

Si nous sommes dans une bibliothèque où se trouve cet autre livre, nous allons devoir rechercher sur un catalogue pour trouver la case où il est rangé. Pour gagner du temps il faudrait que le renvoi indique non pas son titre et son auteur, mais l'endroit où il est possible de trouver ce livre. Pour gagner encore plus de temps, il faudrait qu'une machine apporte rapidement l'information. Mais le livre est volumineux. Pour pouvoir atteindre rapidement l'information qu'il contient, il faut que cette information puisse circuler avec un support miniaturisé. Vannevar Bush en a conscience lorsqu'il écrit « La question du volume est aisément prise en charge par des microfilms améliorés ».

• 1946 : L'ENIAC, acronyme de Electronic Numerical Integrator Analyser and Computer, est le premier ordinateur entièrement électronique construit pour être Turing-complet[49]. Il est considéré comme le premier ordinateur électronique programmable.

Le principe est une idée de John William Mauchly, professeur de physique. Participant à une conférence à l'Ursinus College, il voit des analystes produire des tables de tir, il réalise que ces calculs pourraient être réalisés électroniquement. J. Presper Eckert résout les problèmes d'ingénierie, le principal étant la durée de vie des tubes électroniques.

C'est l'armée américaine qui va financer et construire le projet pour les besoins du laboratoire de recherche en balistique. L'ordinateur est financé le 17 mai 1943 sous le nom Project PX et construit à la Moore School of Electrical Engineering à partir de mi 1944. C'est en février 1946 qu'il est opérationnel puis il est coupé le 9 novembre 1946 pour être rénové et sa mémoire augmentée.

Le 14 février 1946 il est dévoilé au public à l'université de Pennsylvanie puis est transféré à Aberdeen Proving Grounds, Maryland en 1947 où il est remis en marche le 29 juillet et commence les calculs des tables de tirs. Il continue à fonctionner jusqu'à son arrêt en 1955.

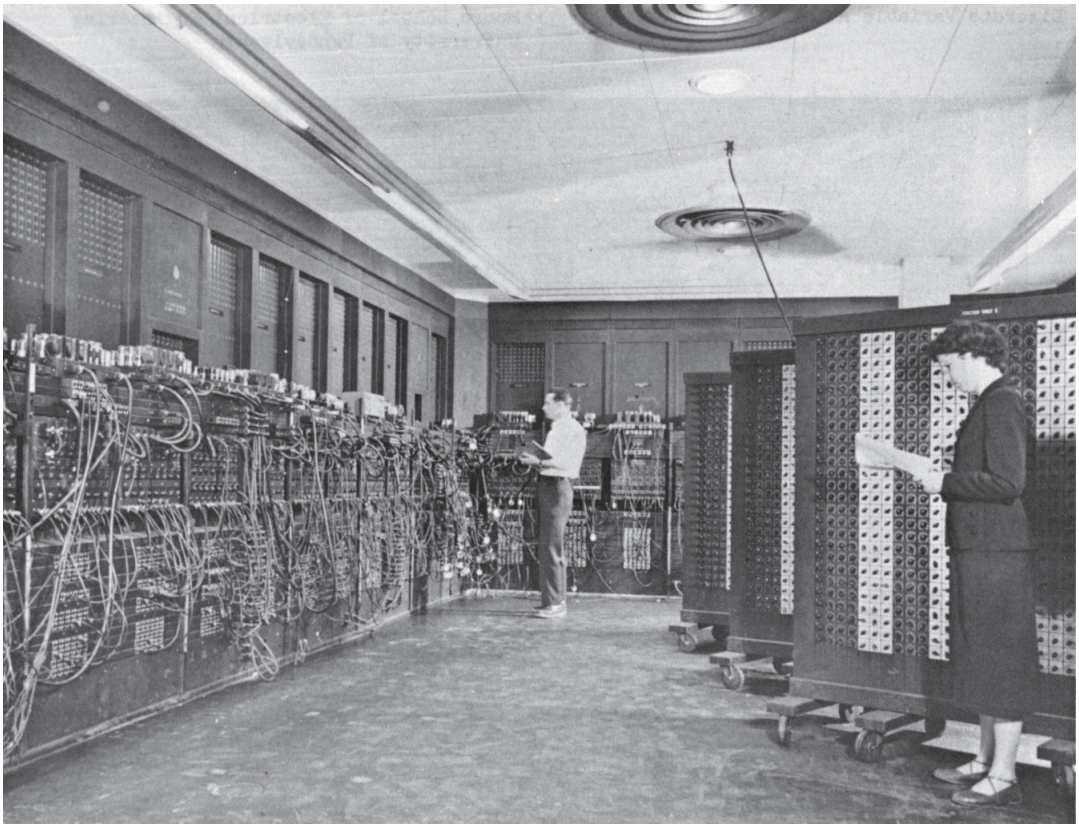
L'ENIAC reçu l'attention des journaux notamment à cause de sa taille imposante, mais d'une certaine manière, il n'est pas la fine fleur de son ère. Contrairement au Z3 de Konrad Zuse (1941) ou au MARK I de Howard Aiken (1944), il doit être recâblé pour exécuter un nouveau programme. De plus, l'ENIAC utilise des registres décimaux et non binaires.

L'ENIAC utilise des compteurs à anneaux à dix positions pour enregistrer les chiffres. L'arithmétique est réalisée en comptant les pulsations avec les anneaux et de générer des pulsations lorsque le compteur

[49] Le terme Turing-complet désigne, en informatique un système formel ayant au moins le pouvoir des machines de Turing : Un langage de programmation est dit Turing-complet s'il permet de représenter toutes les fonctions calculables au sens de Turing (nonobstant la finitude de la mémoire des ordinateurs actuels). La plupart des langages usuels de programmation (C, C++, Java, ...) sont Turing-complets. Le fait d'être Turing-complet est généralement un critère demandé d'un langage de programmation générique, par opposition à un langage dédié au traitement de problèmes spécifiques ; cependant, il s'agit d'une caractéristique qui peut être non souhaitable d'un langage de macro-définitions (le langage de templates du C++ est Turing-complet, sauf à appliquer une limitation de profondeur des instanciations (remplacement d'une variable par une constante)).

fait un tour. L'idée revient en fait à émuler par l'électronique les systèmes de roue à chiffres de machine mécaniques.

Sa capacité est de 20 nombres à dix chiffres signés permettant chacun de réaliser 5000 additions simples chaque seconde (pour un total de 100 000 additions par seconde). Il ne peut en revanche gérer que 357 multiplications ou 38 divisions par seconde.



Physiquement l'ENIAC est un monstre, il contient 17 468 tubes à vide, 7 200 diodes à cristal, 1500 relais, 70 000 résistances, 10 000 condensateurs et environ 5 millions de points soudés à la main. Son poids est de 30 tonnes pour des dimensions de 2,4 x 0,9 x 30,5 mètres occupant un espace de 167 mètres carrés. Sa consommation est de 160 kilowatts.

Il utilise des tubes à vide en base huit, les accumulateurs décimaux sont réalisés avec des flip-flops 6SN7, alors que les fonctions logiques utilisent des 6L7, 6SJ7, 6SA7 et 6AC7. De nombreux 6L6 et 6V6 servent de relais pour acheminer les pulsations entre les différents racks d'éléments.

Certains experts en électronique prédirent que les tubes tomberaient en panne si fréquemment que la machine en serait inutilisable. La prédiction n'était que partiellement correcte, de nombreux tubes brûlaient chaque jour laissant l'ENIAC inopérant la moitié du temps. Des lampes plus fiables ne furent pas disponibles avant 1948, Eckert et Mauchly durent donc utiliser des tubes de qualité standard. La plupart des problèmes liés aux tubes se produisent au démarrage ou à l'arrêt de la machine, car ils sont soumis à un important stress thermique. Le simple fait de ne jamais couper la machine, permet aux ingénieurs de réduire le nombre de pannes à un ou deux tubes par jour. La plus longue période de calcul sans panne est atteinte en 1954 avec 116 heures, ce qui est une prouesse compte tenu de la technologie de l'époque.

L'ENIAC fonctionne jusqu'au 2 octobre 1955. L'architecture décidée et gelée dès 1943, ne permet pas de résoudre certains problèmes notamment l'incapacité d'enregistrer un programme. Toutefois, les idées produites par ce travail et l'impact sur des personnes telles John von Neumann ont profondément influé le développement des ordinateurs suivants (par exemple : EDVAC, EDSAC et SEAC. Certaines améliorations ont eu lieu, notamment un système primitif permettant d'enregistrer un programme dans

une mémoire en lecture seule, une idée proposée par von Neumann. Cette dernière modification ralentissait la vitesse de calcul d'un facteur six, mais la durée de reprogrammation passait de plusieurs jours à quelques heures.

Ecker et Mauchly fondent une société, Eckert-Mauchly Computer Corporation, et produisent le premier ordinateur en 1949 : le BINAC. La firme est rachetée l'année suivante par Remington Rand et renommée Univac.

• 1947 : Invention du transistor par William Shocley et Walter Brattain dans les laboratoires de Bell.

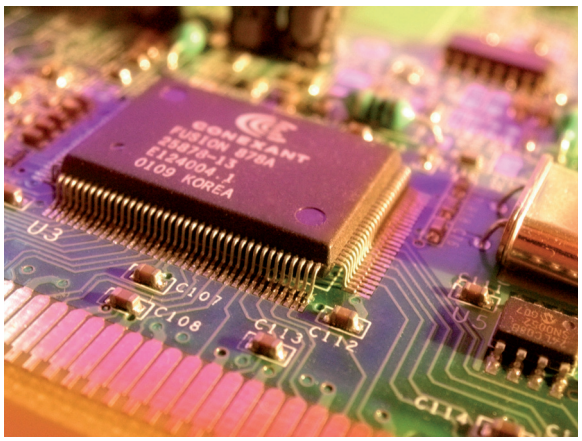
• 1955 : Premier réseau de téléscripteurs : SABRE (Semi Automated Business Related Environment) réseau à but commercial réalisé par IBM. Il relie 1200 téléscripteurs à travers les États-Unis pour la réservation des vols de la compagnie American Airlines.

• 1957 : Suite au lancement du premier Spoutnik par les Soviétiques, le président Dwight D. Eisenhower crée l'ARPA (Advanced Research Project Agency) au sein du DoD (Department of Defense) pour piloter un certain nombre de projets dans le but d'assurer aux USA la supériorité scientifique et technique sur leurs voisins Russes. Cette organisation regroupait certains des plus brillants cerveaux américains qui développèrent le premier satellite opérationnel des US en 18 mois. Quelques années après, l'ARPA commença à s'intéresser aux réseaux d'ordinateurs et aux technologies de la communication.

• Juillet 1958 : Le premier bunker du réseau SAGE (système de défense américain) devient opérationnel. L'ordinateur AN/FSQ7 dans chaque bunker est capable de gérer 400 avions simultanément. Le dernier bunker du réseau SAGE fermera en Janvier 1984.

• 1958 : La BELL crée le premier Modem[50] permettant de transmettre des données binaires sur une simple ligne téléphonique.

•1958 : Invention du circuit intégré. Jack Kilby (1923–2005) est l'inventeur du circuit intégré. En 1958, cet Américain, alors employé par Texas Instruments, créait le tout premier circuit intégré, jetant ainsi les bases du matériel informatique moderne. Pour la petite histoire, Jack Kilby, qui venait de rejoindre la compagnie, a fait cette découverte alors que la plupart de ses collègues profitaient de vacances organisées par Texas Instruments. À l'époque, Kilby avait tout simplement relié entre eux différents transistors en les câblant à la main. Il ne faudra par la suite que quelques mois pour passer du stade de prototype à la production de masse de puces en silicium contenant plusieurs transistors. Cette découverte a valu à Kilby un prix Nobel de physique en 2000, alors que ce dernier siégeait toujours au directoire de Texas Instruments et détenait plus de 60 brevets à son nom.



Circuits intégrés analogiques. Les composants les plus simples peuvent être de simples transistors encapsulés les uns à côté des autres sans liaison entre eux, jusqu'à des assemblages réunissant toutes les fonctions requises pour le fonctionnement d'un appareil dont il est le seul composant.

Les amplificateurs opérationnels sont des représentants de moyenne complexité de cette grande famille où l'on retrouve aussi des composants réservés à l'électronique haute fréquence et de télécommunication.

[50] Le modem (mot-valise de modulateur-démodulateur), est un périphérique servant à communiquer avec des utilisateurs distants. Il permet d'échanger (envoi/réception) des fichiers, des fax, de se connecter à Internet, de recevoir et d'émettre des e-mails. Il peut également être défini comme un acronyme. Techniquement, l'appareil sert à convertir les données numériques de l'ordinateur en données analogiques transmissibles par une ligne de téléphone classique et réciproquement.

Un exemple de circuit analogique : l'ampli op LM741 et une ribambelle de cousins.

Circuits intégrés numériques. Les circuits intégrés numériques les plus simples sont des portes logiques (et, ou, non), les plus complexes sont les microprocesseurs et les plus denses sont les mémoires. On trouve de nombreux circuits intégrés dédiés à des applications spécifiques (ASIC pour Application Specific Integrated Circuit), notamment pour le traitement du signal (traitement d'image, compression vidéo...) on parle alors de DSP (pour Digital Signal Processor). Une famille importante de circuits intégrés est celle des composants de logique programmable (FPGA, CPLD). Ces composants sont amenés à remplacer les portes logiques simples en raison de leur grande densité d'intégration.

• Juillet 1961 : Leonard Kleinrock du Massachusetts Institute of Technology (MIT) publie une première théorie sur l'utilisation de la commutation de paquets pour transférer des données.

• Octobre 1962 : En 1962, alors que le communisme faisait force, l'US Air Force demande à un petit groupe de chercheurs de créer un réseau de communication militaire capable de résister à une attaque nucléaire. Le concept de ce réseau reposait sur un système décentralisé, permettant au réseau de fonctionner malgré la destruction d'une une ou plusieurs machines.

Le docteur J.C.R. Licklider du MIT est nommé à l'ARPA pour diriger les recherches pour une meilleure utilisation militaire de l'informatique. Il avait écrit en août une série de notes décrivant sa vision d'un « réseau galactique » permettant à toute personne d'accéder rapidement à toute information ou tout programme, où qu'il se trouve. Il convaincra ses successeurs, Ivan Sutherland, Bob Taylor et Lawrence G. Roberts du MIT de l'importance de ce concept de réseau. Licklider était un visionnaire qui chercha à rendre l'utilisation des ordinateurs par le gouvernement plus interactive. Pour que la technologie s'étende rapidement, Licklider vit qu'il fallait sortir les contrats de l'ARPA du domaine privé au profit des Universités. Ce faisant, il mit en place des collaborations qui seront les fondations de ce qui deviendrait l'ARPANet.

• 1962 : Engelbart du « Stanford Research Lab » définit les bases du traitement de texte (copie et suppression de caractères/mots/blocs, césure automatique, macros…)

• 1963 : L'American National Standards Institute crée le code ASCII (American Standard Code for Information Interchange)

• 1964 : Leonard Kleinrock du MIT publie un livre sur la communication par commutation de paquets. Il va convaincre Lawrence G. Roberts du bien fondé de l'utilisation de la commutation de paquets plutôt que de circuits dédiés pour réaliser un réseau.

• 1965 : Lawrence G. Roberts va, avec Thomas Merill, connecter l'ordinateur TX-2 au Massachussets avec l'ordinateur Q-32 en Californie par une liaison téléphonique. Cette expérience va prouver la faisabilité et l'utilité d'un réseau d'ordinateurs. Elle va aussi achever de convaincre Roberts de la supériorité de la commutation de paquet par rapport à l'utilisation de circuits dédiés comme ce fût le cas dans cette expérience.

• 1965 : Ted Nelson invente le mot « hypertexte ». Par « hypertexte » il entend « écriture non séquentielle » c'est-à-dire un texte avec des embranchements qui laisserait à l'utilisateur le choix de sa lecture de façon interactive. Il parle bientôt d'hypermédia entendant par là que la technique peut s'étendre à tous les types de médias.

• 1965 : TVEdit du « Stanford Research Lab » est l'un des premiers éditeurs de texte

• 1966 : Douglass Engelbart crée un nouveau périphérique : la souris.

Une souris est un dispositif de pointage relatif manuel pour ordinateur ; elle est composée d'un petit boîtier fait pour tenir sous

la main, sur lequel se trouvent un ou plusieurs (généralement deux) boutons. La souris a été inventée en 1963 par Douglas Engelbart du Stanford Research Institute après des tests d'utilisation, basés sur le trackball[51]. Elle a été améliorée par Jean-Daniel Nicoud à l'EPFL dès 1979 grâce à l'adjonction d'une boule et de capteurs ; il fabrique la souris Depraz qui a été à l'origine de l'entreprise Logitech.

Les premières souris étaient en fait de simples trackballs inversées, où l'utilisateur déplaçait l'appareil. La friction de la boule contre la table permettait le mouvement du pointeur sur l'écran. Depuis, les souris utilisent plutôt des dispositifs optiques, voire à inertie, pour détecter les mouvements : le système de boule avait tendance en effet à ramasser la poussière de la surface horizontale et à encrasser les rouleaux capteurs, ce qui exigeait un nettoyage interne régulier et fastidieux.

• 1967 : Lawrence G. Roberts, récemment arrivé à la tête du projet de réseau informatique à l'ARPA, publie ses « Plans pour le réseau ARPANET » au cours d'une conférence. Lors de cette conférence sera aussi publié un papier sur un concept de réseau à commutation de paquets par Donald Davies et Robert Scantlebury du NPL (National Physical Laboratory – Royaume-Uni) et également un papier de Paul Baran[52] de la Rand Corporation (militaires) au sujet de l'utilisation d'un réseau à commutation de paquet pour transmission sécurisée de la voix. Les militaires s'inquiétaient de voir les dirigeants privés de communication si la guerre froide venait à se réchauffer et que les lignes de téléphones disparaissaient en fumée radioactive après un bombardement. Ainsi, le projet de la Rand s'intéressait à l'idée des paquets passant de nœud en nœud ayant la même autorité sans système central, une anarchie technologique qui même en cas de destruction partielle du réseau, en cas de guerre nucléaire pourrait continuer à fonctionner. Il est amusant de noter que ces groupes ont travaillé en parallèle sur des concepts similaires et sans avoir connaissance des travaux des autres pour aboutir en même temps à la même conclusion !

C'est aussi à cause de la similitude entre le projet de la RAND et le projet de l'ARPA qu'est née la fausse rumeur selon laquelle le réseau ARPANET avait été lancé à cause du besoin de relier les ordinateurs entre eux par un réseau insensible aux destructions d'une guerre nucléaire.

• 1967 : Andy van Dam et deux étudiants de l'université de Brown et financés par IBM développent le premier éditeur d'hypertexte. Il sera utilisé pour produire la documentation du projet spatial Apollo. Leur système utilisait le stylo optique.

• Juillet 1968 : Gordon Moore, Robert Noyce et Andrew Grove créent Intel (INTegrated Electronics)

• Août 1968 : Lawrence G. Roberts et la communauté de chercheurs « sponsorisée » par l'ARPA ont défini la structure et les spécifications du futur réseau ARPANET. Ils lancent un appel d'offres pour la réalisation d'un composant clé du réseau : le commutateur de paquet appelé aussi IMP (Interface Mes-

[51] Une boule de commande (en anglais, trackball) est un outil informatique permettant de déplacer des objets virtuels sur un écran, en fonction des déplacements d'une sphère intégrée dans cet outil. Le principe de fonctionnement en est très simple : la boule repose partiellement dans une alvéole reposant sur des roulettes méridiennes laissant la boule rouler librement. Deux roulettes principales sont reliées à des détecteurs de mouvements et traduisent en signaux numériques les déplacements de la surface de la boule. Les deux capteurs sont orientés à 90° l'un par rapport à l'autre ; l'un capte et transmet les mouvements en abscisse, l'autre les mouvements en ordonnée. L'utilisateur fait « rouler » la partie émergée de la boule (généralement avec la paume de sa main), et différents boutons, placés à des endroits accessibles par le bout des doigts, permettant de sélectionner des actions. Dans le domaine militaire, elle est utilisée pour le pointage radar. Dans le domaine public elle est plutôt utilisée en CAO.

[52] Paul Baran est considéré comme un des acteurs principaux de la création d'Internet. Il eu l'idée, en 1964, de créer un réseau sous forme de grande toile. Il avait réalisé qu'un système centralisé était vulnérable car la destruction de son noyau provoquait l'anéantissement des communications. Il mit donc au point un réseau hybride d'architectures étoilées et maillées dans lequel les données se déplaceraient de façon dynamique, en « cherchant » le chemin le moins encombré, et en « patientant » si toutes les routes étaient encombrées. Cette technologie fut appelée « *packet switching* ».

sage Processor). La société de consultants BBN (Bolt Beranek and Newman) remportera l'appel d'offres en décembre 1968.

• 1968 : Le système NLS de Engelbart du « Stanford Research Lab » utilise non seulement la notion de liens, mais aussi l'édition à la souris.

En avril 1969, nous sommes dans une Amérique plongée dans la lutte contre la guerre du Vietnam. Le mouvement hippie, né de cette mobilisation, est à son apogée. Trois mois plus tard aura lieu le concert gratuit des *Rolling-Stones* à Hyde Park, un mois avant Woodstock. Dans toute l'Amérique, un an après mai 68 (au moment où, en France, De Gaulle démissionne), partout des mouvements se créent, cherchant par tous les moyens à se démarquer de la société de consommation, de ses règles et de ses conventions.

C'est à la fin de ce mois d'avril que Stephen Crocker, étudiant de l'UCLA, rédige la RFC[53] numéro 3, complétée en juillet par la RFC numéro 10.

Le mois précédent, en effet, le « Network Working Group » (groupe informel formé par Crocker et réunissant en dehors de toute directive hiérarchique quelques jeunes chercheurs — dont Vinton Cerf et Jon Postel — travaillant dans la recherche sur les protocoles de communication de serveur à serveur) avait adopté le principe d'enregistrer, lors de ses réunions, toutes les remarques, commentaires et propositions des participants. Les « appels à commentaires » (Request For Comment, RFC) naissent à cette occasion. Jon Postel en assure la diffusion auprès de toutes les personnes impliquées dans le projet ARPANET.

Un RFC, ainsi que le définit les RFC 3 et 10, est conçu comme un système de « documentation ouverte » : toute pensée, toute suggestion relative au logiciel de serveur, écrite par n'importe qui et sans respecter les règles de l'écriture scientifique peut être publiée dans une RFC ». Aucune direction n'est imposée, aucun contrôle : la méthode de travail qui a permis Internet et continue à ce jour d'en développer les futurs protocoles est volontairement libertaire.

L'objectif avoué était d'encourager la créativité et la communication entre les membres du projet. Mais, né dans cette période si particulière de notre histoire, et grâce à leur caractère ouvert, non hiérarchique, souple et informel, les RFC vont rapidement obtenir pas consensus un statut normatif, définissant tant les normes de développement que les standards ouverts dont devront se servir tous ceux qui voudront développer ou améliorer un nouveau protocole (en publiant un nouveau RFC).

Il est à noter qu'un RFC, pour être publié, doit comporter un exemple « libre de droits » d'implémentation. C'est sans doute là qu'on pourra trouver une des raisons principales du développement parallèle des logiciels libres et de l'Internet.

• Septembre 1969 : Les premiers résultats visibles de l'approche de Licklider furent la connexion UCLA (*University of California*, Los Angeles) Stanford: BBN installe le premier équipement réseau IMP (basé sur un mini-ordinateur Honeywell 516 avec 12 Ko de Ram) à l'UCLA et le premier ordinateur (XDS SIGMA 7) y est connecté. Un ordinateur (XDS 940) de l'équipe de Douglas C. Engelbart du *Stanford Research Institute* est alors relié via une liaison à 50 kbits/s. Les premières données sont échangées entre ces machines. Peu après, un ordinateur (IBM 360/75) situé à l'*université de Santa Barbara* et un autre (Dec PDP-10) situé à l'*université de l'Utah à Salt Lake City* sont raccordés. Le réseau ARPANET initial constitué de 4 ordinateurs est alors en fonctionnement fin 1969.

[53] Les request for comment (RFC), littéralement demande de commentaires, sont une série de documents et normes concernant l'Internet, commencées en 1969. Peu de RFC sont des standards, mais tous les standards de l'Internet sont enregistrés en tant que RFC. Les RFC sont rédigées sur l'initiative d'experts techniques, puis sont revues par la communauté Internet dans son ensemble. Cela diffère d'une publication d'institution telle que l'ANSI. Pour cette raison, elles continuent à être appelées RFCs une fois devenues des standards.

Lors d'une interview, le professeur Kleinrock de l'UCLA raconta la première expérience réalisée avec ce réseau : se connecter à l'ordinateur de la SRI depuis celui de l'UCLA en tapant LOGIN :

Nous avons appelé les gens de SRI par téléphone.
Nous avons alors tapé L puis demandé au téléphone « Vous voyez le L ? »
La réponse vint alors : « Oui, nous voyons le L »
Nous avons alors tapé O puis redemandé au téléphone « Vous voyez le O ? »
« Oui, nous voyons le O »
Nous avons alors tapé G et tout le système a crashé !...

Le réseau ARPANET est aujourd'hui considéré comme le réseau précurseur d'internet. Il comportait déjà à l'époque certaines caractéristiques fondamentales du réseau actuel :

- Un ou plusieurs nœuds du réseau pouvaient être détruits sans perturber son fonctionnement ;
- La communication entre machines se faisait sans machine centralisée intermédiaire ;
- Les protocoles utilisés étaient basiques.

• 1969 : Création de la norme de connexion série RS232. RS-232 (aussi appelé EIA RS-232C ou V24) est une norme standardisant un port de communication de type série. Disponible sur tous les PC, il est communément appelé le « port série ». Sur le système d'exploitation MS-DOS qui équipait les PC, les ports RS-232 étaient désignés par les noms COM1, COM2, etc. Cela leur a aussi valu le surnom de « ports COM », encore utilisé de nos jours. Il est fréquemment utilisé dans l'industrie pour connecter différents appareils électroniques (automate, appareil de mesure, etc..).

• Décembre 1970 : Le Network Working Group sous la direction de Steve Crocker termine le protocole de communication entre ordinateurs pour le réseau ARPANET appelé Network Control Protocol ou NCP. De nouveaux ordinateurs furent rapidement branchés sur ARPANET et l'implémentation de NCP sur la période 1971-1972 permit aux utilisateurs de ce réseau de développer les premières applications.

Le protocole de communication

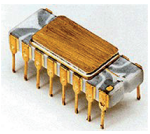
La connexion d'ordinateurs par le moyen de réseaux informatiques nécessite de mettre au point ce que l'on appelle un protocole de communication. En effet, pour assurer la communication entre deux ordinateurs, il faut que ceux-ci puissent parler « la même langue ». Or, si justement les ordinateurs issus de firmes informatiques concurrentes ne peuvent échanger directement des ressources, c'est parce que ceux-ci ne parlent pas le même langage. Et ce que les ingénieurs d'Arpanet proposent en fait, c'est d'implanter dans les ordinateurs un langage qui leur serait commun une fois en réseau. Dès lors, chaque ordinateur posséderait son propre langage pour les tâches particulières qu'il doit exécuter, mais une fois connectés en réseau, tous se mettraient à discuter dans la même langue. Le NCP XXX sera ce premier protocole.

Comme le montre J.-C. Guénon, l'idée du protocole de communication est similaire à celui du projet de l'espéranto. En effet, il est plus pratique pour les individus d'apprendre tous une langue commune plutôt que d'en apprendre plusieurs si on veut instaurer une communication dans un groupe de personnes qui s'expriment tous dans des langues différentes.

• Avril 1971 : À cette époque, le réseau ARPANET est constitué de 23 ordinateurs sur 15 sites différents reliés par des liaisons à 50 kbits/s.

• 1971 : Larry Roberts du DARPA se dit que les gens avaient besoin d'être motivés pour bouger. En octobre 1972 il y aurait une conférence internationale sur les communications entre ordinateurs. Larry demanda à Bob Kahn du BBN d'organiser une démonstration publique de l'ARPANET. Cela prendra

un an à Bob pour que tout le monde soit suffisamment avancé pour pouvoir présenter un ensemble d'applications sur l'ARPANET. L'idée consistait à installer un « packet switch » et un terminal (TIP Terminal Interface Processor) au sous-sol de l'hôtel Hilton de Washington et laisser le public venir utiliser l'ARPANET en lançant des applications n'importe où aux États unis.



• 1971 : Intel invente et commercialise le premier microprocesseur : Le 4004 108 KHz

L'Intel 4004 conçu par l'ingénieur inventeur Marcian Hoff en 1971 est considéré comme le premier microprocesseur du monde.

En 1969, la société japonaise Busicom, premier gros client d'Intel (fondé la même année), désire développer une gamme de calculateurs programmables de calculatrices de grande puissance, et demande à Intel de fabriquer un jeu de douze circuits intégrés qui leur sont nécessaires. Intel charge son ingénieur Marcian Hoff (surnomé Ted Hoff) assisté par Federico Faggin et Stan Mazor d'Intel et Masatoshi Shima de Busicom de ce projet. Ce dernier propose à ses collaborateurs et clients l'idée révolutionnaire de développer un circuit intégré universel sur une seule puce au lieu des circuits personnalisés spécialisés demandés pour chaque projet développé à l'époque. Intel vend le microprocesseur et les droits exclusifs du Intel 4004 à son client Japonais Busicom pour 60 000 dollars.

Par chance pour Intel, la firme Busicom connaît rapidement des problèmes de trésorerie et demande à Intel de renégocier son contrat de partenariat. Intel, accepte de rembourser les 60 000 dollars de frais de recherche en contrepartie de la totalité des droits industriels et commerciaux sur le Intel 4004 de Ted Hoff, à l'exception de ceux pour les sociétés fabriquant des calculatrices de bureau ou de poche.

Deuxième coup de chance pour Intel avec l'arrivé du tout nouveau directeur commercial, Ed Gelbach issu de la société Texas Instruments qui perçoit rapidement le potentiel de développement fantastique des microprocesseurs de type Intel 4004

Bien que le 4004 soit largement considéré comme le premier microprocesseur, une autre modèle à été développé un an avant en 1970 par Ray Holt de la société américaine *Central Air Data Computer* pour équiper l'avion de chasse militaire F-14 Tomcat de l'avionneur Grumman.

• Mars 1972 : Ray Tomlinson de BBN réalise la première application réseau majeure pour ARPANET : un logiciel basique de courrier électronique répondant au besoin de communication des développeurs du réseau. Ce dernier, qui travaille sur des programmes permettant d'envoyer des messages sur le réseau et de les lire, développe un code pour envoyer un message d'un ordinateur à l'autre. Pour définir l'adresse, il a alors besoin d'un séparateur entre le nom et la « résidence » du destinataire. Il opte alors pour l'arobase qui possède le double avantage d'être inutilisé et de se prononcer « at » en anglais, ce qui dans ce contexte équivaut en français à « chez ». Loin du contenu solennel des premiers messages télégraphiques ou téléphoniques, ce premier message n'aurait eu pour texte que la première ligne d'un clavier QWERTY…

• Juillet 1972 : Lawrence G. Roberts améliore les possibilités du courrier électronique en écrivant un logiciel permettant de lister, lire sélectivement, archiver, répondre ou faire suivre son e-mail. À partir de cet instant, la messagerie électronique va devenir pour les dix années qui vont suivre l'application réseau majeure.

• Octobre 1972 : La démonstration publique du réseau ARPANET est réalisée lors de la première conférence sur les communications informatiques à Washington. Un IMP et 40 terminaux sont raccordés au réseau pour la durée de la conférence. La démonstration est un énorme succès. Plusieurs pays se mettent d'accord sur la nécessité de mettre en place des protocoles de communication communs, ce qui mena à la création du groupe de travail INWG (InterNetwork Working Group), dirigé par Vinton Cerf.

• 1972 : L'ARPA est renommé DARPA (*Defense Advanced Research Projects Agency*).

• 1972 : Le succès du programme d'e-mail sur ARPANET a presque aussitôt entraîné la création des mailing-lists (listes de diffusion). L'une des premières mailing-list avec un volume de messages très important fut *SF-LOVERS*, dédiée à la discussion entre fans de Science Fiction.

• 1972 – 1973 : Bob Kahn travaille au sein du DARPA sur un projet de commutation de paquets par radio ce qui nécessite la création d'un nouveau protocole capable de transmettre les paquets d'informations, quelles que soient les perturbations radio. Ayant été un architecte majeur de l'ARPANET, il envisagea d'utiliser NCP (protocole réseau de l'ARPANET). Mais ce protocole étant insuffisant (pas de contrôle d'erreur, pas de possibilité d'adresser des machines au-delà d'un IMP (équipement réseau). Il décida alors, en collaboration avec Vinton Cerf, chercheur à Stanford, de réaliser un nouveau protocole répondant à ce cahier des charges et permettant de relier les réseaux (internetting). C'est ainsi que fut créé TCP (*Transmission Control Protocol*). Les applications Telnet et FTP sont aussi spécifiées dans ces années, elles permettront respectivement d'ouvrir une session sur une machine distante pour y exécuter des programmes et de copier des fichiers depuis ou vers une machine distante…

Louis Pouzin est un ingénieur français en informatique né en 1931 à Chantenay-Saint-Imbert (Nièvre). Il a été diplômé de Polytechnique en 1950.

Pour Météo France, il travaille à la programmation du calculateur et conçoit un système d'exploitation qui restera quinze ans en service.

Louis Pouzin est inventeur du *datagramme* et concepteur du premier réseau à commutation de paquets, innovation essentielle du concept du réseau Internet. Le projet Cyclades, et concepteur des premières formes d'interpréteur de commandes. Ses travaux ont été largement utilisés par Vinton Cerf pour la mise au point d'Internet et du protocole TCP/IP.

• Janvier 1973 : À cette date, 35 machines sont maintenant connectées sur le réseau ARPANET. Une première liaison satellite est mise en place pour raccorder l'Université de Hawai sur le réseau.

• 1973 : Robert Metcalfe met au point l'interface réseau Ethernet chez Xerox en s'inspirant des principes du réseau informatique radio de l'université de Hawai : *Alohanet*.

• Septembre 1973 : Un premier article sur TCP fut publié par ces deux chercheurs lors d'une conférence de l'International Network Working Group (INWG).

• 1974 : La société BBN lance Telenet, le premier réseau à commutation de paquets à usage commercial (utilisation des technologies employées sur ARPANET)

• Mai 1974 : Article sur TCP dans « *IEEE Transaction on Communications* » revue phare de ce domaine de recherche

• Décembre 1974 : Premières spécifications complètes de TCP

• Janvier 1975 : Le magazine Popular Electronics présente le premier ordinateur (en fait une unité centrale programmable) en kit. C'est le mythique Altair dont le succès marque un premier pas vers le micro-ordinateur à la portée de tous.

L'Altair 8800 du constructeur américain MITS est un micro-ordinateur basé sur le microprocesseur Intel 8080A x86 vendu en kit électronique à quelques milliers d'exemplaires pour les particuliers en 1975. Il est considéré comme le premier micro-ordinateur vendu aux particuliers de la gamme des ancêtres des compatibles PC. Il est le concurrent direct de l'Apple I de Steve Jobs et Steve Wozniak. Bill Gates et Paul Allen écrivent leur premier logiciel Altair Basic pour ce micro-ordinateur et créent pour l'occasion leur société Microsoft.

Ed Roberts et Forrest Mims, deux employés du centre de recherche en armement de l'US Air Force de la base aérienne Kirtland à Albuquerque au Nouveau-Mexique décident de concevoir un ordinateur pour particulier à la suite de l'échec de MITS dans le domaine des calculatrices. Ils ont eu la chance d'être

remarqués par un rédacteur de la célèbre revue électronique américaine *Popular electronics* dont ils firent la une. L'Altaïr était un micro-ordinateur en kit à base de microprocesseur x86 Intel 8080A pour amateur décliné d'un de leur projet professionnel en électronique de télémétrie : le Altair 8800

En 1975, deux pionniers de la micro-informatique, Bill Gates et son ami d'école Paul Allen découvrent le Altair 8800 dans la revue et proposent par courrier à la société MITS de développer le langage informatique Altair Basic pour cette machine. Ed Roberts accepte et les deux amis développent leur BASIC en trente jours en travaillant 24 heures sur 24 à Boston sur un simulateur PDP-10.

Une fois la version au point en octobre 1975, Paul Allen s'envole pour Albuquerque au Nouveau-Mexique pour rencontrer son client et lui faire une démonstration de leur Altair Basic avec succès. Miraculeusement l'essai a fonctionné du premier coup alors que leur langage n'a jamais été testé sur un vrai Altair 8800 et qu'il est sauvegardé sur ruban perforé. Paul Allen et Bill Gates fondent alors immédiatement sur place la société Microsoft et passent un accord de commercialisation avec MITS pour toucher 35 dollars de revenu par copie de leur logiciel vendu avec un Altair 8800. La légende de Microsoft est née.

• 1975 : Premières implémentations concurrentes de TCP à Stanford, BBN, et Université de Londres. L'effort de développement des protocoles internet ont été dès leur origine internationaux.

Jusque vers le milieu des années 70, le protocole TCP contenait en fait les deux protocoles TCP et IP. Il va se scinder en deux le couple étant connu sous l'appellation TCP/IP et un troisième protocole apparaît UDP. IP (Internet Protocol) s'occupe de l'adressage et du transfert de paquets individuels entre deux points du réseau. Sur IP se basent deux protocoles de communication. TCP (Transfer Control Protocol) qui s'assure du bon acheminement des paquets, corrige les erreurs et les pertes… (circuits virtuels). UDP (User Datagram Protocol) qui lui donne directement accès aux services de IP et laisse le soin à l'application de gérer sa communication. Le protocole IP se stabilisera a sa quatrième version appelée IP v4 en 1978.

TCP/IP est un protocole, c'est-à-dire des règles de communication.

IP signifie Internet Protocol : littéralement « le protocole d'Internet ». C'est le principal protocole utilisé sur Internet.

Le protocole IP permet aux ordinateurs reliés à ces réseaux de dialoguer entre eux.

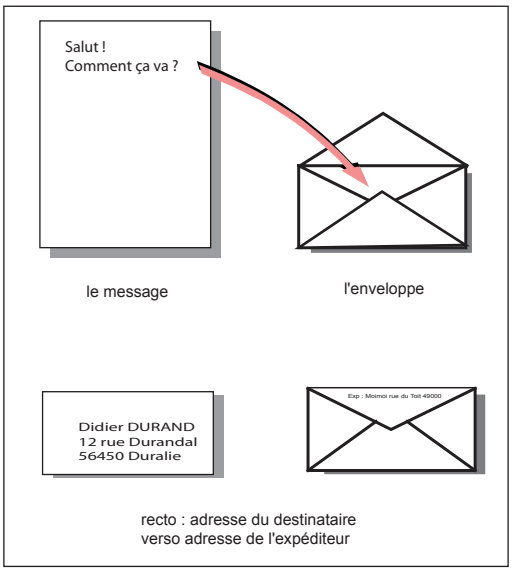
Faisons un parallèle avec la poste.

Quand vous voulez envoyer une lettre par la poste :

• vous placez votre lettre dans une enveloppe,

• sur le recto, vous inscrivez l'adresse du destinataire,

• au dos, vous écrivez l'adresse de l'expéditeur (la vôtre).



Ce sont des règles utilisées par tout le monde. C'est un protocole.

Sur Internet, c'est à peu près la même chose : chaque message (chaque petit paquet de données) est enveloppé par IP qui y ajoute différentes informations :

• l'adresse de l'expéditeur (votre adresse IP),

• l'adresse IP du destinataire,

• différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message).

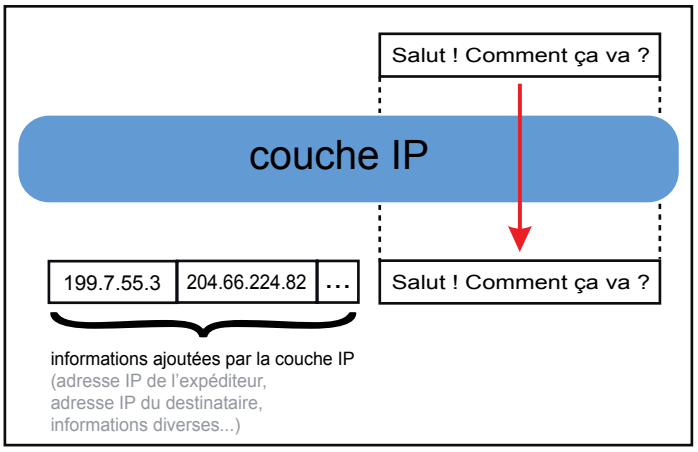
L'adresse IP est une adresse unique attribuée à chaque ordinateur sur Internet (c'est-à-dire qu'il n'existe pas sur

Internet deux ordinateurs ayant la même adresse IP).

De même, l'adresse postale (nom, prénom, rue, numéro, code postal et ville) permet d'identifier de manière unique un destinataire.

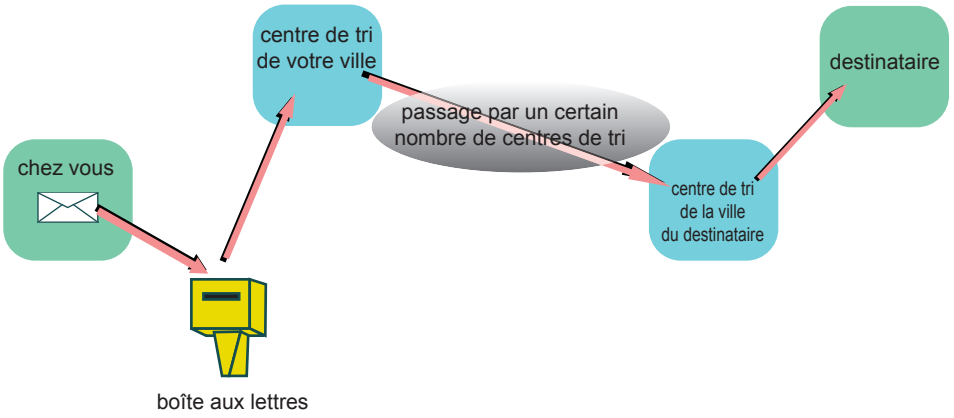
Tout comme avec l'adresse postale, il faut connaître au préalable l'adresse IP de l'ordinateur avec lequel vous voulez communiquer.

L'adresse IP se présente le plus souvent sous forme de 4 nombres (entre 0 et 255) séparés par des points. Par exemple : 204.35.129.3



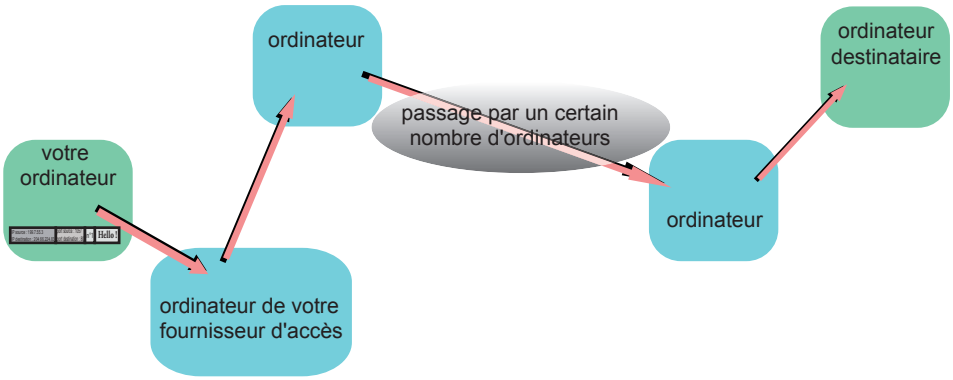
Le routage IP

Pour envoyer votre lettre, vous la postez dans la boîte aux lettres la plus proche. Ce courrier est relevé, envoyé au centre de tri de votre ville, puis transmis à d'autres centres de tri jusqu'à atteindre le destinataire.



C'est la même chose sur Internet !

Vous déposez le paquet IP sur l'ordinateur le plus proche (celui de votre fournisseur d'accès en général). Le paquet IP va transiter d'ordinateur en ordinateur jusqu'à atteindre le destinataire.



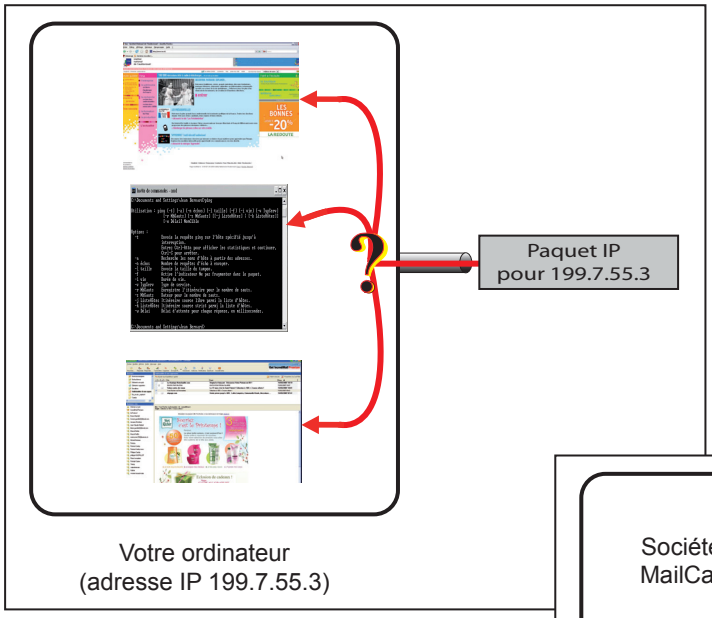
Les ports

Avec IP, nous avons de quoi envoyer et recevoir des paquets de données d'un ordinateur à l'autre.

Imaginons maintenant que nous ayons plusieurs programmes qui fonctionnent en même temps sur le même ordinateur : un navigateur, un logiciel d'e-mail et un logiciel pour écouter la radio sur Internet.

Si l'ordinateur reçoit un paquet IP, comment savoir à quel logiciel donner ce paquet IP ?

C'est un problème sérieux !

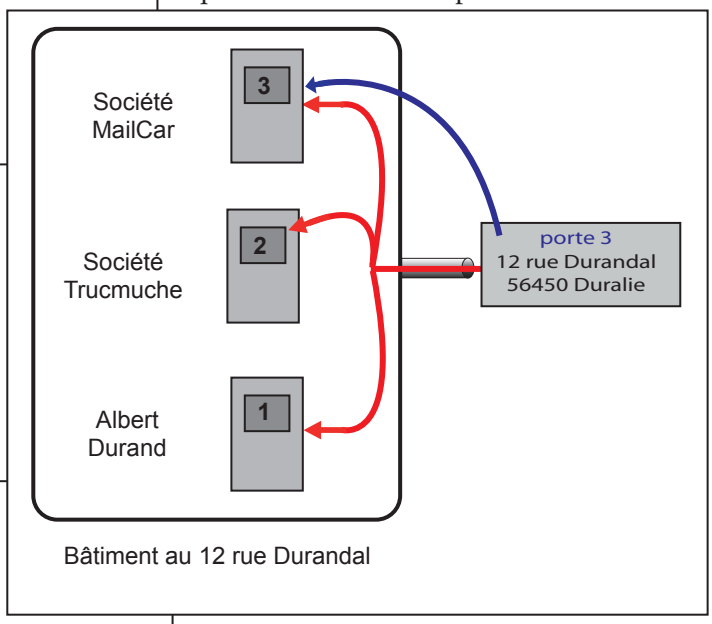


On pourrait attribuer un numéro unique à chaque logiciel dans l'ordinateur.

Il suffirait alors de mettre ce numéro dans chaque paquet IP pour pouvoir s'adresser à tel ou tel logiciel.

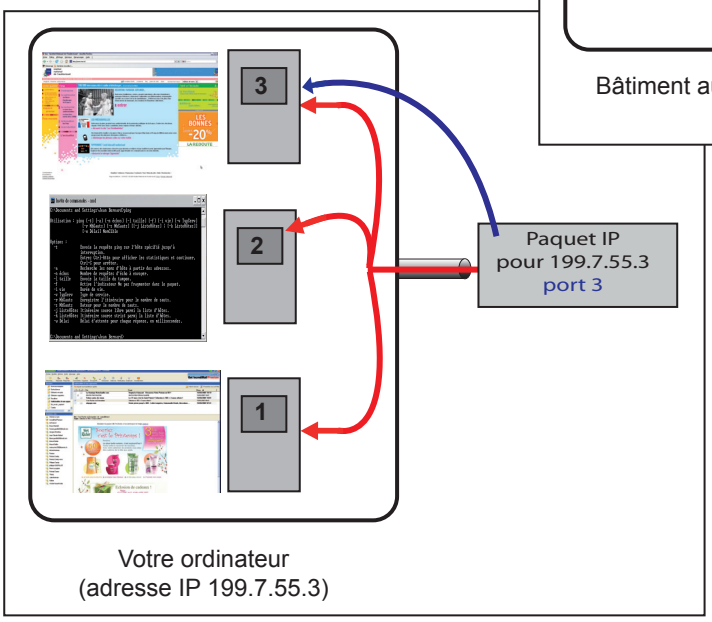
On appelle ces numéros des ports (pensez aux « portes » d'une maison : à une adresse donnée, on va pouvoir déposer les lettres à différentes portes à cette adresse).

Avec la poste, à une même adresse, on peut s'adresser à différentes personnes en indiquant un numéro de porte.



De même, à une même adresse IP, on peut s'adresser à différents logiciels en précisant le numéro de port (ici : 3).

Ainsi, l'adresse IP permet de s'adresser à un ordinateur donné, et le numéro de port permet de s'adresser à un logiciel particulier sur cet ordinateur.

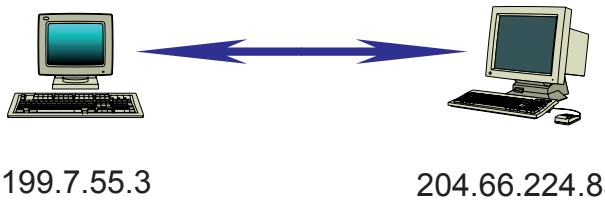


« Mais TCP/IP ? ». On y vient, on y vient... patience.

UDP/IP est un protocole qui permet justement d'utiliser des numéros de ports en plus des adresses IP (On l'appelle UDP/IP car il fonctionne au-dessus d'IP).

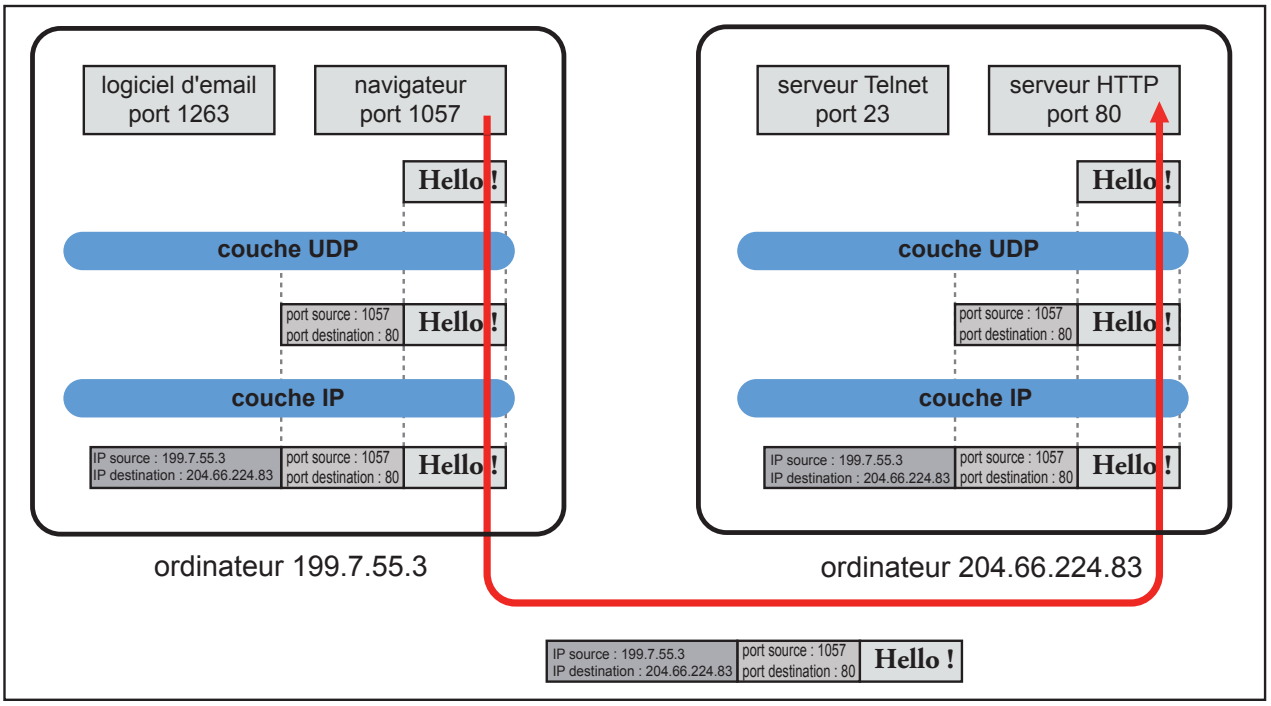
IP s'occupe des adresses IP et UDP s'occupe des ports.

Avec le protocole IP on pouvait envoyer des données d'un ordinateur A à un ordinateur B.



Avec UDP/IP, on peut être plus précis : on envoie des données d'une application x sur l'ordinateur A vers une application y sur l'ordinateur B.

Par exemple, votre navigateur peut envoyer un message à un serveur HTTP (un serveur Web) :



• Chaque couche (UDP et IP) va ajouter ses informations.

Les informations de IP vont permettre d'acheminer le paquet à destination du bon ordinateur. Une fois arrivée à l'ordinateur en question, la couche UDP va délivrer le paquet au bon logiciel (ici : au serveur HTTP).

• Les deux logiciels se contentent d'émettre et de recevoir des données (« Hello ! »). Les couches UDP et IP en dessous s'occupent de tout.

Ce couple (199.7.55.3 : 1057, 204.66.224.83 : 80) est appelé un socket. Un socket identifie de façon unique une communication entre deux logiciels.

Nous pouvons maintenant faire communiquer 2 logiciels situés sur des ordinateurs différents.

Mais il y a encore de petits problèmes :

• Quand vous envoyez un paquet IP sur Internet, il passe par des dizaines d'ordinateurs. Et il arrive que des paquets IP se perdent ou arrivent en double exemplaire.

Ça peut être gênant : imaginez un ordre de débit sur votre compte bancaire arrivant deux fois ou un ordre de crédit perdu !

• Même si le paquet arrive à destination, rien ne vous permet de savoir si le paquet est bien arrivé (aucun accusé de réception).

• La taille des paquets IP est limitée (environ 1500 octets).

Comment faire pour envoyer la photo JPEG du petit dernier qui fait 62000 octets ? (la photo... pas le bébé).

C'est pour cela qu'a été conçu TCP.

TCP est capable :

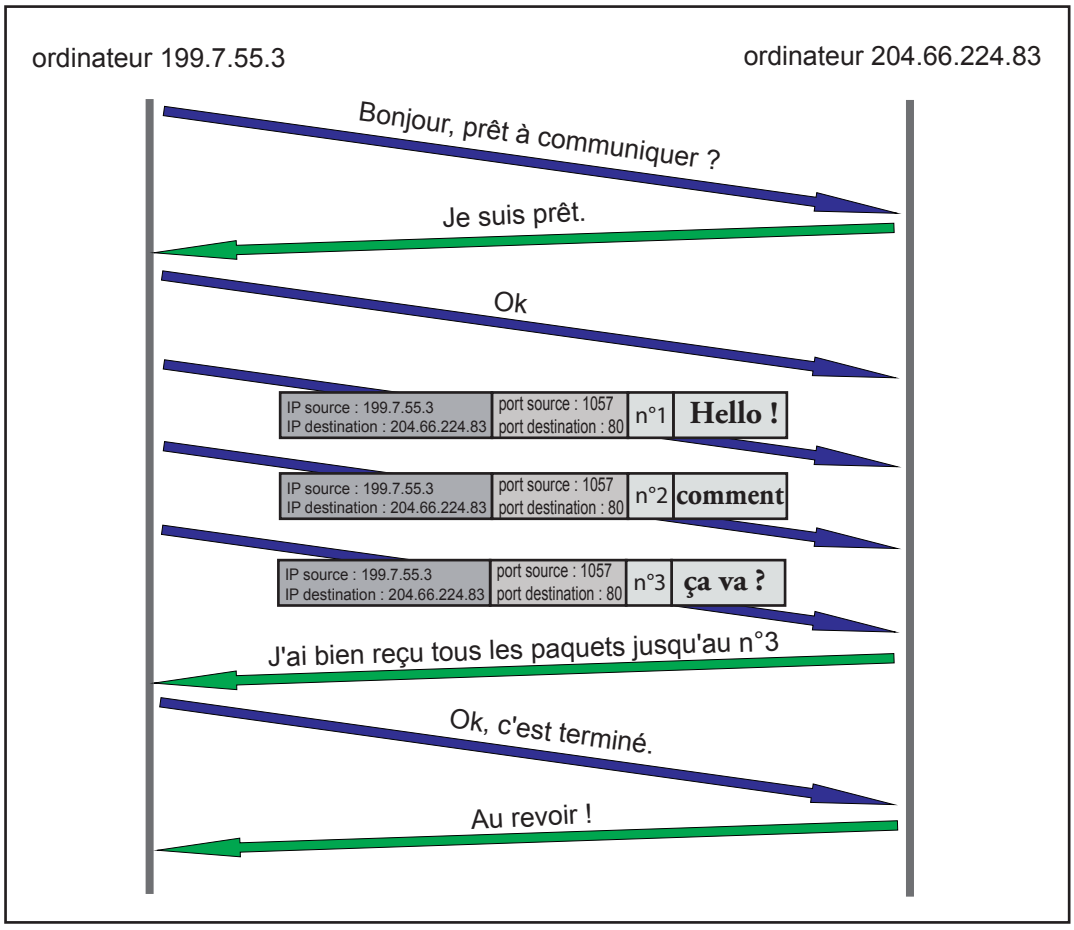
• de faire tout ce que UDP sait faire (ports).

• de vérifier que le destinataire est prêt à recevoir les données.

• de découper les gros paquets de données en paquets plus petits pour que IP les accepte

• de numéroter les paquets, et à la réception de vérifier qu'ils sont tous bien arrivés, de redemander les paquets manquants et de les réassembler avant de les donner aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées.

Par exemple, pour envoyer le message « Salut, comment ça va ? », voilà ce que fait TCP (Chaque flèche représente 1 paquet IP) :



À l'arrivée, sur l'ordinateur 204.66.224.83, la couche TCP reconstitue le message « Salut, comment ça va ? » à partir des 3 paquets IP reçus et le donne au logiciel qui est sur le port 80.

Avec TCP/IP, on peut maintenant communiquer de façon fiable entre logiciels situés sur des ordinateurs différents.

TCP/IP est utilisé pour des tas de choses :

• Dans votre navigateur, le protocole HTTP utilise le protocole TCP/IP pour envoyer et recevoir des pages HTML, des images GIF, JPG et toutes sortes d'autres données.

• FTP est un protocole qui permet d'envoyer et recevoir des fichiers. Il utilise également TCP/IP.

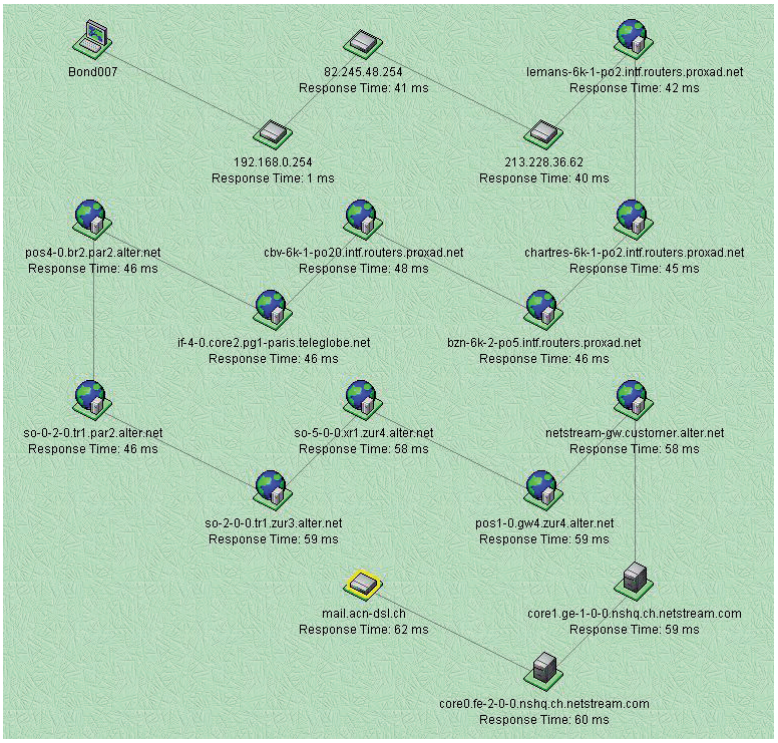
• Votre logiciel de courrier électronique utilise les protocoles SMTP et POP3 pour envoyer et recevoir des emails. SMTP et POP3 utilisent eux aussi TCP/IP.

• Votre navigateur (et d'autres logiciels) utilisent le protocole DNS pour trouver l'adresse IP d'un ordinateur à partir de son nom (par exemple, de trouver 216.32.74.52 à partir de « www.yahoo.com »). Le protocole DNS utilise UDP/IP et TCP/IP en fonction de ses besoins.

Il existe ainsi des centaines de protocoles différents qui utilisent TCP/IP ou UDP/IP.

L'avantage de TCP sur UDP est que TCP permet des communications fiables. L'inconvénient est qu'il nécessite une négociation (« Bonjour, prêt à communiquer ? » etc.), ce qui prend du temps.

Visualisation d'un « routage » entre deux ordinateurs :



• Juillet 1975 : L'ARPANet est 'livré' par le DARPA à l'Agence des Communications de la Défense (Defence Information System Agency) comme étant un réseau opérationnel.

• Juillet 1975 : Deux jeunes américains inconnus du public (Bill Gates et Paul Allen) fondent la société Microsoft.

• 1975 : Première version du *Jargon File* par Raphael Finkel[54] !

• 1975 : Deux ans après la première démonstration, le réseau devient de plus en plus chargé en particulier le vendredi soir…

• 1er avril 1976 : Apple est fondé par Steve Jobs, Steve Wozniak et Ron Waynes.

• 1976 : Fondation de la firme U.S. Robotics.

• 1976 : Les laboratoires Bell d'AT&T développent UUCP (Unix to Unix Copy Program). Il s'agit du premier protocole d'échanges de données largement disponible et qui sera énormément utilisé avant l'avènement de TCP/IP et d'Internet.

[54] Raphael Finkel est un informaticien américain, professeur à l'université du Kentucky. Il a compilé la première version du *Jargon File*. Il est l'auteur du logiciel d'exploitation *Vade-Mecum*, d'un manuel sur les logiciels d'exploitation, et de la conception avancée de langage de programmation, d'un livre d'introduction sur des paradigmes de programmation. Raphael Finkel et J.L. Bentley ont créé la structure de données appelée le *quadtree*. Un quadtree est une structure de données de type arbre dans laquelle chaque nœud peut compter jusqu'à quatre enfants. Les quadtree sont le plus souvent utilisés pour partitionner un espace bidimensionnel en le subdivisant récursivement en quatre nœuds.

• 1976 : Le DoD (Department of Defense) commence ses expérimentations sur TCP/IP.

• 1976 : À ce moment, le réseau ARPANET, en incluant les liaisons radio et satellite est composé de 111 ordinateurs.

• 1976 : Adoption de la norme X25 par le CCITT (Comité Consultatif International Télégraphique et Téléphonique) décrivant l'interfaçage des terminaux sur un réseau de communication par paquets. Cette norme a été définie dans l'urgence pour éviter qu'IBM n'impose mondialement sa propre norme propriétaire SNA (Systems Network Architecture).

Les réseaux à ordonnance de paquet ont été développés par l'Union internationale des télécommunications en poursuivant les recherches de la DARPA et en utilisant les formes de réseau X.25. En 1974, le X.25 sert de base au développement du SERCnet reliant les académiciens anglais avec leurs sites de recherche. Le SERCnet deviendra ensuite JANET lors de son association avec le Joint Academic NETwork.

En mars 1976 l'Union internationale des télécommunications lance le premier standard en X.25.

Le Bureau de poste anglais, Western Union International et Tymnet participèrent à la création de l'International Packet Switched Service, le premier réseau international à aiguillage de paquets ; c'était en 1978. Ce réseau s'étendit depuis l'Europe et les États-Unis pour couvrir en 1981 le Canada, Hong Kong et l'Australie. Dès le courant des années 90, il fournissait une infrastructure réseau mondiale.

Contrairement à l'ARPANET, le X.25 était disponible dans le monde de l'entreprise. Le X.25 sera utilisé pour les premiers réseaux téléphoniques publics, tels CompuServe et Tymnet. En 1979 CompuServe fut le premier service capable de proposer un courrier électronique ainsi qu'un support technique aux utilisateurs d'Ordinateur personnel. Cette société repoussa une nouvelle fois les barrières des télécommunications en proposant l'année suivante des discussions en temps réel grâce à son *CB Simulator*, un simulateur radio. Il y eut aussi les réseaux America Online (AOL) et Prodigy ainsi que de nombreux réseaux BBS comme The WELL et FidoNet. Ce dernier était particulièrement populaire dans le milieu des hackers[55] et radioamateurs.

• 22 Mai 1990 : Lancement de Windows 3.0 qui sera un énorme succès.

• 1990 : Le CERN est à l'époque le plus grand site Internet de toute l'Europe et influence fortement l'acceptation et la diffusion des techniques internet. C'est dans ce contexte qu'arrive la nouvelle révolution.

• Novembre 1990 :

Tim Berners Lee propose à la direction du CERN l'idée du Worl Wide Web : une architecture permettant de lier et d'accéder à des informations en tout genre comme une toile (en anglais « web ») de nœuds dans laquelle l'utilisateur navigue. La proposition repose sur la technique hypertexte (langage HTML, protocole HTTP) et l'interface de navigation est appelée « browser ».

[55] Le terme *hacker* apparaît en 1959 dans le jargon du *Tech Model Railroad* Club (TMRC), une association d'étudiants du *Massachusetts Institute of Technology* (ou MIT). Il désigne alors quelqu'un qui hack, ou construit un hack. En 1996, la Request for comments 1983 (RFC) définit un hacker comme une personne qui enchante autrui par sa compréhension intime du fonctionnement interne d'un système, en particulier des ordinateurs et réseaux informatiques. Cette dernière définition fait écho à celle utilisée depuis les années 1950 par les radio-amateurs pour qui le hacking est une bricolage créatif visant à améliorer le fonctionnement d'un système. Aujourd'hui encore, un hacker désigne un virtuose pouvant intervenir dans différents domaines comme la programmation, l'architecture matérielle d'un ordinateur, l'administration système, l'administration réseau, la sécurité informatique ou tout autre domaine ; les médias grand public utilisent le terme hacker dans le sens de *cracker*, *black hat* (« chapeau noir ») ou pirate informatique, c'est-à-dire un « hacker » opérant de façon illégale ou non éthique. Hackers et pirates informatiques sont parfois confondus avec les *script kiddies*, cyber-délinquants à la recherche de cibles faciles ne demandant pas de connaissance particulière en informatique. La Délégation générale à la langue française et aux langues de France préconise l'emploi du terme « fouineur » alors que le grand dictionnaire terminologique de la langue française favorise le terme bidouilleur, plus proche du sens initial.

• 1991 : Le prototype du navigateur de Tim Berners Lee est développé sur station NeXT dans le langage NeXTStep en quelques mois. Il offre des fonctionnalités de navigation, mais aussi d'édition WYSIWIG[56] permettant à n'importe qui de contribuer à l'ajout d'informations. Les résultats sont impressionnants.

Steve Jobs

Le 25 avril 1991, Steve Jobs vient faire un show au CNIT à Paris, pour la sortie officielle des ordinateurs NeXT en France. Show typique : Steve Jobs admirable, salle en délire. Lors de ce show, Steve a fait de nombreuses démonstrations des machines NeXT et de NeXTSTEP 2.1. Par exemple, il a montré le tableur Lotus 1-2-3 en utilisant l'émulateur SoftPC, puis il a dit qu'il était possible de faire bien mieux, et il a montré Improv, un tableur révolutionnaire. Il a aussi montré des fenêtres contenant des images 32 bits, et quand ils déplaçaient une fenêtre (dans son ensemble), les autres images apparaissaient par dessous de façon instantanée : stupeur des Macounets présents ! Dans une autre démonstration, il a joué le film StarWars dans une fenêtre, puis pour montrer les capacités graphiques de la carte NeXTdimension, il a pris une image de Donald et l'a posé sur l'épaule de Darth Vader qui continuait à bouger. L'ombre de Donald épousait en transparence l'épaule. Waaoooo.

NEXT station

Cependant, les systèmes NeXT ne sont pas très répandus. Une version allégée et facilement adaptable à d'autres ordinateurs est construite, elle abandonne les fonctionnalités d'édition.

• 1991 : *Standford Linear Accelerator Center* en Californie, devient le premier serveur Web aux USA en mettant à disposition une large base de données concernant des articles de physique.

• 1991 : L'association CIX (Commercial Internet eXchange) Inc. est créée après que la NSF ait levé les restrictions sur l'utilisation commerciale du Net.

Le WAIS (Wide Area Information Server) apparaît. Il fournit des mécanismes d'indexation et d'accès à l'information sur Internet (messages électroniques archivés, texte, livres électroniques, articles USENET, codes de programmation, images, graphiques, sons, bases de données…). De puissantes techniques de recherches sont développées ainsi que l'utilisation des mots clefs, qui seront repris par les techniques d'indexation du Web[57].

Le système Gopher est publié par Paul Lindner et Mark P. McCahill de l'université du Minnesota. Une interface texte utilisant des menus permet d'accéder aux ressources Internet sans taper une seule commande. Il sera complètement dépassé par le Web.

Le NSFNet backbone passe à la norme T3 (44.736 Mbps). Le trafic dépasse le trillion d'octets par mois et 10 milliards de paquets par mois.

Linus Torvalds, étudiant de l'Université d'Helsinki, commence à programmer un système UNIX qui tournera sur PC. La version 1.0 sera développée en trois mois.

---

[56] WYSIWYG est l'acronyme de la locution anglaise *What you see is what you get*, signifiant littéralement en français « ce que vous voyez est ce que vous obtenez » ou de façon plus concise « tel affichage, tel résultat ». L'acronyme est couramment utilisé en informatique pour désigner les interfaces utilisateur graphiques permettant de composer visuellement le résultat voulu, typiquement pour un logiciel de mise en page, un traitement de texte ou d'image. L'acronyme désigne, de fait, une interface « intuitive » : l'utilisateur voit directement à l'écran à quoi ressemblera le résultat final (imprimé).

[57] Le World Wide Web, communément appelé *le Web*, parfois *la Toile*, littéralement la « toile (d'araignée) mondiale », est un système hypertexte public fonctionnant sur Internet et qui permet de consulter, avec un navigateur, des pages mises en ligne dans des sites. L'image de la toile vient des hyperliens qui lient les pages Web entre elles. Le Web n'est qu'une des applications d'Internet, avec le courrier électronique, la messagerie instantanée, Usenet, etc. Le Web a été inventé plusieurs années après Internet, mais c'est le Web qui a rendu les médias grand public attentifs à Internet. Depuis, le Web est fréquemment confondu avec Internet ; en particulier, le mot Toile est souvent utilisé de manière très ambiguë.

• 1992 : Un Navigateur[58] allégé Mosaic est mis gratuitement à disposition par le CERN.

Le monde compte de l'ordre de 50 serveurs Web, 4000 News groups[59], et plus d'un million de machines sur Internet.

Jean Armour Polly[60] invente le terme « *Surfing the Internet* »

Charte de l'ISOC (Internet Society). L'Internet Society est une association de droit américain à vocation internationale créée en janvier 1992 par les pionniers de l'Internet pour promouvoir et coordonner le développement des réseaux informatiques dans le monde. Elle est en 2005 l'autorité morale et technique la plus influente dans l'univers du réseau Internet. L'Isoc finance et héberge sur son serveur les normes issues des travaux de l'Internet Engineering Task Force. L'IETF regroupe des ingénieurs et chercheurs du monde entier. Ils sont chargés de faire évoluer les standards de communication en prônant le consensus et la démonstration de solutions opérationnelles. Par ailleurs, elle organise le rassemblement annuel des internautes. En outre, elle publie la revue trimestrielle « *On the Internet* » pour ses membres.

Ainsi, même si l'Internet a une dynamique qui lui est propre, l'Isoc veille à sa progression et à sa bonne marche. L'association regroupe 7800 membres (personnes physiques) venant de 125 pays, ainsi que 129 organisations.

L'ISOC a de nombreux chapitres, dont un chapitre français, l'Isoc France, un chapitre luxembourgeois, l'ISOC Luxembourg et une section québécoise, ISOC Québec...

• 1993 : La NSF (La National Science Foundation (NSF) est une agence gouvernementale indépendante des États-Unis d'Amérique, pour soutenir financièrement la recherche scientifique fondamentale) crée l'InterNIC (Network Information Center), service d'information enregistrant l'ensemble des noms de domaines d'Internet. Cet organisme à été instauré afin de pouvoir faire face à l'ouverture d'Internet au public et vit son rôle disparaître en 1998, lors de l'ouverture à la concurrence ; pour être remplacé par l'Internet corporation for assigned names and numbers (ICANN).

• Janvier 1993 : Marc Andreesseen travaillant pour NCSA, met au point sous Unix et environnement X, une nouvelle version graphique du navigateur Mosaic piloté à la souris.

• Août 1993 : Marc Andreesseen et ses collaborateurs sortent une version de Mosaic pour Macintosh OS et Windows sous DOS.

• Décembre 1993 : Le *New York Times* publie un long article sur le Web et Mosaic. Marc Andreesseen quitte NCSA avec l'intention de laisser tomber Mosaic.

Windows for Workgroups 3.11, Windows fait ses premiers pas vers le réseau.

Mosaic conquiert Internet qui compte maintenant 341 634 sites Web. Mosaic deviendra bientôt une compagnie et un logiciel du même nom : Netscape.

• 1994 : Aux États-Unis, c'est l'arrivée des banques, des centres commerciaux et même des vendeurs de Pizza sur le Web qui dépasse alors les 10 000 sites. Le Web devient le deuxième service le plus utilisé

[58] Un navigateur Web est un logiciel conçu pour consulter le World Wide Web, l'ensemble des sites web. Techniquement, c'est un client HTTP dans une architecture client/serveur. Il peut être graphique ou texte. Les navigateurs internet les plus célèbres et les plus utilisés sont Internet *Explorer*, *Mozilla Firefox* et *Safari*. Le terme navigateur Web (ou navigateur Internet) est inspiré de *NCSA Mosaic* puis de *Netscape Navigator*. D'autres métaphores sont ou ont été utilisées. Le premier terme utilisé était *browser*, comme en anglais. Par la suite, on a vu fureteur (surtout utilisé au Québec), butineur, brouteur, arpenteur, fouineur ou explorateur (inspiré de *Microsoft Internet Explorer*).

[59] Un système en réseau de forums de discussions, inventé en 1979 et basé sur le protocole NNTP. Il a rapidement été rendu utilisable via Internet où il reste aujourd'hui en usage.

[60] Jean Armour Polly est bibliothécaire de profession, auteure d'une série de livres sur la sécurité d'Internet (*Surfing the Internet*), et a été une utilisatrice active d'Internet depuis 1991. Elle a reçu son BA dans des études médiévales à l'université de Syracuse en 1974, et son Master's en Science de bibliothèque de la même université en 1975. Polly est créditée d'avoir inventé l'expression « *surfer sur Internet* », étant l'auteure du premier aspect connu de l'expression dans un article appelé *surfer l'INTERNET*, édité à l'université du bulletin de bibliothèque du Minnesota Wilson en juin 1992.

après FTP et avant Telnet si l'on se base sur le pourcentage de paquets transitant sur NSFNet pour les différents services. Le trafic est maintenant de 10 trillions d'octets par mois.

• 1994 Linux 1.0 est disponible.

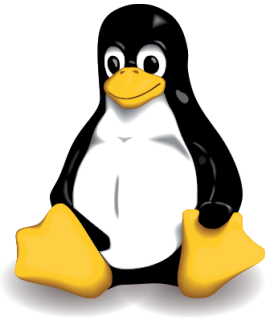
Linux est l'appellation courante du système d'exploitation libre, multitâche, multiplateforme et multi-utilisateur de type UNIX basé sur le noyau Linux.

GNU/Linux est une autre appellation plus technique qui rappelle que ce système d'exploitation dans son ensemble représente le résultat des efforts convergents de nombreux projets développés en mode collaboratif qui se sont déployé via Internet : non seulement le projet GNU et le noyau Linux, mais aussi le système de fenêtrage X Window, et certains logiciels produits par les équipes des Unix libres FreeBSD, OpenBSD et NetBSD.

Y collaborent aussi bien des individus passionnés et des organisations comme la Fondation pour le logiciel libre que des petites et grandes entreprises commerciales (IBM, Sun, HP, Oracle, etc.)

Pour l'utilisateur final, GNU/Linux se présente sous la forme d'une distribution Linux, commerciale ou non, c'est-à-dire d'une solution prête à être installée comprenant une sélection complète et cohérente de logiciels, des programmes d'installation et d'administration de l'ordinateur, ainsi qu'un mécanisme facilitant l'installation et la mise à jour des logiciels.

Linux est aujourd'hui utilisé sur de nombreuses plates-formes, du plus puissant super ordinateur aux systèmes embarqués tels que téléphone portable, assistant personnel, modems Freebox, Livebox, lecteur vidéo DivX, etc., en passant par les ordinateurs personnels, PC et Mac, sur lesquels il peut être installé seul ou en parallèle avec Microsoft Windows ou Mac OS. Linux s'est d'abord imposé dans le domaine des serveurs informatiques grâce à des logiciels tels que le serveur web Apache ou le serveur de fichier Samba qui permet de partager des fichiers avec un réseau d'ordinateurs sous Microsoft Windows. Il a également atteint depuis peu une certaine maturité sur le poste de travail grâce aux interfaces conviviales que représentent GNOME et KDE ainsi qu'aux succès de logiciels comme la suite bureautique OpenOffice.org ou le navigateur internet Mozilla Firefox.



La mascotte de Linux est un manchot qui a pour nom Tux.

Petite histoire de Linux

Le projet GNU

Richard Stallman dévoile le 13 juillet 1985 son Manifeste du projet GNU qui résume l'ambition du projet :

« GNU, l'acronyme de GNU's Not Unix (GNU n'est pas Unix), est le nom du système complet de logiciels compatible Unix que j'écris pour pouvoir le donner librement à tous ceux qui en auraient besoin. De nombreux bénévoles m'aident. Les contributions en temps, en argent, en logiciels et en matériel sont les bienvenues. »

Il entend ainsi réagir aux redevances en hausse des deux UNIX classiques, System V (d' AT&T) et BSD (de Berkeley).

Concrètement il relate l'effort qu'il accomplit depuis 1983 dont on distingue déjà en 1985 certaines pièces maîtresses : le compilateur *gcc*, l'éditeur de texte *Emacs*, etc. L'effort sera opiniâtrement poursuivi, et au début des années 1990, le projet GNU possède une version utilisable de tous les éléments nécessaires à la construction d'un système d'exploitation (outre ceux cités précédemment : un shell (un interpréteur de commandes), des bibliothèques, et de nombreux logiciels) à l'exception du plus central : le noyau.

Le projet GNU initie alors en 1990 le projet de production d'un noyau nommé *Hurd*.

D'après Thomas Bushnell, l'architecte initial du projet Hurd, l'idée initiale était d'adapter le noyau BSD 4.4-lite, et avec le recul « il est parfaitement clair pour moi que celui-ci aurait magnifiquement réussi et la face de l'informatique en aurait été changée ».

À cause d'un manque de collaboration de l'Université de Berkeley, Stallman décide, à la place, d'utiliser le micro-noyau Mach, qui s'avérera extrêmement pénible à faire progresser (un micro-noyau réduit la partie protégée du système à son strict minimum – les tâches régaliennes, en quelque sorte – , et traite autant que possible le reste comme des applicatifs ordinaires).

Hurd ne dépassera jamais réellement le stade de curiosité de laboratoire de recherche, en revanche le travail du projet GNU forme aujourd'hui une part importante d'un système d'exploitation actuel basé sur le noyau Linux (voir plus bas). Une querelle sémantique a, pour cette raison, éclaté ces dernières années concernant l'appellation GNU/Linux afin de faire référence au système dans son intégralité. Ce débat est relaté dans l'article Linux ou GNU/Linux.

1991 : naissance du noyau Linux

Linus Torvalds

En 1991, un étudiant finlandais qu'indisposait la faible disponibilité du serveur Unix de son université à Helsinki entreprend d'écrire un noyau (monolithique) qu'on appellera plus tard « noyau Linux ».

Linus Torvalds fait alors son apprentissage sur Minix, un système d'exploitation écrit dans un but pédagogique par Andrew Tanenbaum. Désirant conserver un système d'exploitation simpliste pouvant être compris dans les moindres détails par ses étudiants, Tanenbaum refuse les contributions visant à améliorer Minix, donnant à Linus la motivation nécessaire pour en écrire un remplaçant.

Il commence par développer un simple émulateur de terminal, qu'il utilise pour se connecter via modem au serveur de son université. Linus désire alors surtout comprendre le fonctionnement de son ordinateur, un 386, machine très moderne pour l'époque. Après l'ajout de diverses fonctionnalités, dont un système de fichiers compatible avec celui de minix, Linus oriente son projet vers quelque chose de plus ambitieux : le noyau d'un système d'exploitation aux normes POSIX.

De Minix à Freax

Le 5 octobre 1991, il annonce sur le forum *Usenet news:comp.os.minix* la disponibilité d'une ébauche de son système d'exploitation en version 0.02, la 0.01 ayant eu une diffusion plus que confidentielle.

Depuis, des centaines de passionnés et des entreprises, petites ou géantes, sont venus participer au projet dont Linus Torvalds est toujours le coordinateur. Éric S. Raymond décrit dans un essai retentissant, le modèle de développement du noyau Linux et d'une partie des logiciels libres.

De Freax à Linux

Initialement appelé Freax par son créateur, le projet trouve son nom définitif grâce à Ari Lemmke, administrateur du serveur FTP *ftp.funet.fi*, qui héberge le travail de Linus Torvalds dans un répertoire nommé Linux. C'est la première apparition d'un terme composé à partir de Linus et Unix, qui deviendra par la suite une marque déposée au nom de Linus Torvalds. Le manchot Tux, dessiné par Larry Ewing en 1996, devient le symbole du projet.

Linux est aujourd'hui utilisé dans de nombreux domaines, des systèmes embarqués aux super ordinateurs en passant par les serveurs avec notamment le très populaire LAMP[61]. Sa part de marché sur les

[61] LAMP est un acronyme informatique permettant de désigner facilement la réunion de ces logiciels libres sur une même plate-forme : « **L**inux », le système d'exploitation ; « **A**pache », le serveur web ; « **M**ySQL », le serveur de base de données ; « **P**HP » à l'origine, puis « Perl » ou « Python », les langages de script. Cet ensemble est très utilisé dans le monde pour construire des applications web.

postes clients est faible, les diverses estimations étant comprises en général entre 0,3 % et plus de 3 % en fonction des méthodes de relevé et de calcul. Ce chiffre est en réalité difficilement estimable, car d'une part, de nombreux navigateurs Web modifient leur identité par défaut (ou à la demande de l'utilisateur) afin de ne pas être gênés par les sites Web bloquant les navigateurs autres qu'« Internet Explorer tournant sur Microsoft Windows », et d'autre part, il est fréquent qu'un utilisateur Linux configure son système de manière à ce qu'il ne communique pas ces informations, car elles pourraient permettre de faciliter la recherche de failles éventuelles par un pirate.

• 1994 : Naissance du VRML (Virtual Reality Modeling Language)

Le Virtual Reality Modeling Language (abrégé en VRML) est un langage de description d'univers virtuels en 3 dimensions. Ce langage interprété est une norme internationale ISO et les fichiers VRML ont habituellement pour extension .wrl.

En fait, c'est à proprement parler un langage de présentation et non de programmation, puisque comme pour le langage HTML par exemple, un fichier VRML ne contient généralement pas une suite d'instructions, mais plutôt les informations permettant au visualiseur d'afficher ensuite les éléments (formes, senseurs, lumières, etc).

Présenté lors de la World Wide Web Conference de 1994, VRML n'est pas l'œuvre d'un unique programmeur, mais plutôt le résultat de la collaboration de plusieurs professionnels de la 3D, dont entre autres Mark Pesce, Tony Parisi, Gavin Bell (Silicon Graphics) et Paul Strauss (Silicon Graphics).

Le but premier de ce langage est de permettre la représentation d'univers interactifs 3D virtuels. Les fichiers .wrl sont des fichiers texte décrivant les scènes virtuelles à l'aide du langage VRML. Les fichiers .wrl, qui peuvent être stockés localement sur un ordinateur ou téléchargés depuis un serveur web, sont visualisés à l'aide d'un visualiseur, qui est soit un plugiciel ajouté au fureteur web ou encore un logiciel autonome indépendant du fureteur web, qui est installé sur l'ordinateur de l'utilisateur.

Les programmes VRML peuvent décrire des formes simples (points, lignes, polygones) ou complexes (sphères, cubes, cônes, cylindres...), du texte, des images, des animations, des éclairages, des sons, des hyperliens, ainsi que leur agencement dans l'espace, leur texture, leur couleur, leur matériau...

• 1994 : Naissance de Yahoo! (Yet Another Hierarchical Officious Oracle) un des plus gros moteurs et portail de recherche sur internet.

• Octobre 1994 : Lancement de Netscape (qui remplace Mosaic) un nouveau browser sur Internet. En six mois 5 millions de copies auraient été diffusées et un an plus tard il serait utilisé par les trois quarts des surfeurs d'Internet.

• 1995 : La NSFNet retourne à l'état de réseau de recherche. L'interconnexion se fait maintenant directement par les fournisseurs d'accès.

• Avril 1995 : Le Web dépasse FTP en pourcentage de paquets et d'octets transitant. Il devient le premier service sur Internet avec 100 000 sites disponibles.

• 24 août 1995 : Sortie de Windows 95. C'est à travers l'interface graphique de cet OS[62] et son successeur que beaucoup de gens du grand public, et beaucoup de familles, vont découvrir la micro et par extension le Web.

[62] Operating System = système d'exploitation.

• 10 octobre 1995 : Netscape 2.0 est disponible pour Windows, Macintosh et Unix. Il inclut Java[63] de Sun pour les Applet.

• 1995 : L'enregistrement des noms de domaines devient payant.

Un nom de domaine (ou NDD en notation abrégé) est un identifiant unique lié à une entité dont les ordinateurs sont reliés au réseau internet. Le système est hiérarchique, permettant la définition de sous-domaine(s) d'un domaine existant. Le DNS (Domain Name System) permet d'associer des adresses Internet à des noms d'hôtes, et inversement. Chaque domaine doit être défini dans deux serveurs DNS au minimum. Ces serveurs peuvent être interrogés pour associer un nom d'hôte à une adresse IP ou bien pour récupérer les adresses IP des serveurs de noms associés à un nom de domaine (entre autres, requêtes possibles).

Pourquoi un nom de domaine ?

L'apparition des noms de domaine résulte d'un besoin bien concret — comme sur une carte Michelin — le besoin de nommer l'espace afin de pouvoir y naviguer (sauf que l'espace en question est numérique).

L'interconnexion d'un grand nombre d'ordinateurs (initialement Arpanet) a créé un espace numérique composé de machines en réseau repérées entre elles par des adresses IP. L'avènement de contenus de niveau évolué ainsi que la popularité croissante du réseau et le nombre de machines connectées à nécessité de segmenter ce dernier en domaines que — pour des raisons de commodité — il était plus facile de nommer de façon humainement compréhensible, d'où l'apparition de « noms de domaine ».

Les machines continuant d'échanger entre elles selon des protocoles de très bas niveau, le système de nom de domaine est doublé d'un système de traduction homme/machine appelé DNS pour « Domain Name System ». Un nom de domaine n'est pas un DNS (souvent un nom de domaine est appelé « DNS » : c'est tout à fait inapproprié). Le système DNS permet de traduire un nom de domaine en adresse IP et ce, à l'usage des machines uniquement, ou une adresse IP en nom de domaine, et ce, à l'usage des humains uniquement.

Les noms de domaines étant destinés aux humains, ils ont été typés en fonction des quelques secteurs concernés à l'époque :

.edu : pour les organismes relevant de l'éducation (marginalisé essentiellement aux universités américaines).

.net : les opérateurs réseau et opérateurs internet, par extension ce qui relève de la technique internet (a largement débordé de cette typologie initiale).

.org : les associations sans but lucratif.

.com : les services à vocation commerciale.

L'internet devenant bientôt une zone de chalandise sans précédent, le .com a largement explosé entraînant avec lui les autres extensions pour lesquelles les noms convoités en .com était déjà pris. Depuis, pour désengorger tout ça et relancer un peu le business à peu de frais ont été introduites les .info et .biz

Il y a en juin 2003 environ 30 millions de gTLD's dans le monde, en février 2004 : + de 34 millions.

[63] Java est le nom d'une technologie mise au point par *Sun Microsystems* qui permet de produire des logiciels indépendants de toute architecture matérielle. Cette technologie s'appuie sur différents éléments qui, par abus de langage, sont souvent tous appelés Java : le langage Java est un langage de programmation orienté objet ; la machine virtuelle Java est une machine virtuelle qui permet d'exécuter les programmes écrits en Java ; la plateforme Java correspond à la machine virtuelle Java plus des spécifications d'API : Java Platform, Standard Edition (Java SE) contient les API de base et est destiné aux ordinateurs de bureau ; Java Platform, Enterprise Edition (Java EE) contient, en plus du précédent, les API orientées entreprise et est destiné aux serveurs ; Java Platform, Micro Edition (Java ME) est destiné aux appareils mobiles tels que PDAs ou smartphones ; JavaScript, l'implémentation de Netscape du langage de script ECMAScript, qui n'a en commun avec le langage Java qu'une syntaxe similaire héritée du langage C.

Notons que si ce marché est un réel succès, son potentiel est toutefois encore quasi intact autorisant l'apparition de nouvelles extensions (à la discrétion des teneurs du système DNS et de ses serveurs) au grès de l'imagination, telles que .sex .doc .tél .presse .pub etc...

• 1995 : Émergences de nouvelles technologies (JAVA, JAVAScript, ActiveX[64], VRML, CU-See-Me[65]).

• Janvier 1996 : Digital lance Alta Vista, un puissant moteur de recherche pour Internet.

• 1996 : Microsoft entre dans la danse : avec Internet Explorer 3.0 en septembre, la guerre des navigateurs commence, les versions se succèdent Netscape 3.0 ne sortira que quelques jours après…

• Octobre 1996 : WebTV Network lance le WebTV pour visionner des pages Web sur la télévision. Ce sera un échec.

• 1997 : Le Palm Pilot, ordinateur de poche de 3Com est un gros succès. Les assistants électroniques ne font qu'arriver. Microsoft sent que le futur est dans le mobile et lance Windows CE. Son système n'aura pas grand succès.

Naissance d'un produit culte

En Avril 1996, les premiers exemplaires étaient en vente dans les magasins. Le succès fut immédiat : 350 000 exemplaires furent vendus avant la fin de l'année. En 18 mois, le premier million d'unités était commercialisé. C'était le début d'une aventure qui allait consacrer un petit appareil électronique pour en faire pour certains un véritable objet culte. Il est reconnu qu'il s'agit là d'une première en terme de vitesse d'adoption par le public, loin devant la télévision couleur notamment. Cet objet à porter sur soi, à l'interface rapide et conviviale et à la reconnaissance d'écriture si affûtée qu'elle crée un lien avec l'utilisateur vécut ainsi une success-story qui n'est pas sans rappeler celle qu'avait connue une dizaine d'années auparavant le *Macintosh d'Apple*. Mais là où Apple, tentant de rééditer l'exploit, n'avait pas réussi le lancement du Newton, probablement apparu trop tôt, Palm avait su proposer la bonne alchimie technique au moment adéquat : le grand public était prêt. Durant les années qui suivirent, le Pilot fut renommé PalmPilot suite à la plainte d'une société française qui commercialisait des stylos sous la même marque. il évolua de 128 Kb de mémoire vive au départ à 256 puis 512 Ko

Le départ de chez 3Com

En février 1997, nouvel épisode pour les employés de la filiale Palm Computing. 3Com, le géant américain de la communication en réseau rachète US Robotics et se pose la question de savoir s'il était économiquement intéressant de garder la partie Agendas électronique. La vente alors envisagée n'eut jamais lieu. Les dirigeants de 3Com actuels, qui viennent de mettre en bourse 95% de leur filiale dans une introduction particulièrement réussie (2 mars 2000) doivent aujourd'hui s'en féliciter. Entre temps, les machines fonctionnant avec le système d'exploitation Windows CE de Microsoft sortaient sur le marché. Portés par la puissance du géant des logiciels et par des constructeurs tels Compaq, HP ou Phillips,

[64] En programmation, le *Component Object Model*, aussi connu sous le nom de *ActiveX*, est un composant logiciel (comme les DLL) créé par Microsoft. Il est utilisé pour permettre le dialogue inter-programmes. Bien qu'il ait été implémenté sur de nombreuses plates-formes, il est toujours majoritairement utilisé sur Microsoft Windows. Son prédécesseur fut Object Linking and Embedding (OLE), qui est lui-même sur le point d'être remplacé par la framework .NET de Microsoft. En début d'année 1996, Microsoft renomma certaines parties de OLE concernant Internet, ActiveX, et petit à petit toutes les parties de OLE passèrent sous le signe ActiveX, exception faites des composants faits pour les documents composés et utilisés par exemple par *Microsoft Office*.

[65] « See You, See Me », « Je te vois, tu me vois ». Logiciel permettant de réaliser de la vidéoconférence sur l'Internet. En fait, il faut une caméra, une carte d'acquisition vidéo, et finalement, on ne peut échanger que 2 ou 3 images par seconde (en 1995). Mais c'est toujours un début...

les analystes ne donnaient pas cher du Palm Pilot. L'histoire semblait devoir ressembler de plus en plus à celle du Macintosh. D'autant plus que d'autres challengers, comme par exemple la très légère carte REX de Franklin faisaient leur apparition. Celle-ci, malgré des qualités (taille et poids d'une carte de crédit) ne s'est toujours pas imposée. Probablement en réaction, le Palm Pilot fut alors proposé sous licence par IBM sous le nom de WorkPad. Le succès de la gamme ne se dément pas. Il faut dire que le Palm bénéficiait de nombreux programmes proposés par une communauté de développeurs séduits et prolifiques.

• Septembre 1997 : Internet Explorer 4.0 est disponible gratuitement, un million de copies auraient été téléchargées en deux jours.

• Février 1998 : Le langage XML (Extensible Markup Language) est présenté par le W3C[66] sous la forme d'une recommandation version 1.0 il pourrait révolutionner le Web et l'Internet de demain.

• Avril 1998 : Netscape contre-attaque Microsoft et livre gratuitement le code source de Netscape Communicator.

• Novembre 1998 : AOL achète Netscape.

• 1999 : 54% des serveurs Web fonctionnent avec Apache (serveur Web célèbre pour sa puissance et sa gratuité).

• 2000 : Cisco (célèbre compagnie d'équipements pour les connexions réseau) possède 80 % de parts de marché des routeurs pour le Net au niveau mondial.

• 19 août 2004 : Entrée en bourse de Google. Après des effets d'annonces, des retards et autre procédés inhabituels, l'action Google gagne 15 % le jour de son introduction en Bourse. La start-up de 1998, devenue incontournable sur le Web, rejoint les « grands » de l'Internet que sont Yahoo !, Ebay ou encore Amazon.

La « gouvernance »

Dire que les gouvernements, y compris le gouvernement américain, ont très largement sous-estimé l'influence qu'aurait sur les sociétés classiques l'existence d'une société virtuelle internationale sans gouvernement est une litote. Et depuis 1995, année durant laquelle ils entamèrent enfin, plus ou moins rapidement cette prise de conscience, leur unique objectif semble être de maîtriser un réseau dont l'origine même est basée sur le principe de la décentralisation totale et sur l'impossibilité de contrôler (ou de détruire) ses fonctionnalités. C'est dire la difficulté à laquelle ils doivent faire face dans leur tentative de « reconquête » de leurs pouvoirs sociaux et territoriaux historiques.

Deux des technologies à la base d'Internet sont cependant centralisées par nature : le mode d'adressage des ordinateurs connectés (IP) et le système de nommage permettant d'associer un nom à une adresse IP numérique. On pourra noter, d'ailleurs, que ces deux technologies auraient pu ne pas être ainsi conçues, et qu'elles le furent à une période historique bien plus récente et bien moins utopiste.

Il est donc tout naturel que ces deux uniques points de centralisation soient l'objet d'une bonne part des débats autour du thème de la « gouvernance » : l'ICANN (*Internet Corporation for Assigned Names and Numbers* est l'autorité de régulation de l'Internet), est en effet très largement sous la surveillance du gouvernement américain, qui a lui-même créé cet organisme destiné à devenir sinon le futur « gouvernement de l'Internet », au moins le lieu où les seules technologies centralisées qui permettent son existence puissent être dirigées. Et si l'Europe fait son possible pour y avoir une influence un peu plus grande, il

[66] Pour assurer un bon développement du Web mondial il ne faut pas que ces instituts agissent chacun de leur côté mais ensemble. Ils décident donc de former un consortium pour défendre ensemble le World Wide Web . Ces trois mots commencent par W et comme ces deux instituts forment un consortium la nouvelle structure va être dénommée W3C. Tim Berners-Lee, l'inventeur du Web, va en assurer la direction. En août 1996, le Campus de Shonan Fujisawa de l'université de Keio est devenu le troisième hôte en charge du Japon et de la Corée. Il est à noter que la contribution des chercheurs français pour un bon fonctionnement du WEB a été importante

est difficile de dire jusqu'où les USA accepteront de perdre le peu de pouvoir qu'un gouvernement ait encore sur le réseau des réseaux.

Reste que, notamment depuis les attentats du 11 septembre, nombre de pays se sont dotés de lois qui leur permettent de réguler, un tant soit peu, les contenus et les échanges qui échappaient jusque-là aux limites imposées par exemple à la liberté d'expression ou aux lois sur la propriété intellectuelle.

En réalisant la vision libertaire de Norbert Wiener, les concepteurs d'Internet (et le nombre de technologies qui le composent et qui ont été spécifiquement construites pour augmenter le pouvoir des communautés basées sur le partage de l'information prouvent que ce n'est pas une coïncidence) n'ont tenu compte ni des notions de droit d'auteur (pour eux, dont la thèse était que la diffusion la plus large possible de la culture créerait toujours davantage de savoir et de création, le contraire eut été surprenant), ni surtout du fait que si chacun pouvait participer, alors le « droit à la liberté d'expression » présent dans la plupart de nos constitutions deviendrait autre chose qu'un droit théorique, limité dans les faits par la notoriété préalable ou le pouvoir de celui qui s'exprimait avant l'arrivée d'Internet.

Et, si les premiers pays s'étant dotés de lois qui leur rendent la possibilité de surveiller leur population dans son usage d'Internet sont évidemment les pires dictatures qui soient, il est à craindre que bien des droits de l'homme soient un peu trop facilement ignorés, y compris par les pays les plus avancés sur ce point, tant la structure même du réseau des réseaux rend les structures de pouvoir antérieures caduques. A moins de se transformer en dictatures les unes après les autres, nos sociétés devront bien faire avec et admettre que la vision des sociologues libertaires des années 60 est désormais une réalité à laquelle il faudra bien s'adapter.

Et que, quelque part, c'était bien prévu comme ça.

Les deux faces de la liberté.

Né d'une stratégie d'autonomisation du monde de la recherche par rapport au champ économique et porteur d'une utopie technologique, Internet inscrit, dans son mode même de fonctionnement, une double liberté qui permet à celui-ci de s'affirmer comme espace communicationnel libre : la liberté d'accès aux standards qui permet la liberté de communication, de publication et d'échange d'informations.

La liberté d'accès aux standards, comme nous l'avons vu avec le TCP/IP, permet d'empêcher que les standards d'Internet se trouvent aux mains d'une quelconque instance qui pourrait définir des restrictions dans leur utilisation. C'est ainsi que les différents services d'Internet comme le courrier électronique et le transfert de fichiers obéissent à des standards libres, c'est-à-dire à des protocoles qui assurent le transfert de courrier et de fichiers que tout le monde utilise sans devoir demander d'autorisation à quiconque et sans devoir payer des droits d'auteurs.

Ce principe de liberté des standards permet d'assurer une totale autonomie de communication, de publication et d'échange d'informations sur Internet. En effet, si on peut utiliser librement les outils de ce réseau, personne ne peut venir mettre des conditions à l'usage de ces outils. De plus, pour protéger cette liberté, les utilisateurs ne sont pas obligés de révéler leur véritable identité, un principe d'anonymat s'est très vite instauré sur le Net. C'est ainsi que pour télécharger un fichier sur un serveur FTP, il suffit de se connecter sur la majorité de ces serveurs, en se déclarant « Anonymous ». De même, on n'oblige personne à posséder une adresse e-mail basée sur son nom véritable. Et, sur les Forums et les Chats, les individus discutent fréquemment entre eux en utilisant des pseudonymes.

Ces deux principes de liberté permettent à Internet de fonctionner sans aucun centre coordinateur, c'est-à-dire sans véritable pouvoir central qui commande sa logique de développement, ce sont en fait les utilisateurs eux-mêmes, par ce qu'ils publient sur le réseau et la communication qu'ils établissent entre eux, qui assurent le développement de cet espace communicationnel. Et ceux qui utilisent le TCP/IP pour connecter de nouveaux réseaux sur Internet, le font afin d'étendre justement les possibilités de libre accès à cet espace communicationnel.

Réflexions en marge de l'histoire d'Internet par Josette Lanteigne

Le maître mot des aspects positifs de l'histoire d'Internet est l'organisation. Qui ne sait que des problèmes aussi criants que ceux de la faim et de la surpopulation pourraient être facilement réglés par une meilleure organisation ? À l'heure où nos gouvernements cherchent de plus en plus les moyens d'économiser les ressources, où les victimes des coupures se plaignent du sort qu'on leur fait, on peut trouver un certain réconfort dans l'idée que la terre n'est pas surpeuplée, mais que les populations sont mal réparties, serrées dans les prétendus « centres » qui ne cessent de s'étendre en se dépeuplant et qu'on pourrait sans doute servir plus de gens si on les nourrissait directement, au lieu de gaspiller les ressources pour nourrir le bétail au seul profit des plus nantis.

Si l'histoire d'Internet se révélait avoir des aspects positifs, ce serait donc au regard de l'organisation, de la réorganisation et de la correction des erreurs du passé. Le Réseau permet d'englober (plutôt que de simplement « rejoindre ») un grand nombre de personnes aux intérêts divers mais compatibles aussi indépendants les uns des autres que des atomes, aussi solidaires que deux ordinateurs peuvent l'être lorsqu'ils sont en réseau. Prenons l'histoire d'Arpanet. Les chercheurs qui y ont participé ont-ils été dupes des militaires ou s'ils ont réussi à passer à la population un outil formidable qui ne lui était pas du tout destiné ? (voir la manière dont Jacques Dufresne relate les faits dans « *La guerre cathodique. Passé, Présent, Avenir* », L'Agora, vol 3 no 9, 1996, p. 13-15). Un peu comme le téléphone est devenu un outil de communication alors qu'il ne devait servir qu'au commerce, comme le télégraphe[67]. Mais qui n'a pas l'impression que les médias se dégradent très vite ? Pour certaines personnes, ceux qui passent leur vie au téléphone ou devant la télévision sont purement et simplement en train de perdre leur temps. Ce n'est pas là attaquer les personnes, mais les médias. Une fois passé l'engouement initial pour Internet et ses possibilités infinies, devrons-nous reconnaître qu'il contribue autant à nous abêtir qu'à nous rendre plus intelligents ?

Pourtant, une philosophie anti-médias nous ferait perdre un acquis important de la civilisation occidentale. Où serions-nous sans le téléphone, la télévision — dont on peut se passer — et, pour un nombre grandissant de personnes, Internet ? Internet permet de se distraire, de faire des affaires, des recherches même : de plus en plus, l'ère du livre est révolue, et devant les librairies qui se vident au profit des magasins de disques, se brancher apparaît comme la manière de continuer à lire — d'une nouvelle manière, en ne séparant plus le contenu du graphisme, du son et de tout ce qui peut le mettre en valeur.

On peut dire tout à la fois qu'on lit moins et qu'on lit plus sur Internet. La présentation en colonnes qui ne se lisent pas une à une, comme les colonnes de journaux, mais simultanément, donne l'impression de pouvoir assimiler beaucoup plus de contenu à la fois, même s'il suffit de fabriquer de tels documents pour savoir qu'on fait beaucoup avec peu. D'où l'impression double de richesse et de pauvreté des sites qui présentent des contenus. Mais nous n'en sommes encore qu'au début du processus de démocratisation d'Internet, même si celui-ci a déjà plusieurs années.

---

[67] Claire Poitras aux séminaires de L'Agora, le 24 mars 96 (nous rapportons ici l'essentiel de ses propos) : « *Les opérateurs du réseau téléphonique ne l'avaient pas du tout conçu comme un outil de communication personnelle ; le téléphone devait être le prolongement du télégraphe, un instrument commercial d'échange et un instrument de contrôle. L'usage le plus répandu de cet instrument — à des fins de sociabilité — a été développé d'abord par les usagers du réseau et non par les opérateurs. Naturellement, ceux-ci ont ensuite récupéré la sociabilité de l'instrument* ». L'intervention de Jean-Claude Guédon va dans un sens apparenté : *[le téléphone] apparut d'abord comme instrument de diffusion, d'abord de pièces de théâtre à l'Exposition Universelle de Paris en 1889, ensuite de programmes divers, nouvelles et variétés, à Budapest avant la guerre. Dans tous les cas, il s'agit d'information stricto sensu. La fonction de communication de cet instrument ne s'affirma que progressivement, suivant en gros la croissance conjuguée des réseaux et surtout les possibilités de la commutation. Péché grave aux yeux de certains gouvernements pour lesquels la distinction entre comploter et communiquer n'est pas toujours claire. Ainsi, en France, l'implantation du téléphone en province demeura-t-elle un temps privilège de médecin, d'instituteur et de quelques autres professions dignes de confiance. Dans l'ex-URSS, les annuaires téléphoniques étaient rares, voire inexistants, manière discrète mais efficace de limiter considérablement la portée de l'instrument* » (La planète cyber. Internet et cyberespace, Découvertes Gallimard, 1996, p. 15-16).

On trouve sur Internet de nombreux sites sur son histoire, dont le plus connu est sans doute celui du *Babbage Institute*, et le groupe *L'Agora, Recherches et Communications* a déjà développé de nombreux liens concernant les aspects historiques dans la section Recherche de son site. On y présente aussi bien l'histoire des personnages que celle des machines, l'histoire officielle aussi bien que celle, plus englobante, qui part de l'invention de la boussole. Or quel est l'intérêt de ces recherches ? Il est certain qu'elles favorisent l'appropriation du médium. Le fait de mettre en relation le télégraphe, le téléphone, la radio et Internet, par exemple, nous permet de constater que pour celui qui est branché, la télévision est superfétatoire, de même que les journaux le deviennent, à mesure que l'on peut avoir des copies électroniques de tous les principaux journaux de la planète. Voilà pourquoi la télévision cherche à se brancher, pour rester dans la course.

Mais la grande question qu'on ne peut jamais s'empêcher de poser à l'histoire est celle-ci : est-ce qu'on y gagne au change ? Si Internet est une télévision interactive, est-il essentiellement différent de celle-ci ? Il n'y a rien qu'on n'ait dit contre la télévision et surtout contre ceux qui s'y adonnent. Sur la page couverture de la traduction française du livre de Neil Postman, *Amusing Ourselves to Death* (Se distraire à en mourir, traduction française de Thérèsa de Cheresy, Paris, Flammarion, 1986, p. 212), la télévision a des ailes de requin avec en face d'elle une paire de pieds coupés. Certes, on peut faire de la bonne télévision, mais une bonne émission est comme un bon cours magistral : le récepteur y joue un rôle essentiellement passif. Voilà pourquoi Postman estime que la télévision « joue le mieux son rôle quand elle présente des divertissements légers, mais elle nous fait le plus grand tort quand elle coopte les modes de discours sérieux — informations, politique, science, éducation, commerce, religion — et les présente sous forme de divertissement ».

Comment prétendre, en s'appuyant sur son histoire récente et plus ancienne, qu'il en ira autrement pour Internet ? Dans la préface d'un livre de Michel Dionne sur *La Télématique* (Éditions Cerveau, Montréal 1988), Jacques Dufresne soutient qu'« *avant même l'avènement de l'ordinateur et de la télématique, il y avait quelque chose d'effarant dans la disproportion entre l'abondance de l'information accessible et la pauvreté des critères et du jugement dont nous disposons pour faire des choix* ». Pour lui, cette disproportion est un nuage noir qui plane sur l'avenir de l'humanité, et les personnes lucides sont celles qui feront un usage de l'ordinateur qui reflète cette conscience critique.

L'information est un principe organisateur

Pour Arnold Gehlen, dont l'anthropologie philosophique nous servira de fil conducteur, l'être humain est seul à avoir un monde (Welt) ; l'animal a seulement un environnement (Umwelt). C'est parce que l'être humain n'est pas conditionné par un environnement (il jouit à cet égard d'une parfaite mobilité qui contraste avec les comportements pathologiques de l'homme moderne, qui par exemple trouve de meilleurs fruits et légumes à la ville qu'à la campagne, ou dans les pays industrialisés plutôt que dans ceux qui ne le sont pas) qu'il peut aussi ne pas tenir compte de l'environnement des animaux, qui est aussi le sien.

La situation particulière de l'homme dans la nature rend nécessaire un autre mode de rattachement à cette nature. L'animal reçoit à la naissance un programme qui lui permet d'interagir avec son environnement sur la base de l'instinct. Or l'homme n'a pas à proprement parler d'instincts, en dehors de ceux qui le relient à ses semblables. Pour énoncer le problème clairement : comment va-t-il pouvoir accéder à l'information dont il a besoin pour survivre ?

N'ayant pas de programme, l'être humain n'est pas soumis au schéma stimulus-réponse ; il peut inverser ce schéma et anticiper la réponse de son environnement, ce qui lui permet jusqu'à un certain point de le contrôler. Mais on a rappelé plus haut que l'être humain n'a pas à proprement parler d'environnement, mais seulement un monde. Celui-ci est d'abord et avant tout un monde fait du langage, et

de tout ce que celui-ci rend possible. Il ne faut donc pas s'étonner que nos machines soient « vivantes », « organiques ».

Cette séparation foncière de l'homme d'avec la nature qui rend possible les guerres, les famines, les villes, etc., rend également possible une organisation de l'information qui soit propre à l'être humain et qui serve ses besoins. Or le but de toutes les techniques est toujours la communication. À une certaine époque, le but était de joindre les peuplades les plus reculées par le téléphone. Il serait maintenant de brancher tout le monde sans exception. L'homme n'étant pas véritablement lié à la nature, comme l'animal, puisqu'il est un être de culture, de seconde nature, l'idéal est pour lui un consensus universel qui le relie à tous les hommes.

La technique est globalisante

Elle recrée le lien avec la nature qui n'existe pas pour l'homme : il peut mettre fin à la nature parce qu'elle n'existe pas pour lui. La technique transforme l'homme parce que l'homme est déjà transformé par rapport à l'animal. Comme dit Max Frish, « *la technologie est l'art d'arranger le monde pour ne pas être obligé de l'affronter* ». Elle est l'art de transformer ses faiblesses en forces, pour combler ses besoins. Philippe Breton nous rappelle ce qui suit :

« Au début, à l'étape même de sa gestation, l'ordinateur est investi symboliquement d'une charge positive, là où la bombe atomique avait représenté le summum d'une charge négative. Dans un certain sens, l'ordinateur est le même objet que la bombe : un seul objet technique qui présente une double face, l'une diabolique, l'autre angélique, en forme de contrepoint et de rachat moral ». Cela peut paraître surprenant. Les deux événements concernent pourtant les mêmes hommes. Le biographe de von Neumann, Steve Heims, affirme de façon convaincante que celui-ci voyait les machines qu'il construisait comme une « extension de lui-même », permettant de dépasser les limitations humaines. Or von Neuman est à la fois celui qui invente l'ordinateur et celui qui, entre autres travaux sur le sujet, calcule la hauteur exacte à laquelle la bombe devait exploser pour causer le maximum de destruction ». (*L'utopie de la communication. L'émergence de « l'homme sans intérieur »*, Paris, Éditions de la Découverte, 1992, p. 105-106.)

La technique n'est pas neutre, elle a un double visage, tel Janus, et se retrouve au cœur de la polémique sur les aspects positifs ou négatifs d'Internet. Nous avons décidé de maintenir le cap sur les aspects positifs, car les aspects négatifs sont suffisamment dénoncés par la classe intellectuelle, dont le discours tend de plus en plus à se restreindre à la critique déconstructive. Du temps de Kant, il ne suffisait pas de critiquer négativement, mais encore fallait-il que cette critique s'appuie sur un projet positif. Le même Kant pourrait fournir le modèle le plus positif qu'on puisse imaginer pour les rapports sur Internet :

Dans son projet de *Paix Perpétuelle*, il écrivit que tous les pays devaient s'unir pour former une « assemblée des peuples » qui veillerait à la paix entre les nations. Il fallut attendre 125 ans après la parution de ce texte, en 1795, pour que soit créée la *Société des Nations*, après la Première Guerre mondiale. Elle fut remplacée après la Deuxième Guerre mondiale par les *Nations unies*. Kant est en quelque sorte le parrain de l'idée des Nations unies. Seule la « raison pratique » de l'homme permettait de faire sortir les États, selon Kant, d'un « état naturel » qui les poussait à d'incessantes guerres entre eux et pouvait créer un nouvel ordre international qui empêcherait les guerres. Le chemin jusque-là n'était pas tout tracé, mais il incombait à l'homme de travailler en ce sens pour « assurer la paix durable et universelle ». La création d'un tel organisme était pour Kant un but lointain, c'était quasiment le but ultime de la philosophie. (Jostein Gaarder, *Le monde de Sophie* [1991], Roman Seuil, 1995.)

Mais on sait bien que le Bien suprême n'est pas encore virtuellement réalisé dans le monde. Suivant Kant, si on a besoin de postuler un plus grand bien, possible également grâce à notre collaboration, ce n'est pas par manque de mobiles moraux pour faire le bien en ce monde, mais plutôt par manque de conditions extérieures dans lesquelles réaliser, conformément à ces mobiles, une fin en soi comme fin ultime morale (« Sur le lieu commun : il se peut que ce soit juste en théorie, mais, en pratique, cela ne

vaut point », dans E. Kant, *Oeuvres philosophiques*, vol III, p. 257). Ce n'est pas qu'on manque de raisons pour faire le bien dans le monde, mais les conditions sont telles que les mobiles communs ont besoin de mobiles supérieurs. L'histoire de l'ordinateur montre, depuis le début, une volonté de faire le bien, d'assurer une forme de service universel n'ayant rien de comparable avec le service militaire. Comme dit Jean-Claude Guédon, « les réseaux d'ordinateurs donnent une nouvelle chance à la communication » (*La planète cyber. Internet et cyberespace*, Découvertes Gallimard, 1996, p. 11). Le télégraphe, le téléphone, la radio, la télévision et finalement l'ordinateur et le multimédia sont à chaque fois une nouvelle chance que l'homme se donne à lui-même, par ses réseaux techniques, de se transformer en l'être qui ordonne intérieurement comme extérieurement toute réalité aussi bien que pourrait le faire le programme animal le plus sophistiqué.

Internet a-t-il un futur ?

Dans l'émission *Talk of the Nation* : Science Friday du 13.12.96, Vinton Cerf (actuel vice-président d'Internet Architecture ayant développé le protocole TCP/IP avec l'aide de Bob Kahn) répond avec beaucoup d'amabilité et d'empressement aux questions que se posent les usagers du réseau. Au journaliste qui lui demandait ce qu'il pensait, en tant que père d'Internet, de l'évolution de son petit, il répond ceci : « *La bonne nouvelle est que l'enfant grandit ; la mauvaise est aussi qu'il grandit* ». La croissance effrénée des réseaux pose des problèmes de logistique, mais plus fondamentalement, le père d'Internet se demande si le réseau est destiné à rester un éternel enfant. Or il n'est pas loin de répondre affirmativement à cette question : l'idéal serait peut-être que le réseau continue toujours de grandir, d'apprendre.

Mais un enfant a besoin d'être soutenu, et Cerf ne pense pas que l'on pourra éviter la commercialisation. Déjà, le réseau ne pourrait être ce qu'il est sans le support des ressources commerciales. Pour lui, ce n'est pas à même les budgets du gouvernement ou de corporations qu'on devrait garantir à la population l'accès à Internet[68]. La structure doit se supporter elle-même. Et si on en croit le « père d'Internet », le futur ira dans le sens d'une différenciation des services (on pourrait par exemple avoir des tarifs qui suivraient la quantité de ressources utilisées par certaines applications), qui devraient être de plus en plus axés sur l'individu, qui devra façonner Internet suivant ses besoins plutôt que de continuer de dire que 90 % de ce qui s'y produit est dépourvu de valeur. On peut d'ores et déjà y effectuer des recherches, (Cerf raconte comment il en a fait récemment l'expérience en visitant des sites sur l'histoire de la radio pour se préparer à rencontrer des représentants de chez Marconi pour les célébrations du centenaire). Un autre exemple fourni par le « père d'Internet » : « *Si les chauffe-eau étaient branchés sur Internet, la compagnie d'hydro-électricité pourrait demander à ses abonnés de diminuer la température pendant 15 minutes, afin de lui permettre de faire face à une augmentation subite de la demande* ».

Si on en croit les premiers fondateurs d'Internet, dont Vinton Cerf est un illustre exemple, l'ordinateur personnel a été créé pour les individus. C'est maintenant à eux de modeler Internet plutôt que de se laisser modeler par lui. Mais comme l'individu est ce qu'il y a de plus vulnérable, on ne saurait négliger les questions de sécurité. Or il semble que les problèmes soient en voie d'être complètement résolus de ce côté, par l'emploi notamment de deux clés d'encryptage et de décryptage plutôt que d'une seule clé d'encryptage.

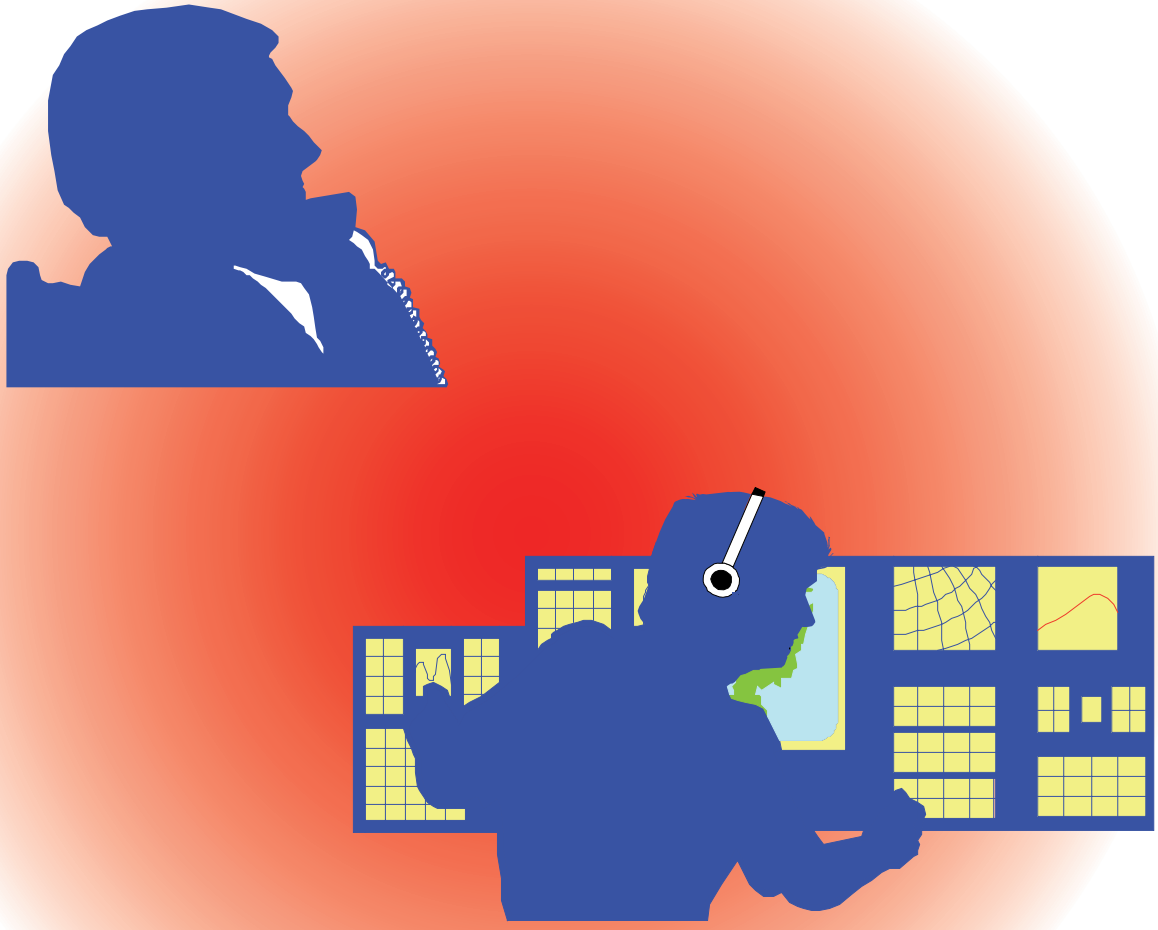
[68] Ce qui n'empêche pas Cerf d'encourager fortement les gouvernements à subventionner la recherche fondamentale et appliquée, qui rapporte beaucoup plus que l'investissement qu'elle coûte, même en faisant la part des échecs : « Lorsque ARPA (Advanced Research Projects Agency) fut fondée à la fin des années 50, son but était d'éviter d'avoir à nouveau à faire face à des surprises du genre Spoutnik. Elle a, depuis, fourni une corne d'abondance de résultats technologiques qui ont favorisé la sécurité nationale de multiples façons, produisant des résultats pourvus d'une pertinence militaire directe ou indirecte, en étendant la base technologique de la nation, sur laquelle l'industrie fait plus d'affaires et produit plus de produits et services que jamais auparavant ».

Une fois réglées les questions d'encryptage et de décryptage, prédit Vinton Cerf, la prochaine vague qu'auront à affronter les internautes sera celle de la commercialisation. Les fournisseurs de services devront travailler de concert avec ceux qui développent les outils multimédias, afin de faire face à la poursuite de l'augmentation du trafic dans les réseaux et à la multiplication des moyens d'en user.

Et finalement, au Québec comme au Canada, il faut tenir compte du contexte historique des télécommunications, qui a toujours été celui d'une lutte contre l'américanisation. D'une certaine manière, Internet met fin à ces luttes et il ne faudrait pas prendre pour une séduction à laquelle il faut savoir résister ce qui est peut-être seulement une nouvelle chance pour la communication, contre la méfiance naturelle.

Derrière la lutte contre l'américanisation se cache une autre lutte, celle pour la suprématie du français. S'il s'agit de l'emporter sur l'anglais, la lutte est perdue d'avance. Mais s'il s'agit seulement d'imposer la présence du français sur le WWW, c'est en se battant pour l'internationalisation qu'on aura le plus de moyens d'y parvenir. Voilà pourquoi *L'Agora* compte éventuellement publier tous ses documents en trois langues sur Internet (français, anglais, espagnol).

Écoutes téléphoniques et captu-re des télécommunications



Introduction à l'espionnage économique :

Nous allons ici dévoiler une face cachée, inconnue du grand public et des petites entreprises, voire même de la justice. Des juges, avocats, policiers, journalistes, ex-salariés, associations de citoyens, découvriront dans ces pages des éléments qu'ils ne pouvaient soupçonner en matière d'écoutes téléphoniques, qui les inciteront peut-être à mieux se protéger. Nous exposerons ici les dangers d'un monde tout électronique basé aussi sur les moyens sans fil. Quels sont les risques ? Aboutir à une dictature organisée à la solde des gouvernements, des dirigeants politiques et groupes industriels, qui obtiendraient ainsi illégalement des informations sur toutes vos décisions. Si vous utilisez le téléphone, un cellulaire, un téléphone sans fil, la visioconférence, un micro-ordinateur portable raccordé sur des réseaux radio ou GSM, alors on peut vous écouter et même vous localiser. Le pouvoir en place et d'autres vont pouvoir vous suivre à la trace, connaître le contenu de vos appels téléphoniques, vos choix, et ainsi vous contrer, surtout si vous les dérangez avec des affaires en justice.

Il n'existe aucune structure de contrôle en France, chargée de vérifier si les opérateurs français ou étrangers ne se livrent pas à des écoutes illégales sur notre territoire. Ils peuvent donc faire de l'espionnage en toute tranquillité, et sans le moindre risque. Il est évident que des petites sociétés ont été victimes de divers procédés visant à éliminer celles qui innovent et qui sont trop efficaces, mais c'est aussi le cas pour de simples citoyens. À ceux qui viendraient hurler que toutes ces affirmations ou déductions sont fausses, je répondrai simplement, qu'ils savent très bien, qu'en raison de jurisprudences abusives, d'une législation à deux vitesses dans notre pays, il est devenu impossible de prouver les malversations effectuées par des individus que l'on dit respectables, sans se mettre soi-même en infraction.

Maintenant les salariés ou professionnels qui ont été témoins ou victimes de ces faits, doivent les dénoncer s'ils ont des preuves. L'aspect plus grave, c'est que la non-dénonciation de ces malversations favorise leur progression, surtout la montée en puissance mafieuse de politiques, PDG, groupes qui se croient tout permis. Il y a des journalistes ou juges intègres qui enquêtent, mais ne peuvent souvent rien faire. D'autres, au lieu de faire le travail pour lequel ils sont payés, préfèrent être aveugles. Ce qui dénote un manque de perspicacité de courage, mais aussi une préférence pour des intérêts douteux.

Sur le plan gouvernemental, un État qui sera en mesure d'acquérir toute la méthodologie nécessaire pour pénétrer les systèmes de télécommunication et informatiques des autres pays, pourra les contrôler. Qui contrôle les communications, contrôle le monde et l'économie internationale. On peut se poser des questions sur l'effondrement économique des pays asiatiques. Tous les systèmes sont interconnectés entre eux aujourd'hui. L'augmentation des moyens de communication sans fil contribue à augmenter fortement les fuites d'informations sensibles. En raison de la miniaturisation et de la sophistication des équipements, il devient impossible de savoir si on est écouté. De plus, les services spéciaux du monde entier recrutent des hackers, phreakers[69] dans le but de pénétrer les centres informatiques ou de commu-

[69] Le *phreaking* est né aux États-Unis dans les années 1970. Un des mythes fondateur du phreaking est l'histoire de *Captain Crunch*. Ce phreaker de renommée internationale avait utilisé un sifflet trouvé dans une boîte de céréales *Captain Crunch* pour accéder à des fonctions spéciales du central téléphonique. En effet, le son émis par ce sifflet avait une fréquence de 2600 Hz, la même fréquence que le signal utilisé pour piloter le central téléphonique. Un des groupes de phreaking les plus connus s'appelle d'ailleurs 2600. Actuellement, avec l'arrivée du numérique dans les systèmes téléphoniques, les procédés utilisés sont beaucoup moins rocambolesques.
En France, au début des années 1970, des chercheurs de l'IRIA (devenu depuis INRIA) avaient remarqué qu'en déclenchant du doigt un très bref raccrochage pendant quelques centièmes de seconde, le standard l'interprétait comme un 1 sans passer par le testeur de numéros. Cela permettait ainsi aux employés n'ayant pas l'accès au téléphone international (à l'époque, préfixe 19) de le composer tout de même. Les télécartes furent l'objet d'actes de piratage pendant les années 1990 notamment

nications des grosses institutions des divers pays industrialisés. Les objectifs sont clairs, ils concernent le vol d'informations dans une première mesure, voire leur altération.

Paradoxalement, certaines de nos institutions chargées de la sécurité du pays sont confrontées à de véritables problèmes, comme le terrorisme ou le trafic d'armes. Elles doivent en effet être en mesure de détecter les risques d'attentats terroristes. Il est donc nécessaire qu'elles disposent des moyens d'écoutes et de décodages les plus sophistiqués. L'évolution technologique très et trop rapide fait que chaque système est périmé d'une année sur l'autre. Cela fait qu'à un moment donné, les systèmes des institutions de sécurité de l'État se retrouvent totalement dépassés pour les missions de sécurité dont elles ont la charge.

La sophistication de l'électronique et la baisse des coûts des systèmes, mettent ce matériel à la portée de n'importe quelle bourse. La volonté de croissance, s'exerce dans notre société de surconsommation au profit des multinationales, et au détriment des citoyens moyens qui sont en réalité les cibles des premiers. Avec la guerre des tarifs, les incitations pour persuader les sociétés et les utilisateurs d'ordinateur d'utiliser les réseaux pour acheter, il faut s'attendre à une augmentation très rapide des « casses » informatiques et téléphoniques par des mafieux en col blanc pouvant même venir d'institutions officielles. On peut dire que ce sport est en augmentation constante depuis 1993.

La sophistication des logiciels permet à une clientèle de moins en moins technique de se connecter de plus en plus facilement sur des sites du monde entier comme avec Internet qui est un des plus grands réseaux d'écoutes illégales. Les uns et les autres font tout pour s'enrichir au dépend des simples citoyens.

Danger de la sous-traitance

Il est indéniable que le programme EO2 de France Télécom dont l'objectif est de diminuer le nombre de salariés et le nombre de sites, va contribuer à augmenter la sous-traitance, les risques de fuites d'infor-

---

pour une communication gratuite entre le phreaker et des BBS pirates distants, via un coupleur acoustique. Mais depuis, France Télécom a mis en circulation un nouveau type de télécarte, la T2G, avec un nouveau système de chiffrement.

Le système de chiffrement de ces nouvelles T2G n'a toujours pas été cassé (ou alors, la chose n'a pas été rendue publique) mais des phreakers ont trouvé un système ingénieux pour téléphoner gratuitement. En effet, il suffit d'utiliser une vraie T2G pour effectuer les authentifications puis d'utiliser un émulateur de T2G une fois la communication établie pour que la cabine ponctionne les unités sur une télécarte qui en fait n'existe pas. Cet émulateur porte le nom de Joséphina.

On peut pirater des systèmes téléphoniques de différentes manières. Généralement on appelle les systèmes capables de pirater un système téléphonique des boxs précédés d'un nom de couleur. Exemples : la beige box, la red box, la blue box etc., il en existe des centaines.

Nous avons vu précédemment que le son émis par le sifflet du Captain Crunch était de 2600 Hz, on peut considérer cela comme une blue box.

La blue box consistait simplement à utiliser les fréquences des opérateurs, qui transitaient par les mêmes circuits des anciens systèmes CCITT5. Aujourd'hui, les pays occidentaux utilisent le système SS7, et la blue box ne fonctionne plus avec ces systèmes plus modernes. Il paraîtrait que cette technique d'emploi des fréquences, est encore utilisée par France Télécom en cas de panne de ligne, mais cela paraît hautement improbable.

Cela dit, il y a encore peu de temps, le blue boxing était encore possible. En effet, on peut appeler des numéros verts internationaux en direction de pays étrangers fonctionnant encore avec ce système en CCITT5 (pays du sud généralement), et là à envoyer une fréquence adéquate, et ainsi rappeler un numéro international.

Il existe encore d'autres boxs. Une des plus simples est la beige box, elle consiste à brancher sur une ligne téléphonique une autre ligne téléphonique. Cette technique, tout comme les autres d'ailleurs, est totalement illégale, et passible de fortes amendes et peines de prison. Il y a un certain temps, il était même possible de gagner de l'argent grâce a cette technique. Il fallait appeler un serveur minitel, rester connecté le plus longtemps possible, et ensuite se faire envoyer des lots... Cette technique est caduque maintenant, il n'y a plus de serveur minitel qui propose des lots de fidélité.

D'autres box existent, aux utilités multiples... Par exemple, écouter une conversation téléphonique, ou alors ne pas faire payer celui qui appelle grâce à un montage (technique dite de la black box, possible en France, mais attention un robot nommé *SIRIUS* de France Télécom repère cette box, et les utilisateurs se faisant repérer risquent de lourdes peines)

Aujourd'hui le phreaking en France n'a plus beaucoup d'adeptes. C'est en effet une discipline dangereuse, et les gens préfèrent s'intéresser au hacking, beaucoup plus médiatisé. De plus, la généralisation de connexions Internet haut-débit et la baisse des tarifs téléphoniques ont limité son intérêt même s'il reste encore techniquement possible.

mations, nous pouvons même dire l'espionnage. Les incidents techniques ou perte financières progresseront dans les années à venir, surtout avec la multiplication des opérateurs étrangers sur notre sol.

Nous pouvons constater que nos grands dirigeants et responsables sont incapables de prendre en compte les aspects confidentialité des communications. Les raccordements de plus en plus nombreux sur Internet et l'explosion du vocal, vont faciliter les écoutes illégales à partir de n'importe quel point du globe puisque la cryptographie lourde est interdite en France. L'utilisation des satellites va faciliter les écoutes par interception des rayonnements électromagnétiques ; un récepteur radio suffit. Le traitement de ce qui est enregistré est plus complexe, mais possible. Ce que beaucoup ignorent aussi, même certains dans les ministères, c'est que ces signaux informatiques sont récupérables par cette méthode, même sur une prise de terre.

Sur ce sujet, tous les responsables de sites stratégiques, comme les énarques, les polytechniciens se défilent en vous riant au nez et en sortant des boutades, et plus ils sont diplômés, plus ils sont virulents et arrogants. Il arrive aussi que les infractions sur les écoutes soient commises par les représentants mêmes de l'État. Mais dans ce cas, les poursuites en justice sont impossibles, car de l'aveu même du Président de la République française, lors de l'une de ses déclarations, notre pays dispose d'une justice à deux vitesses. Il est aussi très intéressant de constater dans notre pays, que des indépendants qui ont des compétences pointues dans le domaine de la sécurité, se retrouvent discrédités par des individus d'entreprises de sécurité ou de gardiennage.

Faire passer quelqu'un pour un pirate, relève de la diffamation et est passible de poursuites, alors pourquoi ce risque inutile ? Eh bien parce qu'il y en a qui ne se gênent pas parmi elles, pour aller récupérer des informations confidentielles chez leurs clients et poser des écoutes téléphoniques, pour le compte des concurrents, qui leur ont passé une commande avec un coût qui permet un bénéfice, bien souvent net d'impôt. Il est aussi courant dans ce milieu, que des individus incompétents, s'approprient la paternité des travaux des conférenciers, et s'amusent à le refacturer à leurs clients, qui n'auront qu'une information incomplète de toute façon.

Préambule

Le maillon faible

Chacun sait que la solidité d'une chaîne ne vaut que par son maillon le plus faible.

Dans le cas des télécommunications, le maillon faible est justement le système de transmission à distance. Qu'il y ait intervention humaine, comme jadis dans le télégraphe ou avec les opératrices du téléphone, ou que la transmission se fasse par câble, radio ou satellites, le simple fait d'envoyer un signal sur un support physique, le fragilise en terme de sécurité.

Nous verrons dans cette section des méthodes d'interception téléphoniques agrémentées de quelques faits historiques piochés ça et là.

Nous étudierons les techniques de détournement et de capture de l'information, depuis le télégraphe jusqu'aux systèmes informatiques, en passant par Internet. Nous évoquerons les différents moyens de protection et de sécurité, les procédés de cryptage faisant l'objet d'un autre chapitre.

Le but n'est pas de former des apprentis pirates ou espions, mais bien d'indiquer les failles courantes que l'on peut rencontrer dans les systèmes de communication et les moyens d'y remédier.

Les écoutes téléphoniques sont les plus répandues aujourd'hui, réalisées aussi bien sur l'ordre des politiciens ou des PDG véreux, d'officines clandestines pour le compte d'entreprise, de la police, voire même de la presse. N'importe qui en réalité, peut écouter n'importe qui. Même les ministres s'écoutent entre eux aujourd'hui, c'est à la mode. Les points de raccordement sont multiples, de même que les méthodes. Les failles viennent aussi des opérateurs. Il faut bien des complicités, ne serait-ce que pour savoir où il faut connecter une bretelle.

Télégraphe et secret

Les problèmes du télégraphe optique de Chappe

Le système de Chappe, que nous avons longuement détaillé, présentait en terme de sécurité une lacune de taille : il suffisait de s'équiper d'une lunette assez puissante et de se placer au bon endroit pour capter les messages qui circulaient sur le réseau. Le monopole institué dès l'origine de ce procédé de transmission ne pouvait qu'aiguiser la curiosité des ennemis politique ou militaire de l'État Français. Dès 1801, seul le projet de transmission des résultats de la Loterie nationale est retenu comme application purement civile.

Pendant la Révolution et l'Empire, les usages du télégraphe sont essentiellement militaires, et sous la Restauration, plutôt de police.

Nous avons vu que Chappe avait mis au point un « vocabulaire » codé, et que seuls les personnels aux extrémités des lignes possédaient ces codes, de sorte que les postes intermédiaires ne savaient pas ce qu'ils transmettaient.

Nous avons parlé d'une affaire de fraude, en 1836, par deux banquiers bordelais qui avaient soudoyé un employé du télégraphe pour qu'il ajoute des signaux supplémentaires à la suite d'envoi de dépêches officielles.

Le télégraphe électrique

Le développement du réseau de télégraphe électrique filaire posa d'emblée les mêmes problèmes de sécurité. Monopole d'usage de l'État au début, les dépêches étaient « chiffrées » par sécurité. Cependant, sous la pression des saint-simonniens, Louis Napoléon Bonaparte voit dans le télégraphe un instrument susceptible de favoriser l'industrie et de commerce. L'assemblée reste cependant hésitante. En perdant son monopole d'utilisation du télégraphe « le gouvernement n'aura plus aucun privilège… ». Pour « éviter « qu'on ne livre l'usage du télégraphe aux factions qui s'en serviront pour ourdir avec plus de facilité et de rapidité leurs détestables complots »[70], la loi exige que les dépêches privées soient en langage clair et signées. L'usager doit déclarer son identité. Ce dispositif de censure n'est pas propre à la loi française ; on trouve des régimes juridiques voisins en Prusse, en Autriche et aux Pays-Bas.

[70] Ferdinand Barrot, discours à la Chambre des députés, 1er mars 1850, in *Le Moniteur universel.*

Le téléphone

Piratage physique des installations téléphoniques :

Les guerres et les écoutes téléphoniques

En 1915, des ingénieurs français s'aperçoivent que, grâce à un phénomène technique lié au mode de communication de l'époque (le « retour » des téléphones se faisant par la terre, au moyen de piquets enfoncés dans le sol), il est possible, dans certaines conditions, d'écouter les conversations adverses. Et ce, d'autant plus que les premières années de la guerre se feront dans les tranchées et que les lignes ennemies sont parfois proches de quelques mètres.

Dès 1916, pendant la bataille de Verdun, un premier poste d'écoute artisanal donnera de bons résultats, et l'expérience se généralise avant la création officielle, début 1917, des Sections spéciales d'écoute mises au service du Service de Renseignements. Celles-ci se composent de techniciens qui doivent repérer les endroits où des « fuites » permettent d'intercepter les conversations ennemies et d'interprètes capables d'écouter, en temps réel, les conversations ennemies. Le rôle de ces interprètes est d'autant plus difficile qu'il leur faut comprendre non seulement l'allemand mais aussi ses différents patois, et être familiarisés, dans la langue de Goethe comme dans celle de Voltaire, avec la terminologie militaire. La plupart des interprètes travaillant déjà pour l'état-major, les Sections spéciales se rabattront sur quelques professeurs et sur des volontaires de la Légion étrangère d'origine allemande ou suisse.

Durant les deux dernières années de la guerre, les écoutes téléphoniques rendront d'inappréciables services, permettant de juger du moral des troupes ennemies, de tenir à jour ses mouvements et, au niveau des champs de bataille, d'être informé de ses offensives et de capter les informations destinées au réglage de l'artillerie. Ajoutons que ces humbles auxiliaires du Service de Renseignements travaillent dans les tranchées de première ligne, directement sous le feu des Allemands. Leur travail de repérage permettra aussi de colmater quelques brèches béantes ouvertes dans les communications françaises. Leur rôle et même leur simple existence sont restés, jusqu'à ce jour, quasi ignorés des historiens.

L'histoire de la Source K. *(Extrait de « Résistance PTT »)*

Le 20 juillet 1940, les services d'entretien des lignes souterraines à grande distance regagnent Paris. L'accord passé entre l'administration des P.T.T. et les autorités d'occupation prévoit la reprise en main par les techniciens français, sous contrôle allemand, de l'ensemble du réseau, à l'exception des territoires intégrés au Reich[71], ou rattachés au protectorat du gauleiter nommé en Belgique

Robert Keller retrouve donc son poste et ses responsabilités. Ses équipes conservent leur ancienne structure, mais doivent supporter l'incorporation d'un ou deux pionniers allemands par groupe. Durant plusieurs mois, la tâche essentielle consiste en une réfection rapide des grands circuits. Keller, qui nourrit déjà certains projets, veille à la bonne exécution des travaux. Il stimule si bien ses hommes que peu à peu la surveillance se relâche et qu'il parvient à visiter ses chantiers sans être flanqué de ses indésirables accompagnateurs. Bientôt même, les équipes d'urgence ne vont plus avoir d'observateurs à leurs côtés lors des interventions.

C'est au cours de ces quelques mois que Robert Keller établit un plan d'action avec schéma visant à neutraliser le réseau des lignes souterraines à grande distance. On ignore tout des liaisons qu'il eut à cette époque, car il a emporté ce secret dans sa mort, mais ce qui est certain, c'est que ce plan parvint en Angleterre puisqu'il figurait parmi les archives du B.C.R.A.[72] Minutieusement rédigé, il montrait comment, en quelques heures, on pouvait bloquer tous les circuits, et isoler téléphoniquement les centres vitaux du commandement allemand. Ce projet, conçu dans le cadre d'un débarquement allié, aurait été

[71] L'Alsace et une partie de la Lorraine sont annexées par l'Allemagne.

[72] Bureau central de renseignements et d'action était un service d'espionnage français, créé en 1940.

d'une importance capitale en juin 1944 si son auteur avait encore été là pour le faire appliquer. Mais la discrétion, bien compréhensive, dont Robert Keller fit preuve, ne permit à aucun de ses camarades de pouvoir l'utiliser.

Devenu, comme on l'a vu plus haut, représentant du S.R. au sein de la Direction des Recherches et du Contrôle technique des P.T.T., le capitaine Combaux s'est assuré le concours de M. Sueur, ingénieur de ce service. Les deux hommes ont longuement réfléchi sur les moyens à mettre en œuvre pour capter les conversations allemandes qui passent par les câbles à grande distance. Sécurisés par l'important dispositif qui contrôle les circuits, les occupants les utilisent en exclusivité pour leurs liaisons avec le Reich. Les lignes : Paris - Reims - Verdun - Metz, reliée à Sarrebruck, et Paris - Châlons - Nancy - Sarrebourg - Strasbourg reliée à Appenweier, sont particulièrement surveillées puisqu'elles mettent en relations toutes les sphères des autorités d'occupation avec leurs hiérarchies de Berlin. Combaux et Sueur savent bien que surprendre les communications qui s'échangent sur ces câbles prioritaires permettrait de percer le secret des plans allemands, et par là même de leur porter un terrible coup en faisant bénéficier les Alliés de ces informations. Seulement atteindre les circuits par les voies normales relève de l'utopie. Tous les postes d'amplification, toutes les stations de répéteurs, sont, ainsi qu'on l'a montré précédemment, placés sous une surveillance sévère. Les vérificateurs français qui en assurent le fonctionnement ne peuvent faire le moindre geste sans éveiller l'attention des techniciens allemands qui les doublent. La seule et unique possibilité qui existe, mais combien illusoire et insensée dans sa réalisation, c'est celle avancée par M. Sueur : le « piquage sauvage sur câbles ».

Pourtant, aussi téméraire et extravagant qu'il soit, c'est à ce projet que s'attaquent les deux hommes. Sur le papier, son exécution ne paraît pas insurmontable. Il faut préparer des amplificateurs spéciaux à grande impédance d'entrée qui puissent être insérés dans les circuits sans modifier les impulsions des stations de mesure. Les câbles étant en effet équilibrés en constantes électriques fixes, la moindre variation est facilement décelable. Or, dans le plan établi par Sueur, il conviendrait d'introduire sur la ligne des appareils et un métrage de câble les reliant au circuit. Un tel branchement présente de gros risques, car il entraînerait sûrement une modification des indices sur les mesures habituelles ; à moins que les appareils espions ne soient appropriés avec une précision rigoureuse. C'est un premier obstacle, mais il peut être franchi grâce à la haute compétence des spécialistes. Le second palier du projet consiste à louer au plus près du lieu de dérivation prévu une habitation discrète dans laquelle on pourrait placer les têtes et les amorces de câble ainsi que les amplificateurs d'écoutes. C'est le point qui présente le moins de difficultés, encore que rechercher une maison libre, présentant des garanties de tranquillité et de sécurité, sur le parcours des lignes, n'apparaisse pas aussi simple que cela.

Mais ces deux premiers volets de l'opération imaginée par Sueur et Combaux ne sont qu'un aimable enfantillage en regard de ce que représente le dernier, car il s'agit maintenant d'intervenir sur le câble lui- même. À partir de là, on entre dans une phase du projet qui semble irréalisable. Il faudrait, en effet, en dépit de la surveillance allemande, ouvrir des fouilles sur la ligne, ce qui peut déjà demander plusieurs jours ; creuser une tranchée préparatoire au niveau de la dérivation ; sortir du pavillon loué les amorces préalablement apprêtées ; accéder au câble en service, l'ouvrir, dénuder les fils un par un et sélectionner sans erreur ceux des circuits à mettre en écoute, les couper, les dériver, puis rétablir vivement le contact afin que l'opération ne cause pas un trop long dérangement susceptible d'intriguer les techniciens allemands ; ensuite, remettre tout en place et refermer les fouilles. Un travail aussi périlleux, comportant tant de risques, qui pourrait le faire ?

Ceux qui tenteraient de l'entreprendre devraient être des hommes aux nerfs d'acier, aux capacités professionnelles affirmées, connaissant parfaitement le schéma des grands circuits et leurs particularités, doués d'une audace hors du commun, et animés d'un esprit patriotique poussé jusqu'à l'abnégation. De plus, il ne pourrait s'agir que d'une équipe soudée, habituée à travailler en harmonie et confiance, dirigée par un responsable lucide aux compétences certaines, capable de maîtriser les impondérables.

Enthousiaste et sceptique à la fois, le capitaine Combaux posa la question :
— Un tel chef d'équipe existe-t-il seulement ?
— Oui, répondit M. Sueur, je le connais, c'est l'Ingénieur Robert Keller.

C'est dans les premiers jours de septembre 1941, la date est imprécise, que les deux instigateurs de ce projet extraordinaire le soumettent à Keller. L'entrevue a lieu dans le bureau de M. Sueur, rue Bertrand. Cet entretien mémorable mérite d'être relaté par l'un de ses participants. Écoutons donc le capitaine Combaux nous en faire le récit :

« Je posai le problème ; M. Sueur développa la solution technique. Robert Keller écoutait et approuvait. J'étais plus ému que je n'aurais voulu le paraître lorsque je m'adressai à lui pour insister une dernière fois, avant la décision finale, sur les dangers de l'aventure. J'étais officier ; le risque de guerre faisait partie de mon métier. Je pouvais sentir au-dessus de moi des chefs militaires qui surveilleraient de loin le combat que nous allions livrer. Il n'en était pas de même pour mes compagnons. Ils devaient agir à l'insu de leurs supérieurs hiérarchiques ; quelque envie que nous en ayons eue, nous avions le devoir de ne point compromettre dans une affaire aussi grave le Directeur des Télécommunications, dont nous connaissions les bons sentiments, mais qui avait la lourde charge de défendre devant l'occupant l'ensemble de nos services. Robert Keller avait, plus que tout autre, des raisons d'hésiter. Il songeait à sa femme et à ses quatre enfants. Il pouvait, sans déshonneur, rejeter une entreprise aussi téméraire, et dans laquelle il allait courir, en raison même de ses fonctions, les risques les plus graves. Il accepta cependant. Il fit avec résolution le premier pas sur la route fatale qui allait le mener au supplice...

Il nous dit tout de suite qu'il avait derrière lui une équipe sur laquelle il pouvait compter, prête à braver tous les dangers pourvu que cela soit contre l'ennemi et pour la France. Le vérificateur Lobreau, les chefs d'équipe Laurent Matheron et Pierre Guillou étaient de ceux-là. Ils l'avaient suivi et assisté au cours de la première campagne de France. Ils allaient être auprès de lui, devant un danger considérablement accru, et avec la même fidélité.

Sur Robert Keller, en vérité, reposait le succès ou l'échec de l'entreprise. Si Sueur pouvait se charger de l'étude et de la réalisation des amplificateurs, si je pouvais régler l'acquisition du local et les questions d'exploitation, lui seul était capable de réaliser l'essentiel, d'accomplir ce tour de force incroyable que représentait le travail sur câble... »

Que Robert Keller eût refusé à cet instant les propositions de ses interlocuteurs, et la Source K serait demeurée à l'état de projet, car aucun technicien des P.T.T. ne réunissait alors ni les compétences ni les qualités requises. Pas un ne possédait suffisamment d'ascendant et n'inspirait assez la confiance pour entraîner une équipe de spécialistes dans cette voie périlleuse.

Et ceux qui au S.R. choisirent l'initiale K de Keller pour désigner la source de renseignements vitaux qui leur parvinrent par ce canal ne pouvaient mieux montrer que c'est à cet homme héroïque qu'ils durent la somme d'informations sensationnelles dont ils firent bénéficier les Alliés.

L'acceptation de Robert Keller déclenche le démarrage de l'opération. Sueur effectue une étude très poussée pour déterminer le nombre d'amplificateurs nécessaires. Il parvient à la conclusion qu'il faut en prévoir un minimum de 6. Leur fabrication délicate, et le coût élevé de celle-ci, posent un premier problème. Un habile travail d'approche permet toutefois à l'ingénieur d'acquérir la complicité active du chef des laboratoires de la Société anonyme de télécommunications, société privée, qui travaille exclusivement pour les P.T.T. M. Lebedinski, russe d'origine, mais naturalisé français, accepte en effet spontanément de faire construire dans les ateliers de son entreprise repliée à Montluçon les pièces détachées des appareils conçus par M. Sueur. Grâce aux camions qui font la navette entre l'usine et les entrepôts demeurés en zone occupée, les éléments d'amplificateurs passeront sans problèmes la ligne de démarcation. De son côté, le capitaine Combaux règle la question des fonds nécessaires à une telle opération.

Doté par les soins du S.R. d'un laissez-passer permanent, il se déplace à volonté entre les deux zones ; ce qui lui permet de recevoir du capitaine Simoneau au cours de ses voyages tout l'argent indispensable à la mise sur pied du projet. Dans le même temps, le poste P 2 du S.R. fait diligence pour recruter et former des opérateurs valables. Tâche ardue assurément, car ceux-ci doivent parler, et surtout parfaitement comprendre la langue allemande, y compris dans les variations de la conversation courante. Il leur faut également posséder le sens de l'initiative et l'instinct de débrouillardise, vitaux pour leur travail et leur sécurité. Enfin, il va de soi que pour noter tout ce qu'ils entendront, il leur est indispensable d'avoir une parfaite maîtrise de la sténo, et de connaître les structures de fonctionnement des services du Reich.

Le premier opérateur envoyé à Combaux par Simoneau arrive à Paris le 5 mars 1942 ; c'est le sergent-chef Édouard Jung. Ayant suivi les cours accélérés du centre d'instruction clandestin du S.R., connaissant parfaitement l'organigramme de la Wehrmacht et les noms des principaux officiers des différents services fonctionnant à Paris, c'est un habile spécialiste des transmissions, Alsacien de naissance, que Simoneau a eu la chance de pouvoir récupérer. Nanti de pièces d'identité irréprochables, il est aussitôt dirigé sur la Compagnie d'Assurances « *La Nationale* » où le sous-directeur M. Grimpel et l'agent général pour la région parisienne, M. Lionel Levavasseur, lui fournissent la carte accréditive d'inspecteur qui lui assurera une couverture de premier ordre.

Quelques jours plus tard, Jung parvient à repérer un pavillon libre sur le parcours du câble dans la Grande Rue de Noisy-le-Grand[73]. Après quelques démarches, il en obtient la location que Combaux s'empresse de régler. Située à moins de 6 mètres de la ligne, cette petite maison offre toutes garanties par son isolement, et son sous-sol surplombe de peu la route nationale sous laquelle court le câble Paris-Metz. Sans perdre de temps, Édouard Jung s'y installe, complétant l'aménagement sommaire laissé par le propriétaire de quelques meubles ramenés du marché aux puces de Montreuil. À peine sur place, sous prétexte de fuites dans les canalisations d'écoulement, il creuse une tranchée jusqu'à la haie de clôture bordant la route nationale, puis le mur du sous-sol est percé afin de laisser le passage à une gaine de protection. Le 6 avril 1942, tout est prêt pour recevoir le matériel d'écoute. Trois jours après, M. Lebedinski fait livrer les amplificateurs que M. Sueur transporte aussitôt au pavillon ; les têtes de câble et les amorces suivent. Il ne reste plus sur place qu'à procéder au montage de tout cet équipement en attente de branchement.

Le 10 avril, c'est chose faite ; la première phase de l'opération est terminée.

Pendant la durée de ces préparatifs, Robert Keller n'est pas resté inactif. Après un minutieux examen des schémas et un relevé de la zone choisie pour la dérivation, il a mis au point le procédé d'attaque du câble et réuni l'outillage le plus adapté à cette intervention. Puis, après mûre réflexion, il a choisi les hommes lui paraissant les plus qualifiés et les plus audacieux pour entreprendre un travail aussi difficile. À chacun d'eux, il a soumis le plan de l'affaire en insistant sur les risques qu'elle comporte. Sûr de leur fidèle discrétion, quelle que soit la décision prise, il leur a demandé de réfléchir avant de donner leur réponse. Mais celle-ci ne s'est pas fait attendre et, l'un après l'autre, les six compagnons qu'il a sollicités sont venus lui dire qu'ils étaient prêts à le suivre dans cette action dont ils savent mieux que personne qu'elle risque de les entraîner sur un mortel chemin.

Les affiches collées sur les panneaux de service dans chaque atelier, dans chaque centre, sont à cet égard éloquentes. L'administration militaire allemande prévient en effet que : « *Tout endommagement des moyens de transmission sera puni de la peine de mort.* » Malgré cette menace, dont ils savent bien qu'elle n'est pas formulée à la légère, les hommes choisis par Keller n'hésitent pas. Et aujourd'hui, l'on ne sait

[73] Ce pavillon était situé au 89 Grande Rue (aujourd'hui avenue Emile Cossonneau) à l'intersection de la N 370 et du CD N° 75 E. Réaménagé ces dernières années, ce carrefour porte maintenant le nom de « Place du 8 Mai 1945 ». La municipalité de Noisy-le-Grand a donné le nom de « rue du Réseau Robert Keller » à l'ancienne rue des Grammonts qui prend naissance à cet endroit pour rejoindre les bords de Marne.

pas ce qu'il convient d'admirer le plus : de cette confiance totale montrée vis- à-vis d'un chef estimé, mais téméraire, ou de ce tranquille courage patriotique bien dans la tradition de l'engagement résistant.

Le 2 avril, l'équipe formée par Robert Keller est constituée. Elle comprend :

Les vérificateurs : Lobreau du centre Paris-Saint-Amand, et Fugier du centre de La Ferté-sous-Jouarre.

Les techniciens sur ligne : Pierre Guilou, Laurent Matheron, Abscheidt et Levasseur.

Dans le plan prévu par Keller, chacun de ces spécialistes aura un rôle important à jouer pour lequel, en dehors des compétences professionnelles, l'audace et le sang-froid ne devront pas faire défaut. Ce plan, il faut maintenant l'exécuter.

Le 15 avril 1942, Robert Keller crée un défaut artificiel sur le câble Paris-Metz. La « Feldschalt-Abteilung » saisit le service de dérangement des lignes souterraines à grande distance d'une énergique réclamation, car deux circuits sont interrompus. C'est bien ce qu'espérait Robert Keller qui, nanti d'une autorisation de travaux en bonne et due forme signée par l'Administration, regroupe son équipe et part à la recherche du point de rupture. Naturellement, celui-ci est découvert à Noisy-le-Grand, en face du pavillon loué par Édouard Jung.

Le 16 au matin, les fouilles sont entreprises sur le trajet du câble. Afin de donner le change à d'éventuels curieux, deux tranchées sont ouvertes à côté de celle dans laquelle la dérivation doit être effectuée. Le 17, en fin de matinée, un technicien allemand vient sur place s'informer de l'état des travaux. Satisfait de la célérité déployée par les spécialistes français et des réponses rassurantes qui lui sont faites, il repart aussitôt. Keller a décidé, pour des raisons de sécurité, que l'intervention sur le câble se fera de nuit, et il en a informé Combaux. Dans la soirée du 18, ce dernier vient rejoindre l'équipe sur le chantier. Une tente d'intempérie a été disposée au-dessus de la fouille centrale afin de masquer un peu les travaux, et de filtrer l'éclairage dispensé par les lanternes ; des lueurs trop vives pouvant provoquer une réaction des patrouilles allemandes obnubilées par les consignes sévères du camouflage lumineux. Un peu avant 21 heures, Keller, Guillou et Matheron descendent dans la tranchée et s'attaquent au câble. Sitôt la gaine de plomb mise à jour, Keller se porte sur la ligne de service et donne l'ordre aux deux vérificateurs des stations de répéteurs encadrantes : Lobreau à Paris-Saint-Amand, et Fugier à La Ferté-sous-Jouarre, de retirer un à un chaque circuit de l'exploitation durant le temps nécessaire à sa coupure et à sa dérivation. C'est ce que font sans hésiter les deux hommes, sous les yeux mêmes des techniciens allemands, en prétextant un contrôle des mesures. Pour eux, la nuit va être longue, car ils vont devoir agir avec une apparente routine désinvolte devant leurs surveillants, tout en portant une extrême attention aux directives précises que leur transmettra Keller. Aucune erreur ne leur est permise, car elle se répercuterait aussitôt dans les autres centres d'amplificateurs dont le personnel a été laissé en dehors de l'action.

Dans la fosse, penchés sur leur ouvrage, les trois hommes travaillent dans un silence tendu. Keller sélectionne les fils, ne quittant pratiquement pas le téléphone qui assure la liaison avec les vérificateurs, annonçant tranquillement les références du circuit à suspendre le temps de l'intervention. Guillou et Matheron, les mâchoires serrées, s'activent, mesurant leurs gestes rapides. Ils coupent, décapent, épissurent, soudent, les mains plongées dans l'inextricable amas de conducteurs, s'arrêtant un bref instant pour essuyer la sueur, due à l'effort et à la l'émotion, qui perle à leur front. Sur la chaussée, Combaux feint de s'affairer à quelque tâche urgente, veillant à ce que les lueurs qui filtrent de la tente mal jointe n'alertent pas les servants d'une batterie de D.C.A. de la Wehrmacht située à moins de 300 mètres en amont. De temps en temps, une estafette motocycliste allemande passe, contournant la barrière mobile du chantier, jetant un regard distrait sur les fouilles. Dans la tranchée, autour du câble, on s'affaire toujours sur le même rythme. Soudain, désastre ! une manœuvre un peu trop rapide entraîne une forte variation de la constante électrique de l'isolement. Au centre de Paris-Saint-Amand, Lobreau, la gorge sèche, voit l'aiguille de l'appareil de mesure battre la chamade. Un bref coup d'œil sur le côté lui montre les deux Allemands de service avachis sur leurs chaises, les paupières lourdes, aux prises avec le traditionnel coup de barre de l'après-minuit. Ils n'ont rien remarqué ; les minutes passent angoissantes pour le vérificateur

qui devrait réagir, mais que sa complicité avec l'équipe maintient cloué sur son siège, le regard fixé sur le cadran témoin. Pourtant petit à petit, l'aiguille revient vers la zone de sécurité. Là-bas, sous la tente, Keller et Guillou se démènent pour rétablir l'isolement. Un quart d'heure encore, et Lobreau, avec le soulagement qu'on imagine, voit la tension revenir à son niveau habituel.

Trois heures du matin. Cela fait maintenant six heures que les trois postiers s'acharnent sur les fils ; cinquante-cinq grands circuits sont déjà dérivés, mais Keller et ses deux camarades poursuivent leur travail. À La Ferté-sous-Jouarre, au poste de répéteur, Fugier, les mains rendues moites par l'énervement, affecte le plus grand calme en déconnectant puis replaçant ses lignes sous le regard endormi de ses surveillants. Imperturbable dans la fosse, Keller continue de donner ses directives tout en refixant les isolants, cependant que Guillou et Matheron, tantôt accroupis, tantôt à genoux, les reins brûlants, endoloris par l'effort constant de recherche d'une meilleure position, maîtrisent leurs gestes, un peu plus gourds maintenant que la fatigue se fait sentir. Au-dessus d'eux, sur la route, Combaux, rongé par l'anxiété, sent les minutes devenir de plus en plus longues au fur et à mesure que le temps passe. En cette nuit froide d'avril, silencieuse, et lugubre sous la pâle clarté des candélabres qui diffusent une faible lumière bleutée, lui seul a tout loisir de laisser ses pensées s'égarer dans l'évocation du risque-tout en écoutant les clochers de Noisy et de Neuilly de chaque côté de la Marne se renvoyer les heures si lentes à s'écouler. Ses trois compagnons, eux, tendus vers le but à atteindre, absorbés par leur difficile travail, ne connaissent pas en ce moment, et c'est heureux pour la réussite de l'opération, ce dangereux vagabondage de l'esprit.

Quatre heures vingt. Robert Keller replie le schéma qui lui a permis de sélectionner les circuits. Guillou et Matheron fignolent la dernière épissure. Le câble est regarni, puis calé soigneusement au niveau du piquage.

Quatre heures quarante. La dérivation est terminée. Les trois hommes remontent. Rapidement la fouille est comblée. L'aube se lève lorsque les dernières pelletées de terre égalisent le terrain.

Abrutis de fatigue dans la camionnette qui les ramène à Paris, les auteurs de cette extraordinaire opération demeurent silencieux. Réalisent-ils qu'ils viennent d'effectuer un véritable exploit ? Soixante-dix grands circuits ont été dérivés, parmi lesquels ceux qui assurent les liaisons de la Kriegsmarine, de la Luftwaffe, de la Wehrmacht, et de la Gestapo, entre Paris et Berlin ! Jamais aucun service d'espionnage n'avait rêvé pouvoir bénéficier d'une telle source !

La dérivation étant effectuée, c'est maintenant à M. Sueur qu'il appartient de mettre la table d'écoute en service. Prévenu par le capitaine Combaux de la réussite de l'opération, il arrive aux premières heures de la matinée du 19 avril au pavillon de Noisy, accompagné d'un fidèle ami, spécialiste des Transmissions de l'État, M. Deguingamp auquel il accorde toute confiance. Immédiatement, ils se mettent en devoir de procéder aux raccordements. Laissés en attente, les fils qui s'épanouissent sur des appareils appelés « têtes de câble » vont être reliés aux amplificateurs, puis les postes d'écoute sont à leur tour branchés. Lorsque Édouard Jung, informé par Combaux, se présente, tout est pratiquement prêt à fonctionner. Avec une infinie prudence, les deux techniciens effectuent les premiers essais. On a choisi le moment où Lobreau et Fugier auront repris leur service afin qu'ils puissent veiller, chacun dans leur centre, sur les mesureurs de tension. Mais tout va bien, le travail accompli par Keller, Guillou, et Matheron ne recèle aucune imperfection. Jung peut commencer ses longues factions ; la Source K est opérationnelle !

C'est le 19 avril 1942 dans la soirée, que l'opérateur du S.R. enregistre les premières conversations; mais c'est vraiment à partir du 20 que l'écoute porte ses fruits. En cette seule journée, Édouard Jung intercepte plus de 60 communications. L'importance du trafic l'oblige alors à sélectionner parmi ce flot continu les circuits présentant le plus grand intérêt, et il se contente de relever les liaisons des armes — marine- aviation-armée de terre — avec le Haut Commandement de Berlin. Devant un pareil afflux, le capitaine Combaux réclame un second opérateur, et le S.R. choisit parmi les agents en stage M. Rocard,

jeune licencié d'allemand, ancien lecteur dans une université d'outre-Rhin. L'arrivée de ce deuxième spécialiste double bien sûr le nombre d'informations. Les deux hommes abattent une besogne écrasante. Aux heures d'écoute s'ajoute le temps passé à transcrire à l'encre sympathique, sur des lettres, rapports, ou contrats, les renseignements les plus importants ; ceux présentant un moindre intérêt sont acheminés irrégulièrement par porteur. À Combaux revient le soin d'organiser la transmission au poste P 2 du S.R. de toutes ces informations. Il parvient à assurer cette liaison et le passage de la ligne de démarcation grâce à un ambulant de la S.N.C.F. ; par la suite, il emploiera également un garçon des wagons-lits, puis un mécanicien de locomotive. Arrivés dans le service du capitaine Simoneau, les renseignements fournis par la Source K sont triés soigneusement. Ceux qui peuvent intéresser le gouvernement de Vichy et influencer sa politique vis-à-vis du Reich sont remis au colonel Rivet qui, après les avoir analysés minutieusement, décide ou non de leur envoi au général Revers, chef d'État-major de Darlan. Mais les plus vitaux, ceux qui fournissent des indications précieuses sur les projets allemands, ainsi que ceux qui font état de la situation militaire et de l'évolution de la stratégie du Haut Commandement, passent directement du S.R. à 1'I.S. par les liaisons « Olga », ou par les liaisons radio de l'équipe du commandant Bertrand, ou encore par les postes de Berne et de Lisbonne[74]. Afin que leur origine ne puisse être décelée, les rapports émanant de la Source K subissent par le poste P 2 un démarquage avant leur transmission à l'échelon supérieur. Cette précaution interdit une remontée à contresens de la filière, et elle est d'autant plus facile à assurer qu'il ne peut y avoir de retours par cette voie-là. Pour compléter la sécurité, un cloisonnement rigoureux verrouille les maillons de la chaîne par groupes de deux à quatre unités. Ainsi, les opérateurs n'ont qu'un seul interlocuteur Combaux, mais les techniciens des P.T.T., mis à part Sueur et Keller, ne le connaissent pas. Parallèlement, les agents de liaison ignorent tout des postiers. En fait, le pivot de l'affaire est le capitaine Combaux ; en cas d'intervention ennemie, c'est donc lui qu'il convient de protéger. Robert Keller l'a parfaitement compris, et il s'y emploiera le moment venu.

Devant les résultats inespérés des écoutes sur le câble Paris-Metz, Sueur, Combaux, et Keller envisagent de réaliser la même opération sur le Paris-Strasbourg. Une étude fouillée des grands circuits a montré que les liaisons téléphoniques allemandes empruntent également ce canal. En juillet 1942, Robert Keller présente à ses deux amis le schéma de la dérivation à entreprendre. Entre-temps, un troisième opérateur formé par le S.R. a été mis à la disposition de la Source K par le poste P 2. Il s'agit d'un jeune Alsacien : Prosper Riss, qui reçoit également une couverture d'inspecteur d'assurances de « La Nationale ». Combaux le charge de rechercher un pavillon libre sur le parcours de la ligne souterraine. Il en trouve bientôt un à Livry-Gargan dans lequel il s'installe aussitôt. Sur la demande de Sueur, M. Lebedinski commande les pièces détachées nécessaires au montage de nouveaux amplificateurs, tandis que Pierre Guillou, promu depuis peu au grade de chef d'équipe, délimite sur place le tracé de la tranchée de jonction.

Fin août, l'aménagement du local est terminé ; il ne reste plus qu'à mettre en place les amplificateurs et à effectuer la dérivation.

Cependant à Noisy-le-Grand, le climat se détériore. Les Allemands ont décidé d'implanter une forte unité à l'Est de Paris et, dans cette perspective, un détachement précurseur sillonne la bourgade afin de rechercher de nouveaux cantonnements. Une vaste opération de réquisition de locaux, de maisons, de chambres commence, au grand dam des Noiséens furieux. Dans le quartier où se trouve situé le pavillon des écoutes, la grogne s'affirme particulièrement, et plusieurs réclamations parviennent à la Mairie pour signaler à la commission de recensement qu'au lieu de « vouloir imposer à de braves Français l'hébergement d'officiers allemands, elle ferait mieux de s'intéresser aux individus suspects, vivant d'on ne sait quoi, qui hantent un pavillon même pas trop meublé ».

[74] Notons qu'il existait, entre autres, une liaison du S.R. Lyon-Londres qui était assurée par le relais d'Annemasse de M. Francillon, qui, arrêté un peu plus tard, sera fusillé par les Allemands.

À ces protestations s'ajoutent des commérages de quartier qui évoquent l'activité d'espions... allemands ! Nous sommes à la mi- septembre, et les ragots prolifèrent de plus en plus.

Prévenu par Édouard Jung, le capitaine Combaux, s'inspirant de la règle des services secrets : « la sécurité prime tout », décide alors le repli immédiat de la station clandestine.

Dans la nuit du 16 au 17 septembre, Robert Keller, Pierre Guillou, et Laurent Matheron, démontent toute l'installation, colmatent les têtes de câble, et font disparaître toute trace de la dérivation. Le lendemain, M. Sueur et Deguingamp viennent récupérer les amplificateurs qu'ils transportent à Livry-Gargan. Le 18 au soir, plus rien ne subsiste de cinq mois d'écoutes permanentes. Le petit pavillon de Noisy-le-Grand retourne à l'anonymat, prêt à accueillir les indésirables locataires dont ses murs ont pourtant enregistré les conversations plus secrètes de leurs dirigeants.

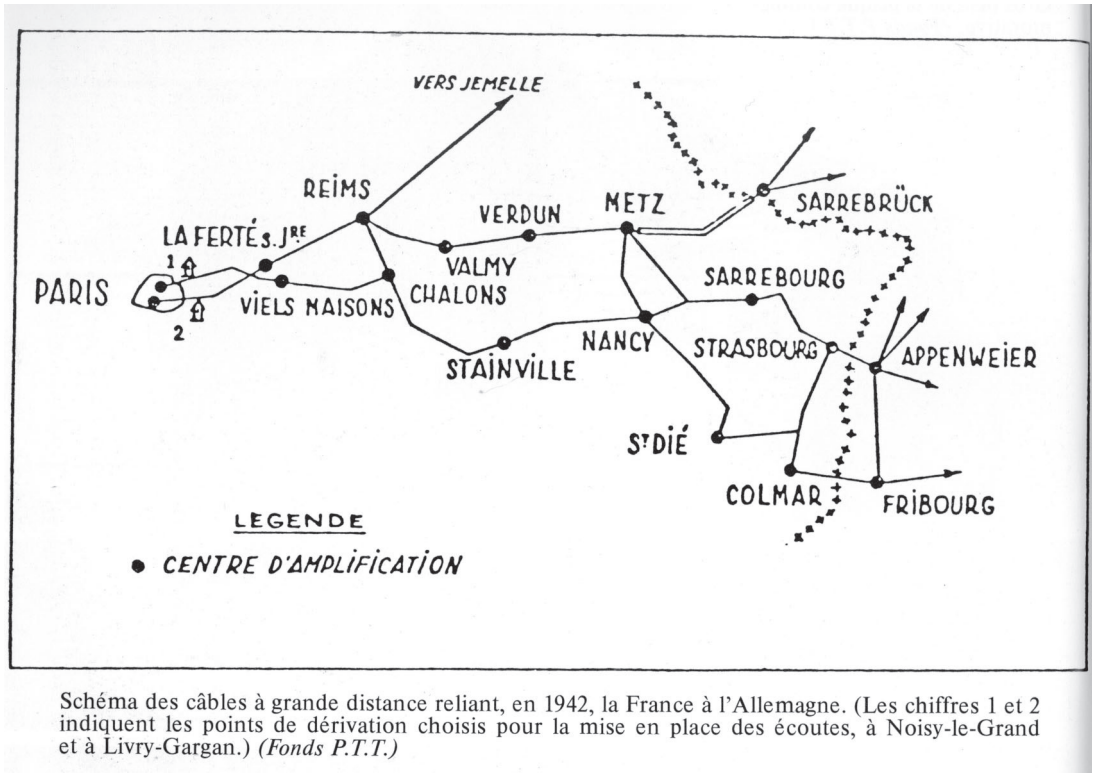


Schéma des câbles à grande distance reliant, en 1942, la France à l'Allemagne. (Les chiffres 1 et 2 indiquent les points de dérivation choisis pour la mise en place des écoutes, à Noisy-le-Grand et à Livry-Gargan.) *(Fonds P.T.T.)*

L'écoute en temps réel d'une ligne par un micro sucre :

Cette solution consiste à écouter et enregistrer les appels à distance en temps réel en intervenant qu'une seule fois pour toute sur la ligne. À un endroit de la liaison de l'abonné on branche un sucre émetteur, en faisant une épissure sur le câble, dans le boîtier de répartition, la prise de bureau ou le téléphone lui-même si on y a accès. Un professionnel évitera les deux dernières possibilités. Tout simplement parce que si la personne écoutée utilise un tuner FM, un scanner, des interférences pourraient trahir la présence du sucre. Si l'émetteur est raccordé à l'extérieur du bureau, de l'immeuble, il ne pourra pas être détecté. L'inconvénient majeur de ce type de système, c'est qu'en plus de l'espion, n'importe qui peut écouter la conversation jusqu'à 200 voire 500 m à condition que son récepteur radio soit réglé sur la bonne fréquence. L'espion disposant d'un récepteur radio intégrant un magnétophone peut enregistrer la conversation directement à distance sans craindre de se faire repérer. Si le subterfuge est découvert, il n'y a que le sucre qui sera localisé et détruit. Il existe un autre problème, ce petit gadget consomme du courant ne serait-ce que pour son fonctionnement, il pourra donc être éventuellement repéré par un spécialiste doté d'un analyseur de ligne ou d'un détecteur de microémetteur. La haute fréquence peut suivre le câble sur une certaine distance, assez courte, mais qui peut-être suffisante.

On trouve en vente libre sur Internet ce type de matériel. Une Société propose, par exemple, « Pack émetteur de conversations téléphoniques + récepteur. Ce pack complet prêt à l'emploi va vous permettre de mettre en surveillance une ligne téléphonique de la façon la plus simple possible. Branchez le MP114 dans la ligne analogique que vous voulez superviser puis à l'aide du récepteur, écoutez dans un rayon de plusieurs dizaines de mètres les conversations émises et reçues sur cette ligne. Idéal pour contrôler une ligne téléphonique lors d'audit ou de formation de personnel (standardiste, etc. ...). « Transportez » par exemple vos conversations téléphoniques afin de pouvoir permettre à des collaborateurs de partager vos conversations lorsque vous le désirez. Par ailleurs, si vous ajoutez notre VR2 à ce pack, vous pouvez aussi enregistrer les conversations en toute simplicité même en votre absence et ainsi les analyser ultérieurement ! » La prise se présente sous la forme suivante : (Fig. mp114.jpg).

Raccordement sur une ligne analogique :

C'est la méthode la plus facile, mais aussi la moins discrète qui finira par l'arrestation du fraudeur s'il l'utilise en plus pour téléphoner gratuitement. Par contre dans le cas d'une écoute légale ou illégale cela peut durer plus longtemps. Elle est simple et peut être réalisée à peu de frais sur les lignes analogiques. Elle consiste à installer une bretelle en Y sur une ligne déjà existante. Il est en effet possible de se connecter sur tous les points d'un cheminement, de la sortie du central téléphonique au point final d'implantation du poste. Généralement, cette connexion est réalisée au niveau d'un sous-répartiteur ou d'un boîtier de répartition de quartier. Cette solution provoque généralement un défaut d'impédance et un affaiblissement sur la ligne. Un spécialiste équipé d'un matériel comme un analyseur de ligne analogique, peut détecter une anomalie.

La police, la gendarmerie, la DST découvrent dans les égouts, des épissures dans les câbles sur lesquels des bretelles sont réalisées. Les manchons raccordant deux câbles sont ouverts, des bretelles, des *straps*[75] mettant deux lignes en parallèle, des magnétophones ou émetteurs miniatures sont retrouvés à l'intérieur. Dans les gaines techniques ou les cabines de brassage, on retrouve le même type de piratage. Il ne coûte que très peu. Le piratage s'effectue le plus souvent en faisant des épissures sur les câbles, cette solution est en effet plus discrète, qu'un raccordement au niveau du répartiteur général, ou sur la tête PTT, puisque les techniciens de France Télécom y interviennent à chaque fois qu'ils ont une ligne à rajouter. Sur cette partie de l'installation, le PDG d'une société ne peut pas faire grand-chose. Il n'y a que la police qui peut intervenir sur dépôt d'une plainte.

Il existe un autre moyen d'espionnage peu connu, qui peut être utilisé sur les postes analogiques. Il peut permettre d'écouter en plus ce qui se passe dans un local, même si le téléphone est raccroché. La micro-pastille du combiné continue à capter des sons en permanence. Cette pastille va donc générer des impulsions. Les électroniciens qui connaissent l'effet piézo-électrique du quartz, comprendront où je veux en venir. Avec un équipement sensible, il est parfaitement possible de faire de l'écoute avec certains postes. Ce type de technique est plutôt utilisé par les laboratoires des services secrets étrangers très en pointe dans le développement des nouvelles technologies d'espionnage. Ce moyen concerne plutôt les sites ou personnes ultra-sensibles.

Un fait historique d'écoute microphonique

Pour diriger le C.E[76]. en Afrique du Nord, le S.R. a désigné le lieutenant-colonel Chrétien, qui, après un ultime stage à la villa « Eole[77] », arrive à Alger en mars 1941. En Algérie, au Maroc, et en Tunisie,

[75] Cavalier utilisé en électronique.

[76] Contre Espionnage

[77] La villa Eole à Marseille, sur la promenade de la plage, était le « siège social » du C.E. français, émanant du « 5e Bureau ». La couverture était assurée par la Direction du Génie Rural au Ministère de l'Agriculture.

les Allemands et les Italiens ont envoyé des commissions dites « d'armistice » dont la mission officielle est de vérifier que les clauses du cessez-le- feu sont bien appliquées par les autorités civiles et militaires dépendant du gouvernement de Vichy. En réalité, ces commissions sont formées d'une majorité d'agents de l'Abwehr chargés d'organiser un réseau de renseignements et de recueillir des informations sur les agissements anglais et américains dans le Maghreb.

À Alger, le pouvoir officiel est détenu par le général Weygand qui, après un bref passage au Ministère de la Défense à Vichy, a été désigné comme Délégué général du gouvernement pour l'Afrique Française, fonction et titre créés spécialement pour lui. Investi de pouvoirs jamais atteints par un officier supérieur, son autorité s'exerce, tant sur le plan militaire que civil, sur toute l'Afrique du Nord et sur l'Afrique-Occidentale française. Les gouverneurs Noguès au Maroc, Esteva en Tunisie, Abrial en Algérie et Boisson en A.O.F. se trouvent placés sous ses ordres et il va veiller à ce que soient strictement appliquées toutes les décisions prises à Vichy. Dans certains cas, notamment dans la mise en place des mesures édictées contre les juifs, il ira même au-delà des décrets promulgués par le gouvernement Pétain. Adepte farouche de la « Révolution nationale », il mène la lutte contre tous ceux qu'il nomme « les mauvais Français », anciens partisans du Front Populaire, francs-maçons, communistes, gaullistes, républicains convaincus, et il accorde tout son soutien à la « Légion française des Combattants », aux sections de « l'Ordre légionnaire », aux militants de Bucart, de Déat, et de Doriot, bref à tous ceux qui dansent sur le cadavre de la République. Son comportement en Afrique du Nord reflète donc parfaitement ses convictions. Weygand pense sincèrement qu'il faut à la France un ordre nouveau, duquel seraient bannies les institutions et les idées républicaines. Hostile à l'Angleterre, surtout depuis Mers el-Kébir, haineux vis- à-vis de De Gaulle qu'il qualifie de déserteur, méfiant à l'égard des Américains auxquels il reproche de n'être pas venus au secours de l'armée française, violemment anticommuniste, il ne s'en considère pas moins comme un ennemi irréductible de l'Allemagne. C'est en jouant sur cette dernière carte que le lieutenant-colonel Chrétien, et Paul Paillole lui-même, obtiendront le feu vert pour leur service.

Déjà à Vichy, alors qu'il détenait le ministère de la Défense, Weygand avait donné son accord au colonel Rivet pour la création d'un S.R. et d'un C.E. clandestins, sous le couvert d'un service des Menées antinationales, chargé de « suivre » les agissements allemands et italiens, et ce, malgré l'opposition de la clique Laval-Marquet-Darlan. À cet égard, il avait fait connaître son opinion en déclarant à son interlocuteur : « la guerre continue, l'armistice n'est qu'une suspension d'armes ».

C'est en s'appuyant sur cette position nuancée que les T.R[78]. parviendront à leurs fins, car il faut bien admettre que sans cet appui, Paillote et ses camarades ne seraient jamais parvenus, malgré toute leur bonne volonté, à organiser et à structurer aussi rapidement leurs antennes clandestines.

Dès son implantation à Alger, le T.R. 119 s'est vite rendu compte du danger représenté par les commissions d'armistice italo-allemandes. Véritable vivier du renseignement, elles informent régulièrement l'O.V.R.A.[79] et l'Abwehr[80] sur le climat politique, ainsi que sur l'activité des milieux musulmans indépendantistes qu'elles entretiennent sournoisement. Mais elles s'acharnent surtout à tisser, avec leurs homologues du Maroc et de la Tunisie, un filet d'espionnage sur toute l'Afrique du Nord ; filet destiné à recueillir toutes indications utiles à leurs pays, et à enserrer dans ses mailles les agents des autres nations directement, ou indirectement, mêlées au conflit.

Le lieutenant-colonel Chrétien, dès son arrivée à Alger, s'est attaché à rechercher les moyens les plus efficaces pour contrer l'action de ces commissions. Installées dans plusieurs hôtels de la ville, l'*hôtel d'Angleterre, l'hôtel Aletti, l'hôtel Albert*, où elles ont regroupé leurs bureaux et appartements privés, elles

[78] Entreprise Générale de Travaux Ruraux, nom de couverture du service de contre-espionnage.

[79] OVRA (*Organizzazione di Vigilanza Repressione dell'Antifascismo*) ; en français : Organisation pour la vigilance contre l'antifascisme, était la police secrète du régime fasciste italien. Elle fut créée en 1927.

[80] Abwehr, mot allemand signifiant « défense », est créée en 1925. Elle est le service de renseignements de l'état-major allemand de 1925 à 1944.

travaillent officiellement avec leurs ambassades ou consulats respectifs. Évidemment, le T.R. est parvenu à s'assurer les services de quelques employés qui lui apportent de temps en temps des renseignements non négligeables, mais c'est loin d'être suffisant pour assurer une surveillance efficace. Chrétien et son adjoint, le commandant Le Capelain, voudraient percer à jour le jeu ennemi afin d'en prévenir les retombées. Naturellement, des tables d'écoutes ont été mises en place, mais elles ne s'affirment guère rentables, car les adversaires ne sont pas des novices. Ils savent très bien que leurs conversations téléphoniques doivent être interceptées. La preuve : un officier allemand téléphonant de l'*hôtel Aletti* à l'un de ses collègues de Casablanca sera entendu lui disant : « Je vous en prie, mon cher, parlez plus lentement afin que ces messieurs aient le temps de prendre en note notre conversation ! » Ce n'est donc pas par ce canal-là qu'il faut s'attendre à des révélations. L'idéal serait de pouvoir écouter les propos qui s'échangent dans l'intimité des pièces de travail ou d'habitation, lorsqu'Allemands et Italiens se croient entre eux, lorsqu'ils reçoivent leurs informateurs ou qu'ils évoquent leur activité. Il faudrait avoir une oreille dans chaque chambre, dans chaque bureau, mais comment ?

C'est alors que le commandant Le Capelain parla d'un réseau d'écoutes microphoniques permanentes !

C'est en juin 1941 que le Commandant Le Capelain songe pour la première fois à réaliser un dispositif qui permettrait d'enregistrer les conversations ennemies sur les lieux mêmes où elles doivent être, par définition, les plus confidentielles. Sans avoir des idées très précises sur les moyens, il pense que le réseau téléphonique peut offrir un champ d'investigations intéressant, et il sollicite le concours de son collègue, le commandant Guérin du bureau des Transmissions. Du point de vue technique, Guérin est évidemment bien placé pour juger des possibilités du projet, mais il ne dispose pas des éléments nécessaires à sa réalisation, pas plus qu'il ne possède de locaux ou de matériel pour en effectuer l'étude. Mais, et cela va s'affirmer d'un grand intérêt pour le T.R. 119, il a noué d'excellentes relations avec le chef du service central des P.T.T. en Algérie : M. Escande, haut fonctionnaire intègre et courageux dont le patriotisme ne fait aucun doute.

Guérin lui expose sans détour l'idée de Le Capelain, et les deux hommes réfléchissent ensemble à l'aspect pratique de ce plan. Ayant la haute main sur la totalité des systèmes de communication existant alors en Algérie, Escande se trouve remarquablement placé pour entreprendre, ou couvrir, toute action requérant les moyens techniques de son administration, mais il ne peut rien faire sans le concours de spécialistes éprouvés et discrets. Le projet qui lui est soumis demande en effet une étude très approfondie, et nécessite des recherches originales que seuls des ingénieurs des P.T.T. peuvent mener. Or il se trouve que trois de ces spécialistes ont été détachés par l'administration auprès du bureau des transmissions, et qu'ils travaillent donc dans cet ensemble technique qu'on appelle : le *Central protégé*.

Afin de rendre plus compréhensible le récit qui va suivre, il est bon d'en « planter le décor ».

Accrochée au flanc des collines du Sahel, au débouché de la plaine de la Mitidja, la ville d'Alger est construite en amphithéâtre. Ses immeubles et ses villas s'étagent sur les hauteurs qui dominent la baie jusqu'aux plateaux environnants. Dans le centre, la dénivellation contraint les ruelles et les voies à suivre une pente assez sensible ; c'est ainsi que la place du Forum, où se dresse l'imposant bâtiment du Gouvernement Général, s'étale à près de quarante mètres au-dessus du niveau de la rue d'Isly. La place Bugeaud, lieu de l'implantation des bureaux de l'État Major du 19 Corps, se situe à l'intersection des rues d'Isly et Généraux Morns, soit en contrebas d'une vingtaine de mètres par rapport à la rue Berthezène qui ceinture les immeubles de la Résidence. Accolé à l'un de ceux-ci un local de service communique, en fonction de cette dénivellation, par un escalier en puits, avec un tunnel qui débouche à l'intérieur même de la cour desservant les garages de l'État-Major. Dans ce souterrain, à l'abri de toute incursion et de tout bombardement, les transmissions ont établi leur central téléphonique, d'où son nom de « *Central protégé* ». On ne peut donc y accéder que, soit par l'enceinte militaire, soit par le puits partant des communs de la Résidence; deux lieux étroitement surveillés.

Les trois agents des P.T.T. qui assurent le bon fonctionnement de ce central et représentent leur administration dans la liaison avec l'équipement militaire sont, à cette époque M. La Maïda ingénieur, M. Pettenati ingénieur des travaux, et M. Rebaudingo contrôleur I.E.M. En raison de leur fonction et de leur mission, ce sont évidemment des hommes qui présentent toutes garanties de discrétion et de patriotisme ; la sélection de la sécurité des armées ne souffrant aucun doute à ce sujet. C'est donc tout naturellement vers eux que M. Escande se tourne pour envisager la réalisation du projet du commandant Le Capelain et, comme il le souhaitait, il recueille aussitôt leur adhésion. Quelques notes de service anodines leur laissent d'ailleurs bientôt les mains libres pour s'assurer du contrôle total des lignes qu'il s'agit de « métamorphoser ».

En 1941, l'espionnage microphonique fait un peu figure de science-fiction. Certes, les Américains sont déjà parvenus à capter des conversations en utilisant un système de micros clandestins reliés à un appareillage d'écoutes, mais au prix d'une installation réalisée par fils dissimulés. En Europe, et à fortiori, en Afrique du Nord, cette technique n'apparaît que futuriste. On ignore encore tout des moyens d'écoute qui se développeront d'une façon fulgurante après la guerre avec la transistorisation et la miniaturisation, puis grâce aux progrès importants de l'électronique. Seuls, quelques techniciens des communications et transmissions savent que l'on peut, en utilisant la liaison téléphonique, à l'aide de quelques astuces professionnelles, espionner les bruits d'une pièce, mais l'audibilité en est toujours médiocre à cause du phénomène de résonance.

C'est malgré tout en partant de ce procédé que l'ingénieur La Maïda va établir un schéma parfait, avec le concours de ses collègues Henri Pettenati et Louis Rebaudingo. Le plan général étant défini, chacun de ces hommes se met au travail pour monter une maquette d'essai, suivant sa spécialisation. Le principe retenu paraît simple : tout poste téléphonique comporte un microphone normalement alimenté par une batterie située dans le central auquel il est rattaché. Le courant ne parvient dans ce microphone que lorsque l'appareil est décroché, c'est-à-dire en position de conversation. Le fait de raccrocher le combiné provoque le fonctionnement d'un interrupteur dont le rôle est de couper le courant ; le microphone n'étant plus alimenté, il devient sans effet. Or, si l'on établit une jonction métallique entre les deux lames de l'interrupteur, celui-ci se trouve neutralisé, et le courant continue d'arriver jusqu'au micro, même si le poste est en position « raccroché ». Dans ces conditions, le microphone reste opérationnel en permanence, et il transmet tous les bruits qui s'échangent dans la pièce où se trouve l'appareil. On voudra bien nous pardonner d'aborder ces problèmes techniques, mais ils sont nécessaires pour la compréhension des faits.

Cependant, une telle modification du circuit normal entraîne une répercussion sur le fonctionnement du central. En effet, un poste ainsi « trafiqué » provoque irrémédiablement un incident de ligne que les téléphonistes désignent sous le nom de « faux appel », et il risque fort d'éveiller l'attention d'un usager un peu méfiant, surpris par les interférences qui peuvent survenir en cours d'utilisation. Ce premier problème va pourtant être solutionné par l'ingénieur La Maida qui met au point un relais doté d'une bobine à 3 enroulements à flux différentiels, et conçoit une platine de retransmission qui rétablit le circuit initial malgré les modifications apportées au poste d'abonné. Un premier essai effectué au petit laboratoire de la direction des L.S.G.D.[81] montre que ce système s'avère satisfaisant dès lors qu'un bâti métallique est adapté pour recevoir la platine. Puis, Louis Rebaudingo, au câblage, équipe un montage adéquat à cette nouvelle fonction, tandis qu'Henri Pettenati étudie un modèle d'amplificateur perfectionné. De la régularité et de la précision de cet appareil, dépend en effet la possibilité d'une écoute normale.

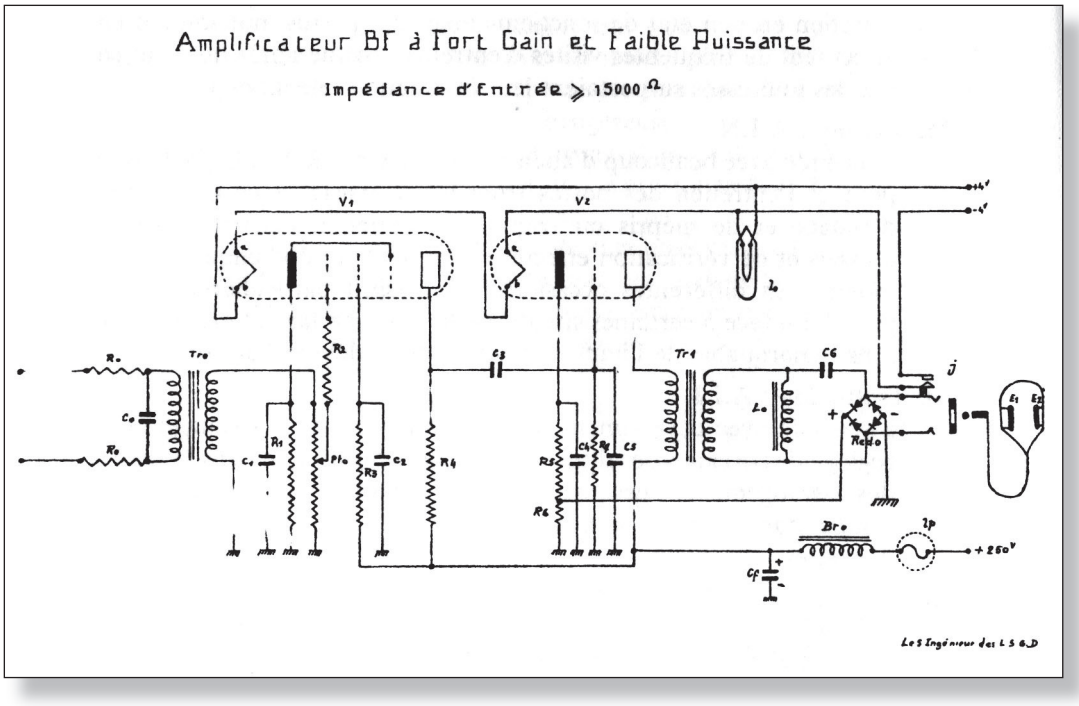
Une maquette originale essayée au répartiteur du central d'Isly montre que le bruit de fond des lignes en câbles urbains devient rapidement gênant, et qu'il faut, par conséquent, utiliser un courant micro-

[81] Lignes souterraines à grande distance.

phonique aussi fort que possible. L'ennui d'un tel courant, c'est qu'il manque de « discrétion » et risque d'être facilement décelable par un appareil de mesure de sensibilité courante, mais tous les essais effectués avec un courant plus faible aboutissent à un résultat négatif pour l'intelligibilité de l'écoute. Il faut donc en prendre le risque. Pendant ce temps, le commandant Le Capelain est parvenu, grâce à M. Escande, à se procurer une « couverture » civile qui lui permet de se trouver au cœur de l'action ; sa nomination au poste d'Inspecteur des P.T.T. sous le nom de Paul Edmond l'autorise à se déplacer comme il l'entend dans les locaux administratifs. Son premier souci, dans cette nouvelle fonction, est de recenser soigneusement le nombre d'appareils devant faire l'objet d'une modification. C'est ainsi qu'il détermine qu'il y aura lieu de truquer 29 postes d'abonnés répartis entre l'*hôtel d'Angleterre*, l'*hôtel Albert-Ier*, l'*hôtel Aletti*, et la résidence de l'amiral Saiza à El-Biar.

À la mi-septembre 1941, la maquette définitive de l'ensemble est réalisée. Louis Rebaudingo a parfaitement maîtrisé le problème d'incorporation des platines de retransmissions montées sur des bâtis métalliques, et il a installé des machines d'appel spéciales. De son côté, Henri Pettenati, après bien des tâtonnements, est parvenu à mettre au point un amplificateur spécifique à deux étages, d'une impédance d'entrée supérieure à 15 000 ohms, comportant un dispositif antichocs placé aux bornes du casque de l'opérateur, qui permet d'éviter l'écho résonnant des chocs mécaniques auxquels pourrait être soumis le poste, et risquant de gêner la finesse de l'ouïe. De plus, un filtre à variations sélectionne les fréquences de voix pour rendre encore plus compréhensibles les conversations en écoute.

L'ensemble paraît au point et donne toute satisfaction aux essais. On passe alors immédiatement au stade de la réalisation. Deux collaborateurs de Louis Rebaudingo, MM. Mergny et Trottignon, mis



dans le secret de l'opération, acceptent de prêter leur concours, et il va s'affirmer essentiel. C'est en effet Mergny qui se charge de procéder à la pose chez les intéressés des appareils truqués ou d'en effectuer le changement sous un prétexte quelconque. Trotignon lui, agent des installations intérieures, assure le montage en série des platines de relais des retransmetteurs sur lignes automatiques et vérifie leur réglage. Un autre technicien du service, M. Legée, recruté par l'ingénieur La Maïda, construit, suivant les plans de ce dernier, le meuble d'écoute comportant dix positions plus une position de dirigeur. Dans le même temps, Henri Pettenati surveille attentivement la fabrication des sept amplificateurs imaginés par lui ; le personnel qui les réalise ignore leur destination. Quelques jours plus tard, par fragments, les tables et le

meuble d'écoute sont transportés dans le tunnel du central protégé. L'ensemble est monté de telle façon que les tables peuvent être, à la moindre alerte, transformées en un système d'écoutes téléphoniques normal. Pièce par pièce, tous les éléments arrivent ; les connexions sont faites et les branchements préparés. M. La Maïda pousse même le soin jusqu'à doter cette implantation clandestine d'un confort qui sera fort apprécié des opérateurs. Agents du T.R., ceux-ci sont sélectionnés par le commandant Le Capelain, alias Paul Edmond, qui les instruit de leur fonction. Se relayant par équipes de trois, ils doivent assurer leur travail vingt-quatre heures sur vingt-quatre. Au début du mois d'octobre 1941, Mergny et Rebaudingo commencent leur prospection. Des interférences ont été créées astucieusement sur les lignes à surveiller, et les abonnés allemands et italiens ne tardent pas à formuler des réclamations. C'est le moment qu'attendent les deux hommes pour agir. Se rendant sur place, ils s'empressent de changer là un appareil soi-disant défectueux pour le remplacer par un autre préalablement « équipé ». Ailleurs, ils démontent les postes et remplacent subrepticement la capsule microphonique par une autre. Sur la recommandation de Pettenati, soucieux d'obtenir les meilleures conditions d'audition pour ses amplis, ils agrandissent discrètement les trous percés dans les coiffes d'ébonite qui protègent le microphone. Pendant ce temps, au central protégé, on met la dernière main à l'équipement de l'appareillage. MM. Escande et La Maida assistent aux ultimes essais, aux côtés du commandant Le Capelain et de ses opérateurs. Le 25 octobre, tout est prêt ; le plan « Écoutes microphoniques d'Alger » devient une réalité. Pour la première fois, dans l'histoire des services du Contre-Espionnage français, un réseau entier d'écoutes microphoniques fonctionne !

Dès les premières auditions, le commandant Le Capelain se rend compte qu'il dispose d'une source d'informations secrètes de première grandeur. Après l'émotion du début, liée aux craintes de voir le système rapidement découvert par les « abonnés », le ton des conversations interceptées montre à l'évidence que ni les Allemands ni les Italiens ne soupçonnent une indiscrétion. Leurs propos reflètent une confiance totale dans l'inviolabilité des locaux qu'ils occupent. Sur le plan technique, les opérateurs souffrent de la volubilité des officiers de Mussolini dont les bavardages ininterrompus et l'élocution particulièrement rapide perturbent l'intelligibilité de l'écoute. Averti, Henri Pettenati va d'ailleurs concevoir un filtre spécial gommant un peu l'acuité des sons[82] et « sélectionnant », grâce à des caractéristiques différentes, les amplificateurs recueillant les voix italiennes aux sonorités plus aiguës que celles des Allemands à fond guttural.

Chaque jour, et souvent deux fois dans la même journée, les informations captées sont triées, puis résumées en rapports condensés remis aux services du colonel Chrétien. Classés suivant leur origine et leur nature, ceux-ci sont ensuite répertoriés avant d'être acheminés vers leurs destinataires. Par ce canal clandestin, des renseignements d'importance vitale sur les agissements et les intentions des représentants de l'Axe parviennent aux Alliés, et, pour ce qui le concerne, à l'État-Major de l'Armée d'armistice. C'est ainsi que les visites de contrôles périodiques effectuées à l'improviste par les membres des commissions allemande et italienne dans les camps militaires seront toutes annoncées quelques heures, voire quelques jours, avant aux responsables d'unités ; ce qui leur permettra de dissimuler le matériel et l'armement dont les stocks sont supérieurs aux normes prévues.

À la mi-janvier 1942, les ingénieurs des P.T.T. ont terminé la première tranche du programme. 29 lignes sont sous contrôle-écoute :

[82] Les travaux des spécialistes ont mis en évidence, après la guerre, que l'être humain possédait une « oreille géographique ». On sait maintenant qu'une oreille française a une courbe de sélectivité qui s'étend de 500 à 2 000 périodes, alors que celle d'un Anglais va de 2000 à 6000 périodes. Ni l'un ni l'autre ne perçoivent les sons de la même manière qu'un Japonais ou un Africain. On a créé d'ailleurs depuis une oreille électronique en s'inspirant de cette découverte. C'est ainsi que les travaux du Docteur Tomatis ont abouti à la réalisation d'appareils auditifs permettant à certaines formes de surdité de connaître une quasi-guérison.

21 lignes Mogador aboutissant à l'hôtel d'Angleterre

5 lignes Mogador aboutissant à l'hôtel Albert

3 lignes Mogador aboutissant à la résidence privée de l'Amiral Saiza. Le système donnant entière satisfaction, le commandant Le Capelain demande alors qu'il soit étendu à l'*hôtel Aletti* et au Consulat d'Allemagne. Justement, les Allemands réclament de nouvelles lignes pour leurs bureaux consulaires en cours de réaménagements. Louis Rebaudingo, qui s'est rendu sur place pour reconnaître l'implantation des postes, gagne un peu de temps, malgré les récriminations de ses interlocuteurs, afin de laisser la possibilité à ses monteurs et câbleurs d' « équiper » les bâtis. Le 8 février 1942, accompagné de son fidèle Mergny, il procède à une première installation chez le Secrétaire Général du Consulat. Cette ligne, portant le nº 324.16, est mise en service dès le lendemain. Le 18 février, soit neuf jours plus tard, une seconde ligne truquée : nº 331.51, posée dans le bureau même du consul, s'ajoute au faisceau des tables d'écoute. Deux jours après, M. Escande reçoit une demande pressante du Secrétariat consulaire qui exige l'installation d'un standard à plusieurs directions. Pris de court, le chef du service central des P.T.T. manœuvre habilement pour gagner quelques jours, le temps nécessaire à Louis Rebaudingo et Henri Pettenati pour fabriquer un nouveau matériel spécialement élaboré pour un standard. Une semaine ne s'est pas écoulée que les Allemands reviennent à la charge, déclarant avoir un besoin urgent de cet appareillage. Louis Rebaudingo répond qu'il attend l'arrivée d'un matériel convenable pour leur donner satisfaction. Pendant ce temps, une troisième ligne truquée, ayant le nº 333.65, est installée dans le bureau de l'Ambassadeur Pfeiffer, avec un renvoi dans sa chambre à coucher, à la tête de son lit. Là, on peut dire que les opérateurs vont capter bien des... conversations qui n'auront aucun caractère politique, même si elles sacrifient au confidentiel.

Ne pouvant différer plus longtemps, Mergny et Rebaudingo, pourvus d'un combiné multiple modifié par leurs soins, installent chez les secrétaires du Consulat un tableau administratif 1 + 4 dont les lignes viennent se joindre à celles du meuble-écoutes. Ainsi, presque toutes les pièces de l'immeuble passent sous le contrôle auditif des opérateurs du Commandant Le Capelain.

Ce délicat et discret travail, qui fut mené à bien par les agents des P.T.T., ne s'effectua pourtant pas sans problèmes, car le Consulat allemand se trouvait dans une zone différente du secteur Alger-Isly, et il fallut passer les lignes en coupure sur le répartiteur du Central protégé et les raccorder sur l'autocommutateur de ce secteur.

Sans doute jaloux des aménagements obtenus par leurs collègues, les Italiens manifestèrent à leur tour le désir de voir leur Consulat doté des mêmes installations, et, sans se faire autrement prier, nos techniciens procédèrent à l'installation d'un circuit semblable au Consulat italien rue Charras. Le résultat devait s'affirmer particulièrement payant, puisque c'est par ce canal d'écoutes que les opérateurs apprirent le code secret des transmissions de la Marine italienne, lequel fut aussitôt fourni aux Britanniques. On conçoit aisément quels bénéfices ceux-ci purent en tirer !

La masse d'informations fournies par les écoutes microphoniques d'Alger fut considérable. Parmi tous les rapports qui parvenaient régulièrement au TR 119, certains influèrent d'une façon décisive sur le sort de la guerre. Mais c'est certainement en muselant l'activité des services d'espionnage italo-allemands en A.F.N.[83], qui agissaient, rappelons-le, sous la couverture des commissions d'armistice, que le dispositif imaginé par Le Capelain et réalisé par les postiers d'Alger joua un rôle déterminant dans la lutte souterraine que se livraient l'Abwehr et le C.E. français.

Si les hommes de Paillole réussirent à neutraliser près de 400 agents de l'ennemi au cours de la période de fonctionnement des écoutes, ils le doivent avant tout à la remarquable équipe du Central protégé. La plupart de ces agents allemands ou italiens, dont l'arrivée était signalée aux responsables de l'organisation

[83] Afrique Française du Nord, nom donné à l'ensemble géographique colonisé par la France à la fin du XIXe siècle, et correspondant actuellement au Maroc, à l'Algérie et à la Tunisie.

nazie par un code oral, rapidement découvert par les spécialistes du C.E., n'avaient pas plus tôt posé le pied sur la terre algérienne qu'ils étaient aussitôt interceptés. De la même façon, plusieurs traîtres furent démasqués. Ainsi un secrétaire des services français de la commission d'armistice dont les écoutes révélèrent les relations qu'il entretenait avec le commandant allemand Schmidt, officier chargé de la liaison entre les trois commissions, fut arrêté. Trouvé porteur de documents secrets signés par Weygand, il fut interrogé longuement et ne tarda pas à donner l'un de ses complices. Tous les deux furent passés par les armes. Une affaire extrêmement importante, qui aurait pu avoir de graves conséquences, fut également décelée par les écoutes. Un officier français, très lié avec un membre de ce groupe qu'on appela « le Comité des Cinq[84] », avait pour maîtresse une fort jolie jeune femme brune à qui il ne cachait pas grand-chose de ses activités secrètes. Or, cette élégante personne au charme indéniable n'avait, de son côté, pas su résister à la virile prestance d'un lieutenant allemand qui lui soutirait habilement les renseignements qu'elle recueillait, sans trop y attacher d'importance il est vrai, auprès de son ami en titre. C'est au cours d'une conversation captée dans l'un des salons de l'*hôtel Albert-Ier* que l'attention de l'opérateur fut attirée, car les propos échangés n'avaient plus rien d'un tendre duo. Le lendemain, le téléphone de la belle était mis sur écoute normale. Quinze jours plus tard, le C.E. possédait suffisamment d'éléments pour intervenir discrètement. On peut s'interroger sur les prolongements que cette affaire aurait pu avoir, notamment dans le cadre de l'opération « Torch[85] », si le dispositif du Central protégé n'avait pas joué son rôle. D'autres cas de trahison ou de compromission furent dévoilés par les écoutes, notamment celui d'un double jeu, subtil et compliqué, mené par un collaborateur de l'amiral Bonetti, membre apparemment zélé de l'O.V.R.A., qui devait finir par perdre brutalement la vie au cours de cette partie truquée qu'il avait engagée.

Certains rapports d'écoutes eurent des conséquences inattendues, tel celui qui révéla l'existence d'un cercle de jeux clandestin qui réunissait plusieurs fois par semaine des hommes d'affaires, mais aussi des officiers allemands, italiens, français et américains du service consulaire de Murphy ; tout ce beau monde fraternisant dans l'ambiance fiévreuse et enfumée d'un salon particulier ! Pour y mettre fin, le C.E. fit intervenir, sous le couvert d'une dénonciation anonyme, le commissaire de police Achiary. Grâce à cette source exceptionnelle, il put également être mis fin à un scandaleux trafic de tissus et de vaisselle, devenus introuvables en Algérie, dans lequel étaient compromis des fonctionnaires importants acoquinés avec certains membres des commissions d'armistice. Mais c'est évidemment sur le plan politique et militaire que les informations recueillies au Central protégé s'affirmèrent les plus précieuses. Plus de 500 renseignements vitaux furent fournis par les écoutes microphoniques entre octobre 1941 et septembre 1942, dont, on l'a vu, le code des transmissions de la Marine italienne, et les lieux d'implantation des antennes de 1'Abwehr en A.F.N. et en zone sud dans la métropole. Et c'est finalement l'importance de ces fuites qui alerta les services de l'Ausland-Abwehr à Berlin.

C'est à partir de juin 1942 qu'il devint évident aux responsables allemands de la section III C du Contre-espionnage que leur commission d'armistice d'Alger n'était plus sûre. Ils montèrent donc une opération-test dans le but de vérifier leurs craintes. Leur représentant sur place, le capitaine Von Gagern, paraissant au-dessus de tous soupçons, il leur fallait éprouver les autres membres de leur mission en poste dans la Ville Blanche. Ce contrôle, doublé d'une enquête individuelle serrée sur chacun d'eux, ne donna rien. La disparition, ou l'élimination par identification, des agents envoyés sur place et annoncés par le code habituel signifiait pourtant que leurs desseins étaient chaque fois percés à jour. Un conseil de spécialistes émit, après un minutieux examen des faits, l'hypothèse d'un espionnage par micros. Alerté

[84] *Le Comité des Cinq* : formé de MM. Lemaigre-Dubreuil, Jean Rigault, Jacques Tarbé de Saint-Hardouin, Henri d'Astier de la Vigerie, lieutenant-colonel Van Hecke, et Robert Murphy, consul général des États-Unis à Alger, complotaient pour mettre en place en Algérie, sous l'égide des Américains, un pouvoir placé sous les ordres du général Giraud.

[85] Débarquement allié en A.F.N.

par un câble codé, Von Gagern fut prié de passer au peigne fin les locaux de travail et les appartements privés. Sa réponse, huit jours plus tard, désola les chefs de la III C, il n'avait rien trouvé. Curieusement, c'est presque par hasard que les Allemands furent aiguillés dans la bonne direction : un employé du chiffre apporta un beau matin une revue étrangère qui relatait la visite d'un ambassadeur soviétique à une personnalité politique d'un autre État, et l'article signalait le geste de ce diplomate qui, préalablement à l'entretien, couvrit l'appareil téléphonique de son manteau en disant : « On peut nous écouter par là ! »

Ce reportage banal fut une révélation pour les responsables allemands qui s'empressèrent d'enjoindre à Von Gagern de « surveiller » ses postes téléphoniques. Dans un premier temps, celui-ci se contenta, afin de toujours pouvoir utiliser son appareil, de « coiffer » le microphone du combiné d'une calotte de caoutchouc qu'il retirait pour téléphoner. Au central protégé, les écoutes devinrent plus sourdes sur la ligne desservante, mais l'audition resta acceptable.

Cependant, décidés à tout mettre en œuvre pour juguler les fuites, les chefs de la branche III C de l'Abwehr finirent par se décider à envoyer à Alger une équipe de techniciens de la *Siemens Halsk*. Ayant transité par le Maroc, ceux-ci ne parvinrent sur place qu'au début du mois de septembre. Les opérateurs de Le Capelain furent parmi les premiers informés de cette visite ; un secrétaire du consulat ayant cru bon d'en faire état dans une conversation banale avec deux de ses collègues. Il ne fallut bien évidemment que quelques heures aux ingénieurs allemands pour déceler l'anomalie présentée par les micros des appareils. Mais, fait extraordinaire, ils ne vérifièrent que les postes des bureaux et appartements de l'*hôtel d'Angleterre*, sans se préoccuper de ceux du consulat ! Cette attitude laisse supposer qu'ils accordaient toute confiance au personnel qui se portait lui-même garant de l'inviolabilité du lieu, et qu'ils ne soupçonnaient pas les agents des P.T.T. (Mergny et Rebau dingo) qui avaient procédé à l'installation et en assuraient l'entretien. Quoi qu'il en soit, pressés semble-t-il d'aller poursuivre leur tâche en Tunisie, ils ne menèrent pas plus loin leurs investigations.

Pour Von Gagern, soulagé par l'éclaircissement du mystère des fuites, restait à déterminer à qui cet espionnage subtil profitait et, partant de là, quels en étaient les auteurs.

Cependant, pour mener à bien son enquête, son champ d'action était réduit. Ne disposant pas, ou de très peu, d'informateurs locaux — on a vu que presque tous les agents envoyés furent interceptés, grâce aux écoutes, par les hommes de Paillole —, contraint de cantonner ses agissements dans le cadre étroit de ses attributions officielles qui devaient respecter l'apparente souveraineté du gouvernement de Vichy, il dut en passer par la voie diplomatique et adresser à son interlocuteur patenté — la commission française d'armistice — une réclamation en bonne et due forme. Celle-ci parvint au général Merlin qui désigna aussitôt le capitaine Flambard, des Transmissions, pour le représenter. On ne pouvait faire meilleur choix, puisque ce dernier, en tant qu'adjoint du commandant Guérin, qui, comme on l'a vu plus haut, dirigeait ce service, était parfaitement au courant du dispositif d'écoutes !

Le 28 septembre 1942, sur l'initiative de la commission d'armistice italo-allemande, une réunion se tient à l'hôtel d'Angleterre. Sont présents : d'une part, l'Amiral Saiza, le capitaine Von Gagern, et le lieutenant de vaisseau Forési ; de l'autre : le capitaine Flambard, le capitaine interprète Lucioni, et pour représenter l'administration des P.T.T. : MM. La Maïda et Pettenati.

D'entrée, Von Gagern se plaint d'être victime d'un « espionnage auditif » affectant les locaux à usage de bureaux, ainsi que certains appartements privés. L'Amiral Saiza, pour les Italiens, formule la même réclamation. Tous les deux insistent sur le fait que ces « indiscrétions » sont dues à des appareils téléphoniques truqués qui permettent d'enregistrer les conversations même lorsque les combinés sont raccrochés.

Bien entendu, Flambard montre son étonnement, et déclare hautement que si ces faits sont confirmés ils ne peuvent être imputés à la commission d'armistice française, ce qui est effectivement vrai. Interrogés par l'officier des Transmissions, La Maïda et Pettenati se montrent catégoriques : une telle modification intervenant sur les postes aurait provoqué de graves incidents de fonctionnement sur les lignes et se serait

répercutée au Central de la rue d'Isly. Ils proposent à leurs interlocuteurs de vérifier eux-mêmes les installations. À ce moment, le lieutenant de Vaisseau Forési sort de sa serviette un schéma de câblage relatif à l'un des appareils en service dans son bureau et il en démontre l'anomalie. Henri Pettenati l'examine attentivement et fait répondre par l'interprète

— « Il est évident que le schéma tel qu'il est présenté ici comporte une irrégularité. S'il a été relevé sans erreur, il ne fait aucun doute que le câblage du poste observé n'est pas correct. »

Monsieur La Maïda ajoute de son côté « qu'en fonction du manque de personnel qualifié, les femmes actuellement affectées au montage des postes en service ont pu commettre certaines erreurs ». Il propose donc que les appareils douteux soient remplacés, et renvoyés aux ateliers pour examen approfondi. Puis il indique, après avoir brièvement exposé les principes de fonctionnement, quelles sont les tensions utilisées. Le lieutenant de Vaisseau Forési reconnaît que ces valeurs sont bien conformes à celles mesurées par les techniciens de la *Siemens Halsk*, mais, tout en prétendant ne pas y connaître grand-chose, il s'étonne que les micros modifiés n'aient pas provoqué d'incidents sur les appels en batterie centrale ou automatique ! Henri Pettenati répond qu' « il ne comprend vraiment pas non plus, ce cas ne s'étant jamais présenté à sa connaissance et qu'il serait plutôt porté à douter de l'exactitude du schéma relevé ».

Après une courte discussion, il est alors convenu que des essais devront être effectués au plus tôt avec un haut-parleur pour constater la possibilité d'écoute de chacun des appareils en service à l'*hôtel d'Angleterre*, à l'*hôtel Albert-Ier*, à la villa-résidence de l'Amiral Saiza et au Consulat italien de la rue Charras. On note qu'il n'est pas question de l'*hôtel Aletti*, ni du Consulat allemand ; ce qui prouve bien que pour ce dernier Von Gagern n'imagine même pas qu'il ait pu être espionné. On retrouve là une forme d'aveuglement souvent manifestée par les Allemands pour ce qui appartient exclusivement à leur domaine. Ils conçoivent bien que de tels faits se produisent dans un lieu échappant à leur contrôle, mais se refusent à les admettre comme possible dans les sphères placées en totalité sous leur autorité.

Le capitaine Flambard établit alors le procès-verbal de la réunion, et les participants se séparent après avoir pris date pour une nouvelle séance au cours de laquelle il sera procédé aux essais de tous les postes.

Pendant que ce premier colloque de l'enquête se déroulait à l'*hôtel d'Angleterre*, M. Escande prenait ses dispositions, sur instructions du commandant Le Capelain qui craignait une visite des Commissions d'Armistice au Central protégé, pour effacer toutes traces du dispositif. L'après-midi même, et toute la nuit, une équipe placée sous les ordres de l'ingénieur Lacroze s'empressa de démonter les installations. Celles-ci furent remises en place dans un local désaffecté situé rue Généraux Morris, donc en un lieu pas très éloigné du Central protégé. Ce déménagement, réalisé en si peu de temps, fut un véritable tour de force.

Le 29 septembre au matin, rien ne subsistait de l'appareillage qui avait si bien fonctionné pendant de longs mois, mais il pouvait redevenir rapidement opérationnel si besoin était. Par prudence, Le Capelain ne le remit pas en service, alors qu'il était toujours possible d'intercepter les conversations du Consulat allemand.

Deux jours après, les mêmes protagonistes se retrouvent à l'*hôtel d'Angleterre*. Les premiers essais commencent, effectués par Mergny, requis comme exécutant, et en présence bien entendu des officiers de chaque commission. Suivant les instructions qui lui ont été données préalablement par Henri Pettenati, Mergny utilise les amplificateurs de telle façon qu'un effet de couplage Larsen provoque un hurlement intense démontrant évidemment l'anomalie du poste examiné, mais interdisant également d'entendre la moindre parole intelligible. Pettenati le fait constater à ses interlocuteurs assez surpris, et, sans insister davantage, enjoint à son compère de remplacer l'appareil défectueux. La même scène va se répéter dans plusieurs pièces ; tant et si bien qu'au onzième contrôle la surveillance hostile et méfiante du début se relâche. Ces messieurs préfèrent rester dans l'un des salons où, enfouis dans de profonds fauteuils, ils

savourent leurs cigares tout en évoquant le déroulement des opérations sur le front de l'Est ; seul un sous-officier appelé en renfort suit le travail des postiers. Cette négligence va permettre à Mergny, tandis que Pettenati détourne l'attention de l'Allemand, de démonter plusieurs postes sans les avoir essayés, et ainsi il ne pourra plus être prouvé que tous les appareils étaient truqués ! L'ingénieur des P.T.T. feindra de déplorer la hâte de son subordonné, mais elle n'entraînera aucune réaction du sous-officier du Reich qui signera sans objections le procès-verbal établi à la fin de la journée.

Cependant, Von Gagern va veiller par la suite, au cours des autres séances d'essais, à ce que tous les postes soient contrôlés. Quelques controverses surgiront d'ailleurs au moment de la signature du rapport contradictoire final ; Allemands et Italiens voulant qu'il soit précisé que tous les appareils ont été vérifiés, ce que refuse Henri Pettenati soutenu par Flambard. Finalement, après de longues discussions, les deux parties demeurèrent sur leurs positions, laissant aux Commissions italo-allemande et française le soin de rédiger un texte d'accord. Traitée par correspondance officielle et retardée par les Français qui firent traîner l'affaire, la signature définitive n'eut jamais lieu car le 8 novembre 1942 l'opération « Torch » commençait. Les Alliés prenaient pied en A.F.N. Quelques jours plus tard, l'Algérie rentrait dans le camp de la liberté.

De l'avis même des plus hauts responsables des services secrets français et alliés, les écoutes microphoniques d'Alger jouèrent un rôle déterminant dans la guerre du renseignement. Les Allemands eux-mêmes, et Canaris le premier, admirent que l'organisation mise en place par Chrétien et Le Capelain, sous les ordres de Paillole, leur porta un grave préjudice. Ils reconnurent s'être grossièrement trompés en mésestimant les capacités du S.R. français et principalement celles de ses antennes T.R. en A.F.N. Lorsque les écoutes furent découvertes, ils en imputèrent la réalisation aux Alliés, et principalement à l'I. S. C'est pourquoi leurs représentants à Alger ne s'intéressèrent guère, en tout cas pas en profondeur, aux agissements des postiers, pourtant les plus aptes à monter une telle opération. Cette erreur d'appréciation coûta fort cher aux forces de l'Axe au moment du débarquement anglo-américain sur les côtes marocaines et oranaises, de même qu'elle leur fut fort préjudiciable dans la bataille souterraine des S.R., car leurs ennemis détenaient, grâce aux écoutes, bien des renseignements qui, se juxtaposant, allaient démanteler en partie une organisation patiemment mise en place depuis des années. Il serait faux de dire que cette erreur de l'Abwehr fut la cause de la disgrâce de Canaris, mais il serait pareillement inexact de prétendre qu'elle n'y contribua pas.

Ce qu'il faut retenir de cette affaire, très peu connue, des écoutes microphoniques d'Alger, c'est le rôle essentiel, déterminant, joué par une poignée d'hommes, par une équipe de postiers, qui n'hésitèrent pas à s'engager dans une partie difficile et dangereuse dont les conséquences étaient imprévisibles. Dans l'atmosphère pétainiste qui régnait en 1941-42 en Algérie, alors que la puissance de l'Axe se manifestait partout, il fallait placer bien haut le sens du patriotisme et de l'honneur pour affronter les risques d'une activité clandestine en faveur des Alliés et de la France libre. Le travail accompli par les techniciens des P.T.T. d'Alger, travail obscur, délicat et ingrat qui réclamait non seulement du courage, mais aussi un formidable effort de recherche et d'imagination, appartient indiscutablement à l'histoire de la lutte clandestine et s'inscrit en bonne place dans l'épopée de la Résistance. Pourtant, aucun de ceux qui l'assurèrent n'a obtenu la plus petite médaille de reconnaissance. Seules, quelques lettres de félicitations de chefs d'État-Major témoignent de la valeur d'un comportement discret certes, mais particulièrement efficace.

Liaisons numériques et analogiques :

Dans le cas d'une société avec un raccordement numérique en RNIS[86] sur son PABX[87], il ne sera pas possible de se raccorder sur la liaison venant du central public, avec des moyens aussi faibles que précédemment. Si un particulier a demandé une ligne RNIS, une interface S0, là aussi, il n'y a qu'un électronicien performant qui pourra intercepter la communication. Un piratage de ce type nécessite des équipements d'un coût très dissuasif. Pour les grosses sociétés, la partie sensible se situe donc entre la PABX et la prise murale à la condition que l'abonné utilise un poste analogique. Le piratage ne pourra être réalisé qu'à l'intérieur de la société ou de l'immeuble. On retrouvera donc la solution des sucres, des bretelles, ou des magnétophones dissimulés dans des gaines ou cabines techniques avec les mêmes inconvénients que précédemment. Cette possibilité, bien que délicate, reste à la portée des personnes pouvant rentrer régulièrement dans un immeuble, dans le cas d'un enregistreur. Pour ce qui est du sucre, il suffit d'y entrer une seule fois pour toutes et de l'installer. Ce genre d'opération est réalisée dans un faux plafond, une gaine technique, ou un endroit discret, ne subissant jamais la moindre visite technique. Les méthodes de détection, sont les mêmes que précédemment, détection d'une haute fréquence résiduelle, d'un défaut d'impédance, d'un affaiblissement anormal sur la ligne. Pour contrer ces procédés, le responsable des installations techniques doit veiller à ce que les gaines et les salles soient fermées à clef. Les chemins de câbles doivent être propres et ne comporter que les câbles de communication, d'un même type si possible, afin de permettre le repérage d'un nouveau câble, qui ne serait pas destiné à une utilisation normale des systèmes de la société. Il ne doit y avoir aucune épissure sur l'un d'eux. C'est toujours à l'endroit des boîtes de jonctions, que les risques existent.

L'affaire du Canard Enchaîné

Le 3 décembre 1973 au soir, un dessinateur et administrateur du journal passe devant le futur siège du Canard Enchaîné, au 173 rue St Honoré. Il aperçoit de la lumière et décide d'aller voir quel journaliste fait du zèle dans cet immeuble pas encore fini, à cette heure tardive.

Il surprend alors plusieurs hommes occupés à « sonoriser » les futurs locaux du journal. Ces derniers s'empressent de prendre la fuite, mais le mal est fait.

Le Canard va alors mettre à jour l'opération Palmes, commanditée par la DST[88]. Le journal va publier comme à son habitude un certain nombre de détails croustillants (nom de la division de la DST, nom de la section technique qui s'est chargée des écoutes, noms et prénoms des commissaires et inspecteurs chargés de cette opération).

Le procès qui a suivi cette affaire mériterait à lui seul un livre :

Le Canard dépose une plainte pour « atteinte à la vie privée » et « violation de domicile ».

— Fin décembre 1976, le juge d'instruction déclare un « non-lieu » ... Ils n'ont tout d'abord pas retrouvé les auteurs de l'effraction. De plus, le bureau étant alors inoccupé il n'y avait pas à proprement parler de « domicile » et les conversations qui auraient pu s'y tenir ne pouvaient être que « professionnelles et non privées » (sic).

— Le Canard fait appel de cette décision, mais, en juillet 1977, la Cour d'Appel confirme le premier jugement.

— Le Canard se pourvoit alors en Cassation. La Cour de Cassation casse alors l'arrêt de la cour d'Appel pour un vice de forme dans le dossier.

— Le dossier est donc renvoyé devant la Cour d'Appel d'Amiens, qui estime qu'il y prescription sur les faits.

[86] Réseau numérique à intégration de services

[87] Un *Private Automatic Branch eXchange* (plus généralement appelé PABX et parfois PBX) est un commutateur téléphonique privé.

[88] Direction de la Surveillance du territoire

— Un ultime pourvoi en Cassation viendra clore ce dossier brûlant en février 1980.

On ne peut s'empêcher de se poser des questions sur l'indépendance des magistrats de l'époque ...

Les écoutes étaient vraisemblablement l'œuvre de la DST, qui en avait marre de ce palmipède qui semblait avoir des informateurs dans les plus hautes sphères de l'État. Mais une fois de plus, il semble que le pouvoir en place ait réussi à étouffer plus ou moins bien cette affaire.

Depuis cet épisode, l'administration du Canard enchaîné a laissé une plaque commémorative dans ses locaux à l'endroit où les agents avaient percé un mur pour y installer leurs équipements. Elle serait même devenue lieu touristique...

L'affaire des « plombiers » ou *Watergaffe* (comme on l'avait surnommée à l'époque), par son retentissement, a indirectement conduit le Premier ministre, Pierre Messmer et le président de la République, Georges Pompidou, deux mois et demi après les faits, à permuter les ministres de l'Intérieur et de l'Agriculture lors de la formation du troisième gouvernement de Pierre Messmer, le 1er mars 1974 : Raymond Marcellin, jusque-là ministre de l'Intérieur et ayant la tutelle de la DST, a ainsi échangé son poste avec celui de Jacques Chirac, ministre de l'Agriculture et du Développement rural. L'arrivée de Jacques Chirac au ministère de l'Intérieur a eu un effet non négligeable dans la campagne pour l'élection à la présidence de la République du successeur de Georges Pompidou, décédé le 2 avril 1974, l'affaire des plombiers devenant ainsi, parmi d'autres, l'un des éléments qui ont contribué à la victoire de Valéry Giscard d'Estaing lors de l'élection présidentielle de 1974.

Liaison numérique / numérique :

Dans le cas d'une liaison numérique de bout en bout, le piratage à peu de frais devient impossible si à la place d'un poste analogique on installe un poste numérique. Chaque constructeur de PABX dispose de sa propre signalisation pour alimenter ses postes téléphoniques numériques. Ils ne sont donc pas interchangeables. Un professionnel des écoutes sera contraint de réaliser un adaptateur spécifique s'il veut écouter à distance un poste numérique. La solution la moins coûteuse et la moins compliquée techniquement consiste par exemple à remplacer le combiné d'origine du poste numérique du constructeur par un autre combiné qui lui, aura été trafiqué à l'avance en y incorporant un sucre émetteur. Nous allons donc retrouver les mêmes inconvénients que cité plus haut.

Si l'accès est impossible au poste souhaité, il ne reste plus qu'une connexion pirate sur la ligne RNIS en amont du TNL qui contient les MIC[89] du PABX. On ne peut croire à cette solution pour diverses raisons. En plus d'être coûteuse, plusieurs centaines de milliers de francs, ce type de matériel nécessaire est peu discret et nécessite un emplacement sûr pour son camouflage et à l'abri des intempéries. Il est aussi nécessaire de disposer de très bonnes connaissances techniques. Dans ce cas, ce matériel est immédiatement repéré. Je ne vois pas de professionnels des écoutes illégales installer un matériel aussi volumineux et coûteux dans les souterrains ou une cabine de sous-répartition. L'équipement en plus doit être de qualité et raccordé en très haute impédance. Toutes dégradations de ligne entraînent des erreurs qui seraient immédiatement détectées par le central et même l'utilisateur. Des appareils comme les analyseurs dont le bas de gamme commence à 40 000 F ne permettent d'écouter qu'un seul IT (canal), alors qu'un MIC en comporte 30. En plus, un abonné derrière un PABX n'utilise jamais le même IT, il faut donc enregistrer les 30. En clair, même en 95, un équipement sophistiqué avec enregistrement des 30 canaux ne pouvait pas coûter moins de 200 KF et encore en faisant preuve d'ingéniosité. Aujourd'hui, même si on sait se connecter sur la liaison à peu de frais, il reste toute la partie traitement à réaliser derrière, pour sélectionner et écouter les conversations nécessaires. Avec un autre surcoût, on peut prendre un analyseur de protocole de l'IT16 de signalisation, qui permet d'enregistrer l'abonné après détection de son numéro sur n'importe quel IT. Il faut en plus être certain qu'il utilise toujours le même poste. Il faut donc être

[89] Carte électronique (Modulation par Impulsion et Codage) qui transforme la voix (signal analogique) en signaux numériques (octets).

un bon ingénieur, compter de 30 à 50 KF, et développer son propre logiciel pour faire une interception efficace sur un MIC T2.

On ne peut donc croire à ce type d'écoutes illégales sur les installations des grosses sociétés. Même une liaison pour une écoute légale ou illégale réalisée par un service officiel sur un MIC, peut entraîner des perturbations. Pour les gros sites dépassant les 4 MIC, il est possible de demander un raccordement sur un ROF s'il y en a un de disponible dans le quartier. Il s'agit d'un raccordement en fibre optique. Les spécialistes comprendront ici qu'il n'est plus question de faire un branchement pirate avec une épissure dans ce type câble, car c'est impossible. Avec une solution en ROF, une écoute ne peut s'effectuer qu'au niveau du central (CPE).

Écoutes téléphoniques sauvages par les fonctions soft

Ces méthodes sont encore plus vicieuses, car non détectables.

Écoute par la fonction de décroché automatique :

C'est une autre méthode moins connue, qui peut permettre de faire des écoutes illégales à l'intérieur d'un local en toute discrétion, en intervenant par le biais d'une programmation. Il n'y a aucune intervention physique comme le câblage d'une bretelle sur une ligne. Cette fonction est inutilisable avec des postes téléphoniques simples sur tous les types de PABX. Par contre, on peut programmer cette fonction sur certains calculateurs, pour que des postes numériques décrochent automatiquement et se mettent en mode mains libres tout seul, au bout d'un nombre de sonneries défini. Ce moyen est dangereux, car il permet une écoute insidieuse à l'intérieur d'un bureau. Il est possible d'affecter un autre numéro de ligne sur une touche de fonction inutilisée d'un poste numérique. Cette méthode a l'avantage de permettre à la ligne de l'utilisateur de rester disponible pour ses appels extérieurs et il ne peut donc détecter la supercherie. Il n'est pas impossible que des pirates, des officines non autorisées, ou même des services de renseignements étrangers, tentent ou utilisent cette fonction à l'insu des utilisateurs. Il ne faut pas oublier que des systèmes téléphoniques complexes ont une origine étrangère. On ne peut connaître la totalité de toutes les fonctions disponibles même pour les meilleurs techniciens. Pour cela, il faut des ingénieurs systèmes capables d'éplucher les programmes des calculateurs. Plus les systèmes sont complexes, plus ils sont dangereux, car moins facile à maîtriser. Seule une quantité limitée d'ingénieurs des constructeurs respectifs connaissent la totalité des fonctions disponibles, pour avoir participé à la réalisation des programmes. Rien ne peut garantir à un utilisateur que ce type de fonction n'existe pas sur les postes numériques RNIS, ou qu'un jour, un pirate, un service de renseignement étranger trouvera une parade pour déclencher le poste et espionner en toute impunité sur n'importe quel type de système. D'où la nécessité de système d'observation de trafic pour les appels entrant sur une société. La taxation dans ce cas précis ne sert à rien puisque les appels entrants ne sont pas facturés, puisque cela ne se réalise que sur des appels sortants. Il faudrait être inconscient pour affirmer à 100 %, que ce moyen n'existe pas sur les systèmes présents sur le marché. Cette fonction peut autoriser l'écoute des conversations des syndicalistes, s'ils sont dans une salle réunion dotée d'un poste numérique.

Écoute téléphonique par la fonction conférence :

La fonction conférence permet normalement à plus de deux interlocuteurs de dialoguer sur une même ligne. L'appelant compose les numéros de ses (x)correspondants et appuie sur la touche conférence afin de permettre le dialogue dans tous les sens à travers le téléphone, donc le PABX de son site.

Un technicien de bon niveau par diverses astuces peut déclencher cette fonction sur certains PABX afin de réorienter la communication entre deux interlocuteurs ou plus, vers une autre ligne afin de réaliser une écoute ou un enregistrement pirate. Ce moyen est possible sur les postes numériques, mais aussi analogiques, et à condition que le PABX dispose d'assez de cartes électroniques dotées de circuits confé-

rence. Sur certains PABX, le calculateur est capable de faire appel aux circuits conférence disponibles dans tous les châssis, si le châssis du poste demandeur n'a plus de circuit disponible. Un utilisateur ne peut donc découvrir l'anomalie. Par contre, d'autres systèmes imposent la limite de 2 ou 5 correspondants par (x)demandeurs dans un châssis. Dans ce cas, lors d'essais en faisant plusieurs appels simultanés, il est possible de découvrir la supercherie.

Ce moyen peut se repérer assez vite par l'exploitant de l'installation contrairement au cas précédent. Si la conversation est réémise simultanément sur une deuxième ligne parallèlement à celle du demandeur, nous aurons une double trace sur le système de taxation téléphonique, avec une date et une heure d'appel identique à chaque fois sur deux lignes différentes. Ce procédé peut cependant passer inaperçu, si l'auteur a pris la précaution d'intervenir sur le filtrage des tickets de taxation du PABX, ou sur le système externe de taxation téléphonique. Il est rare que l'on arrive un tel point de sophistication dans le piratage soft. Il est en effet plus facile de mettre une bretelle. Il est aussi possible de réorienter l'appel par ce biais vers un enregistreur magnétique, raccordé sur une ligne analogique interne à la salle PABX. Là, nous sommes dans le cas où le PDG de la société fait écouter et enregistrer les communications de ses salariés. Il faut savoir que très souvent, les communications des salles de marchés des grandes banques ou bourses, sont enregistrées afin de limiter ou d'empêcher les malversations.

Écoute par la fonction double appel :

La fonction double appel, connue par les utilisateurs sous la touche R2, permet aussi de réaliser des écoutes illégales. Dans la réalité tout dépend des fonctions disponibles dans les logiciels des calculateurs des PABX, et même des bugs logiciels inconnus de leurs concepteurs, qui peuvent permettre, par l'addition d'astuces successives, de faire une écoute illégale, par le biais d'une programmation pirate par la voie de la télémaintenance. Le principe est en effet le même que précédemment, mais inverse. Au lieu d'avoir un appelant qui appelle sur deux lignes deux correspondants extérieurs, nous avons ici deux personnes extérieures qui vous appellent l'une après l'autre. Il y a donc deux lignes au niveau du central, si l'une a été programmée pour permettre une écoute illégale, vous ne pourrez jamais prendre le deuxième interlocuteur.

Écoute par fonction priorité d'appels vers l'extérieur :

Un procédé permet de rendre un poste prioritaire comme celui des exploitants techniques ou des directeurs par exemple, pour appeler l'extérieur, lorsque toutes les lignes réseau sont occupées. Il suffit pour cela de déclarer les postes concernées en prioritaires. Ils prendront automatiquement une ligne extérieure, et couperont les communications en cours des postes non prioritaires.

Cependant, ce procédé présente un risque. Il permet aussi d'écouter une communication en cours à l'insu des deux interlocuteurs. Cette fonction n'est pas à installer par exemple dans un immeuble qui utilise le même PABX pour plusieurs sociétés. Cet inconvénient peut provenir d'un bug logiciel, mais peut être aussi volontaire pour prévenir les personnes en communication, qu'on va les couper pour récupérer leur ligne. Cette fonction se retrouve le plus souvent sur le poste opérateur de la standardiste ou des exploitants, afin qu'ils puissent appeler l'extérieur en cas d'urgence, effondrement d'un réseau pour cause de surcharge, incendie, panne électrique, etc. C'est ce qui permet aussi à certaines standardistes d'écouter les conversations internes des salariés, des cadres de direction et PDG.

Affaires contemporaines d'écoutes téléphoniques

Un roman-feuilleton policier à l'américaine

L'affaire du Watergate est le plus grave scandale politique qu'aient jamais connu les États-Unis. Il contraignit le président en place à démissionner, et modifia pour longtemps les rapports d'influence entre le président et le Congrès, tout comme le prestige attaché à l'institution. Jamais une affaire policière n'avait eu de telles répercussions à l'échelle de la politique intérieure. Et pourtant, tout avait commencé comme une « tentative de cambriolage de troisième ordre » (selon un porte-parole de la Maison Blanche)...

En effet, le 17 juin 1972, à une heure du matin, le gardien de l'immeuble du siège du Parti démocrate, le *Watergate*, fait sa ronde de nuit. Il remarque que deux portes, qu'il avait pris soin de fermer quelques temps auparavant, ont été forcées. La police, discrètement alertée, saisit cinq hommes en flagrant délit dans les locaux du parti. Une banale arrestation.

Banale ? Pas si sûr. À y regarder de plus près, ces cinq cambrioleurs ne ressemblent guère à des cambrioleurs ordinaires. On trouve sur eux de l'argent liquide leur appartenant, un impressionnant arsenal de matériel électronique d'écoute et d'espionnage, qui les fait plus ressembler à des agents secrets qu'à des voleurs.

Tout de suite se pose la question : d'où cet argent vient-il ? Flairant le scoop, deux journalistes du *Washington Post*, Carl Bernstein et Bob Woodward, vont mener tambour battant une enquête qui va très rapidement les amener jusqu'au CRP (*Comité pour la Réélection du Président*), et, par delà cet organisme-écran, le proche entourage de Nixon. De son côté, l'enquête judiciaire met rapidement en lumière le rôle occulte joué par la CIA, ainsi que ses collusions avec le CRP. C'est alors que les têtes commencent à tomber. Un homme de main, Hunt, puis le président du CRP, parti « s'occuper de sa famille ». Mais bien d'autres questions restent sans réponse. La plus importante d'abord, pourquoi les cinq hommes se sont-ils introduits dans le quartier général du Parti démocrate ? Pour poser des micros, semble-t-il, mais au profit de qui ? Pour voler des documents, peut-être, mais lesquels ? Ah ! si du moins l'on connaissait le nom du responsable de l'opération, de celui qui a donné le feu vert...

De son côté, le 22 juin, le président Nixon a fait une déclaration publique : « La Maison Blanche n'a aucune part dans cet incident précis ». Et l'intérêt pour l'affaire s'affaiblit lentement. Rien de sensationnel à annoncer ou à lire dans ce magouillage politicien. Un relent qui se dégage de la vie politique, rien de plus. Mais le *Washington Post*, influent, bien informé, empêche que le scandale soit étouffé. Il révèle que des sommes colossales ont été blanchies par le CRP pour soutenir tout un tas d'actions à la légalité plus que douteuse.

Le Watergate, c'est déjà en 1972 un scandale qui souligne le financement parfois illégal de la campagne électorale des républicains.

Cependant, l'élection présidentielle est un véritable triomphe pour Nixon. Il en conclut que sa victoire vient de balayer le dernier souffle du scandale et les dernières semaines de 1972 lui donnent raison. Le réveil de 1973 n'en est que plus brutal.

C'est le 8 janvier que s'ouvre le procès des cinq « plombiers » du Watergate, plus deux de leurs commanditaires. L'un d'eux, McCord, cède sous la pression et les activités illicites du CRP apparaissent au grand jour. Le juge Sirica reporte la sentence de McCord en espérant que les choses vont se calmer et les langues se délier, mais voilà que le Congrès s'en mêle. En janvier, le chef de la majorité démocrate confie au sénateur Sam Erwin la présidence d'une commission spéciale d'enquête sur la campagne présidentielle. Mais avant même le début de ses travaux, le bruit du scandale commence à remonter jusqu'aux proches du président. De rebondissement en rebondissement, le Watergate se présente comme la révélation de pratiques gouvernementales qui, en utilisant l'abus de pouvoir, ne visent ni plus ni moins qu'à saper les fondements du régime démocratique.

C'est l'heure du grand chambardement. Nixon décide enfin d'agir. Le 30 avril, il prononce une allocution télévisée pour faire savoir que ses plus proches collaborateurs, Dean, Ehrlichman et Haldeman démissionnent. Ceci a pour effet de leur coller l'étiquette de coupable sur le dos. S'ils sont responsables, il est innocent. Le reste n'est que manipulation de l'opinion. Mais ce sacrifice reste vain.

Car, de son côté, la commission Erwin va de surprise en surprise. Son rôle est déterminant, mais il faut en saisir les limites. Le Congrès peut créer, à sa guise, des commissions d'enquête, les doter de crédits de fonctionnement et les transformer ou non en commissions permanentes. Il arrive qu'elles reçoivent le droit de subpoena[90], le droit de réquisition judiciaire qui les autorise à faire comparaître des témoins. En ce cas, les témoins déposent sous la foi du serment et sont susceptibles, s'ils mentent, d'être inculpés pour faux témoignage.

Ces commissions ne sont cependant pas des tribunaux. Elles ne jugent pas et ne condamnent pas. Mais elles sont redoutables et redoutées. Dans le passé, elles ont servi à débusquer les gaspillages du gouvernement fédéral, les réseaux de gangstérisme, les infiltrations communistes. Leur puissance fait d'autant plus peur que leur composition repose sur des fondements politiques. Leurs auditions étant télévisées, les Américains ont ainsi l'impression qu'ils participent au fonctionnement de la démocratie. Et force est d'admettre que le spectacle les passionne. Les chaînes alternent retransmissions et commentaires sans regarder sur le temps d'antenne. La commission entend des témoins tout à fait inattendus.

Assistants auprès du président, anciens membres du cabinet, responsables des services de renseignement, animateurs du CRP... Leur fidélité à Nixon ne fait aucun doute. Mais l'heure n'est plus à l'héroïsme. Il faut parler, sous peine d'être contredit par le suivant et poursuivi pour faux témoignage. En un mot, c'est le sauve-qui-peut général. Le témoignage de Dean est accablant, mais il est contredit par Ehrlichman, et les preuves irréfutables manquent.

Et le miracle finit par se produire. Alors qu'elle interroge un des collaborateurs de Haldeman, la commission lui produit une note transmise par les services du président, sur une conversation avec Dean. La note est précise, trop précise pour être un résumé. Et le collaborateur, d'une voix calme, d'annoncer que la conversation est extraite d'un enregistrement. D'un enregistrement ? Oui, le président enregistre tous ses entretiens à l'insu de ses interlocuteurs. Le système est complexe. Les bandes magnétiques se mettent en route dès que les voix sont audibles. Pas de bouton à pousser, pas de levier à actionner. Émotion. « Nixon espionnait ses propres bureaux », titre le *New York Times*. Les Américains découvrent que leur président espionne, dissimule, ne cesse de mentir.

[90] Subpoena : une Citation, c'est « une commande d'apparaître à un certains temps et endroit pour donner le témoignage sur une certaine question. »

À la vérité, le contenu des bandes devrait faire progresser l'enquête. On saura enfin ce que Nixon a appris, dit et ordonné depuis plus d'un an. C'est pourquoi la commission sénatoriale et le procureur ont demandé immédiatement qu'un certain nombre de bandes leur soit communiquées. Nixon hésite sur la conduite à tenir. Il ne peut plus détruire ces bandes. Faut-il les donner au Sénat et à la Justice ? Non, car l'Exécutif n'a pas à livrer au Législatif des documents confidentiels qui touchent la sécurité nationale. La Maison Blanche fait traîner la procédure, au point que l'Attorney General (équivalent du juge d'instruction) et le procureur spécialement mis en place démissionnent.

Les journalistes s'empressent de trouver une expression qui fait mouche : « *le massacre du samedi soir* ». La réaction des médias frise l'hystérie. On parle d'Apocalypse, de coup d'État, on parle de « *la nuit des longs couteaux* ». Impossible pour la Maison Blanche de dissimuler davantage. L'opinion en a assez des mensonges, elle veut savoir.

Pour peaufiner le tableau, le vice-président, Spiro Agnew, a été contraint de démissionner, par trop mouillé dans une affaire de corruption. Et c'est alors que le Sénat met en route une procédure mal connue, mais qui va faire parler d'elle, et qui constitue son atout majeur dans le contrôle du Législatif sur l'Exécutif : la procédure d'*Impeachment*[91].

Elle a été déclenchée le 31 juillet 1973 par un représentant, mais est restée sans effet. C'est au lendemain du 20 octobre que l'opinion réclame que le Congrès agisse. Quatre-vingt-quatre membres de la Chambre signent une motion d'Impeachment. Malgré les concessions de Nixon sur l'accès aux bandes magnétiques, malgré une opération « Honnêteté » que monte la Maison Blanche pour prouver une fois

[91] Lorsque se posa aux constituants américains la délicate question du contrôle des diverses responsabilités du président des États-Unis, il fut opté pour la reprise pure et simple d'une procédure traditionnelle britannique, qui, sans trop démettre la séparation des pouvoirs, donne au Législatif un certain contrôle sur l'Exécutif.
L'*Impeachment* est donc une invention anglaise. Au départ, il s'agissait, conformément à la tradition, d'une procédure pénale, destinée à sanctionner un ministre ayant commis dans l'exercice de ses fonctions, une infraction. La Chambre des Communes l'accusait et la Chambre des Lords le jugeait. Sur ce fondement, deux ministres de Charles I^er^ (Stanford et Laud) furent exécutés. Aussi, à la fin du XVIII^e^ siècle, la simple menace d'Impeachment suffit à provoquer la démission du cabinet : en 1782, le ministre présidé par Lord North donne sa démission à la suite d'une motion de défiance votée par la Chambre des Communes et considérée comme susceptible d'entraîner la mise en œuvre de la procédure d'Impeachment. À partir de cette période, on peut considérer que la responsabilité pénale et individuelle se transforme en responsabilité politique et collective du cabinet. La responsabilité politique se traduisait par une perte du pouvoir. Cette procédure est double : tantôt le premier ministre prend l'initiative de vérification, et pose la question de confiance. Tantôt, au contraire, l'initiative du débat est prise par les membres de l'assemblée, qui déposent une motion de censure. Signalons que le gouvernement dispose toutefois d'une arme de dissuasion : le droit de dissolution contre le parlement. C'est de même une procédure de contrôle du Législatif sur l'Exécutif qui a été mis en place dans la procédure américaine.
Aux États-Unis, l'Impeachment est la procédure selon laquelle le Congrès a la possibilité de mettre en cause la responsabilité du président, en le destituant, lorsque, dans l'exercice de ses fonctions, il est reconnu coupable, aux termes de la section IV article 2 de la constitution de 1787, de trahison, corruption ou autres délits graves. Cet article 2 souligne le caractère exceptionnel de la procédure, qui ne s'applique qu'au président, au vice-président, des États-Unis et à tous les fonctionnaires civils. Dans le droit américain, tous les crimes sont soumis au jugement d'un jury, sauf ceux qui entraînent L'Impeachment.
L'Impeachment se déroule en deux temps. La Chambre des représentants (l'équivalent de l'Assemblée en France, par sa composition) prend l'initiative. Il suffit que l'un de ses membres dépose une proposition d'Impeachment qui est transmise à la commission des affaires judiciaires (commission permanente formée dans le but de déterminer l'éventuelle responsabilité des membres du Congrès dans l'exercice de leurs fonctions). Si la commission émet un avis favorable, l'assemblée se prononce, à la majorité simple, sur sa mise en accusation. Dans le cas d'un vote positif, la Chambre assume le rôle de procureur général et délègue à plusieurs de ses membres, les managers, le soin de présenter l'affaire aux sénateurs. Le Sénat se transforme alors en Haute Cour. Il se prononce sur le dossier qui lui a été soumis, après avoir entendu l'accusation, les témoins et la défense. Si la condamnation est votée à la majorité des deux tiers, le coupable est démis de sa charge. Si la majorité des deux tiers n'est pas atteinte, l'acquittement est prononcé. Reste à savoir, et c'est là un problème que les Américains ne cessent de débattre, ce que sont « la trahison, corruption ou autres crimes et délits » qui déclenchent la procédure. Ce flou a débouché sur une pratique extrêmement hésitante.

de plus que la page du Watergate a été tournée, la procédure est lancée. Dès la fin d'octobre, la motion est transmise à la commission des affaires judiciaires que préside Peter W. Rodino, un démocrate du New Jersey. À ses côtés, 20 autres démocrates et 17 républicains. La commission s'entoure d'une centaine d'experts, dont 45 avocats, reçoit de la Chambre un crédit d'un million de dollars pour mener l'enquête et, le 6 février 1974, se fait attribuer par la Chambre (410 voix pour, 4 voix contre) le droit de préparer un rapport sur L'Impeachment et de citer à comparaître les témoins indispensables. Il ne reste plus au président Nixon qu'à renforcer l'équipe de ses défenseurs et à promettre sa collaboration « dans les limites des devoirs de sa charge ».

Pour mener à bien sa mission, la commission ne manque ni de moyens, ni de pouvoirs. Elle obtient la communication du dossier qui a été préparé par le grand jury (jury d'assises qui avait suivi l'instruction du procès des cinq « plombiers »). Elle bénéficie de l'aide de la presse. Mais il lui faut, en plus, une source indispensable qui lui permettra de juger de la sincérité du président : les bandes magnétiques.

Jusqu'à la fin de juillet 1974, Nixon livre bataille, cède pied à pied du terrain et concentre involontairement l'attention de tous, y compris la sienne, sur le contenu des enregistrements. Le procureur spécial avait réclamé 9 bandes. Nixon est contraint de lui nommer un successeur, Leon Jaworski, et de promettre que les 9 bandes seront transmises au juge qui occultera, lui-même, les secrets de la défense nationale. Un geste de conciliation de la Maison Blanche. Et puis, l'on apprend que sur l'une des bandes, la conversation capitale entre Nixon et Haldeman à propos de l'effraction alors toute récente, est amputée de 18 minutes. Les spécialistes précisent qu'il s'agit d'un effacement par opération manuelle. Qui est responsable ? Avec dévouement, la secrétaire particulière du président, Rose Mary Woods, s'accuse de maladresse dans la manipulation des bandes. L'explication passe mal. D'ailleurs, la commission des affaires judiciaires demande maintenant à la Maison Blanche des documents et d'autres bandes magnétiques. Refus. La commission se fâche, rappelle qu'elle dispose du droit de citation à comparaître et que tous les Américains, quelle que soit leur fonction, sont contraints de s'y soumettre.

Nixon croit alors avoir une idée géniale, qui en fin de compte lui coûtera cher.

Le 30 avril, le voici de nouveau devant les caméras de télévision. Le ton est solennel. Un an jour pour jour après la démission de Dean, Ehrlichman et Haldeman, le président annonce la nouvelle qui devrait mettre fin à l'agitation des esprits. La Maison Blanche a transcrit 46 conversations sur le Watergate. Elle publie la transcription en un volume de 1.300 pages, qui porte le sceau officiel. Une sorte de *Livre Blanc* définitif. Définitif, peut-être, incomplet, très certainement. Et surtout, très révélateur sur la personnalité de Richard Nixon, l'atmosphère de la Maison Blanche, le goût du secret et de la manipulation qu'expriment Nixon et ses collaborateurs. À lire le texte de ces conversations impromptues, sans fard ni précautions, les Américains apprennent que leur président se croit entouré d'ennemis, qu'il n'a qu'un souci, se tirer par n'importe quel moyen du mauvais pas dans lequel le Watergate l'a fait glisser.

D'innombrables « exclamations supprimées » témoignent de l'exactitude de la transcription et de la violence du ton. Le *Chicago Tribune*, qui a soutenu Nixon depuis 1968 résume l'opinion générale : « *Nous avons, au cours du premier mandat, vu l'homme public et nous avons été impressionnés. Maintenant, nous venons de voir l'homme privé et nous sommes atterrés* ».

Nixon perd bataille après bataille. Ce n'est pas qu'il ne dispose pas d'atouts. Sa politique extérieure connaît des succès appréciables depuis 1974 : le Moyen-Orient, l'URSS et l'OPEP sont des victoires diplomatiques incontestables, mais tout ceci ne sert à rien. Pour trois raisons :

1 — L'année 1974 est celle où les séides, puis les proches de Nixon sont condamnés. C'est la longue litanie des peines de prison qui frappent ces hommes, hier tout-puissants, aujourd'hui réduit à quémander la clémence des juges. Ils tombent les uns après les autres : les sept du Watergate, puis les proches de Nixon de l'époque. Leur chute ne peut que susciter deux questions. Le vrai responsable, n'est-ce pas leur chef ? Et Nixon n'a-t-il pas déclaré plusieurs fois qu'il assumerait l'entière responsabilité ? Les procès,

longs et détaillés, ont retenu l'attention. L'Amérique mène une œuvre de purification. Elle en oublie le monde.

2 — Les tribunaux fédéraux manifestent une incontestable indépendance. La liste des condamnés l'atteste et l'on se rappelle la détermination du juge Sirica, même si ses méthodes, voire sa brutalité inspirent des réserves. Le plus remarquable, toutefois, reste l'attitude des juges de la Cour Suprême.

En 1974, quatre de ses membres, y compris le Chief Justice Warren Burger, ont été nommés par Nixon avec l'approbation du Sénat. On a donc parlé d'une « Cour Nixon » qui aurait les mêmes idées conservatrices que le président et ne nourrirait qu'un seul désir : faire plaisir à Richard Nixon. Pure calomnie. Les magistrats ont montré une inébranlable rigueur. Ils ont dû donner leur avis sur l'accès aux bandes magnétiques. Le 24 juillet, ils sont unanimes (8 voix pour, 0 contre, 1 abstention) à déclarer que le président ne peut refuser la demande du procureur spécial.

C'est une décision capitale qui brise les dernières résistances de Nixon. Le 5 août, le président livre la transcription des trois conversations du 23 juin 1972 avec Haldeman. Il en ressort que Nixon a tout fait pour empêcher la poursuite de l'enquête judiciaire, et qu'il a dissimulé à ses propres avocats une partie de son rôle. La guerre est perdue. Nixon se résigne à la reddition sans condition. La décision du 24 juillet confère aux tribunaux fédéraux, à la Cour Suprême en particulier, un prestige exceptionnel. Ils ont contribué, eux aussi, à sauver le régime démocratique.

3 — Le rapport des forces politiques fait pencher définitivement la balance. C'est le temps des élections législatives et les nixoniens ne peuvent plus tirer profit de leur fidélité pour le président. Le navire coule. Il est temps de quitter le bord.

Dès la mi-juillet, il est évident que la Chambre des représentants votera la mise en accusation. Quant à la commission des affaires judiciaires, elle passe à l'élaboration de son rapport. Elle adopte un à un les articles établissant les chefs d'accusation. Ces articles, la Chambre doit les examiner dès la séance du 19 août. Le Sénat, de son côté, se prépare à se transformer en Haute Cour. Que peut faire Nixon ? Ses amis au Congrès le lâchent. Il pourrait décider de se battre jusqu'au bout. Somme toute, pour n'être pas démis de ses fonctions, il lui suffit que 34 des 100 sénateurs lui soient favorables. Mais ces 34 voix, il ne les a pas. Et puis, si le procès a lieu, les États-Unis seront paralysés pendant plusieurs mois et le président sortira de l'épreuve vaincu ou affaibli. S'il démissionne, il reconnaît implicitement sa culpabilité. Et depuis le 5 août, il a reconnu qu'il avait tout fait pour étouffer l'affaire. Le 7 août, la rumeur circule avec insistance : le président va démissionner. Le lendemain soir, Nixon annonce à la télévision qu'il quitte la Maison Blanche dans les 24 heures.

Le président Nixon quitte la Maison blanche

Le 9 août à midi, le président Ford prête serment et devient président des États-Unis. Nixon se retire en Californie.

L'épilogue a lieu le 8 septembre, quand le président Ford prend une décision très impopulaire : il accorde à Nixon « son pardon pour toutes les offenses commises ». Ce pardon présidentiel évite un procès en bonne et due forme qui aurait éclairé les dessous de table du scandale, résolu les énigmes et établi les véritables responsabilités, qui appartiennent désormais à l'Histoire.

Affaire des écoutes de l'Élysée

L'affaire des écoutes de l'Élysée est une affaire d'écoutes téléphoniques illégales qui s'est déroulée sous le premier septennat de François Mitterrand (de 1983 à 1986).

La cellule antiterroriste de l'Élysée dirigée par Christian Prouteau et créée par François Mitterrand en 1982 serait impliquée.

Cette affaire, fut révélée pour la première fois par le quotidien *Libération* le 2 avril 1993.

Elle aurait selon le dossier concerné 150 personnes, dont 7 dans des conditions contestables. Près de 3000 conversations auraient été enregistrées entre janvier 1983 et mars 1986. Les écoutes, que les initiés appellent les « bretelles du président », ont apparemment cessé au moment de la victoire de la droite au élections législatives de mars 1986 qui a entraîné une période de cohabitation.

Comme la presse l'a rapporté, ce ne furent pas les premières écoutes téléphoniques effectuées par les services de la république...

Le procès des écoutes de l'Élysée sous Mitterrand débute le lundi 15 novembre 2004

Le procès des écoutes de l'Élysée, portant sur l'existence d'un « cabinet noir » qui écoutait illégalement des centaines de personnalités entre 1983 et 1986, lors du premier septennat de François Mitterrand, s'ouvre lundi 15 novembre 2004, à Paris, avec douze prévenus à la barre.

Douze personnes comparaissent, à partir de 13 h 30, devant le tribunal correctionnel de Paris dans le cadre de l'affaire des écoutes illégales par l'Élysée de centaines de personnalités entre 1983 et 1986, sous le premier septennat de François Mitterrand.

Au cœur de cette affaire : la cellule antiterroriste de l'Élysée, officine créée en 1982 à l'initiative du chef de l'État. Mais sous prétexte de défense de la sécurité nationale, la cellule a surtout cherché à étouffer certaines affaires compromettantes pour le pouvoir ou taire les secrets d'alcôve du président, écoutant des personnalités aussi diverses que l'actrice Carole Bouquet, l'écrivain Paul-Loup Sulitzer ou l'avocat Jacques Vergès.

Parmi les principaux prévenus, poursuivis pour les fonctions qu'ils occupaient entre 1983 et 1986, figurent Gilles Ménage, 61 ans, ex-directeur adjoint de cabinet du chef de l'État, et Christian Prouteau, 60 ans, ex-chef du Groupe d'intervention de la gendarmerie nationale (GIGN), directement chargé de la cellule.

Après s'être longtemps réfugiés derrière le secret-défense, les deux hommes ont fini par admettre, devant le juge chargé de l'instruction, certaines des écoutes qui leur étaient reprochées, tout en les jugeant légitimes et en soulignant avoir agi sur ordre de leur hiérarchie.

Parmi les prévenus figureront également Michel Delebarre, 58 ans, directeur de cabinet de l'ancien premier ministre socialiste Pierre Mauroy de 1982 à 1984, aujourd'hui député, maire (PS) de Dunkeque (Nord), ainsi que l'actuel PDG de Renault, Louis Schweitzer, 62 ans, directeur de cabinet de l'ancien premier ministre socialiste Laurent Fabius de 1984 à 1986.

Parmi les mis en examen comparaîtra aussi Paul Barril, 60 ans, ex-équipier de Christian Prouteau à l'Élysée et acteur central du scandale des Irlandais de Vincennes[92], l'arrestation en 1982 de prétendus dangereux terroristes, qui apparaîtra en fait comme une manipulation orchestrée par ses soins.

[92] En arrivant en 1981, François Mitterrand fait appel aux gendarmes du GIGN pour constituer sa garde présidentielle, plutôt qu'aux policiers. Le 29 août 1982, à 21 h 30, des membres du GIGN emmenés par le capitaine Paul Barril font irruption

Quant aux huit autres prévenus, il s'agit principalement des « opérateurs » de la cellule, de hauts gradés de la direction de la surveillance du territoire/contre-espionnage (DST), des renseignements généraux (RG) ou de la gendarmerie, directement chargés de ficher, écouter et retranscrire les conversations de leurs « cibles ».

Deux personnalités en particulier seront au cœur des débats devant le tribunal correctionnel, pour avoir fait l'objet d'une surveillance particulièrement serrée : le journaliste Edwy Plenel, aujourd'hui directeur de la rédaction du quotidien *Le Monde*, et l'écrivain Jean-Edern Hallier, décédé en 1997.

Selon l'accusation, le premier menaçait les intérêts du pouvoir par ses enquêtes, notamment sur l'affaire des Irlandais, le second par un chantage constant sur le locataire de l'Élysée, concernant principalement la révélation de l'existence de sa fille cachée, *Mazarine Pingeot*.

Le principal délit retenu à l'encontre des prévenus, « atteinte à l'intimité de la vie privée », leur fait encourir une peine maximale d'un an d'emprisonnement.

Le Monde (15 novembre 2004) « grandes oreilles de l'Élysée »

Vingt ans après les faits, le procès des « écoutes de l'Élysée » s'est ouvert lundi devant le tribunal correctionnel de Paris. Douze personnes, anciens collaborateurs du président François Mitterrand ou ex-militaires de haut rang, figurent dans le box des accusés.

Essentiellement poursuivis pour « atteinte à la vie privée », les 12 prévenus du procès des « grandes oreilles » de l'Élysée ont fait leur entrée au Palais de justice de Paris, lundi après-midi (15 novembre 2004).

Parmi eux, Christian Prouteau, 60 ans, ex-chef du GIGN et « patron » de la cellule antiterroriste de l'Élysée, a déclaré attendre « sereinement » l'issue du procès.

Son avocat, Me Francis Szpiner, a traité l'affaire, qui remonte à une vingtaine d'années, d'« archéologie judiciaire ». « On reproche à mon client d'avoir fait son devoir », a-t-il ajouté.

De son côté, Paul Barril, 58 ans, ex-équipier de Christian Prouteau, a simplement affirmé : « tout va bien se passer ». Son défenseur, Me Jacques Vergès, a dit attendre du procès que « sorte la vérité concernant tout le monde, même les plus haut placés : qui a ordonné, qui a manipulé tout ça en faisant porter le chapeau à d'autres ? ».

Les politiques convoqués

Lors des interrogatoires d'identité, les prévenus ont fait état de reconversions et de revenus disparates : Christian Prouteau est préfet sans affectation à 5.000 euros par mois, Louis Schweitzer touche 165.000 euros par mois de Renault, Paul Barril anime une société de sécurité privée et gagne 7.000 euros par mois.

Le tribunal de Paris a décidé d'entendre comme témoins les deux anciens Premiers ministres socialistes Pierre Mauroy (1981-1984) et Laurent Fabius (1984-1986) qui, s'étant déclaré « totalement étranger à cette affaire », ne souhaitait pas déposer. À la demande de la défense, les juges ont aussi convoqué Raymond Barre, Premier ministre de 1976 à 1981. Seront également entendus l'ex-ministre des Affaires étrangères Roland Dumas et Paul Quilès, ancien ministre de la Défense.

« Une lourde atteinte à un droit fondamental »

Les prévenus se voient reprocher d'avoir utilisé la « cellule antiterroriste » de l'Élysée pour faire écouter entre 1983 et 1986 les conversations d'environ 150 journalistes, écrivains, avocats et personnalités du show-business.

---

dans l'appartement d'un nommé Michael Plunkett, à Vincennes. Les gendarmes avaient apporté eux-même des explosifs dans l'appartement de Vincennes. C'est le début de l'affaire des *Irlandais de Vincennes*...

Après l'attentat de la rue des Rosiers, le commandant Christian Prouteau est chargé de coordonner la lutte anti-terroriste, après s'être vu confier, un mois plus tôt, la réorganisation de la sécurité présidentielle. Après les neuf mois de détention des Irlandais de Vincennes, libérés fin mai 1983, l'affaire des Irlandais de Vincennes est devenue celle des gendarmes de l'Élysée.

Deux personnalités « victimes » seront particulièrement au cœur des débats devant le tribunal correctionnel pour avoir fait l'objet d'une surveillance particulièrement serrée : le journaliste Edwy Plenel, aujourd'hui directeur de la rédaction du *Monde*, et l'écrivain Jean-Edern Hallier, décédé en 1997.

M. Plenel a indiqué qu'il avait « décidé de ne pas (s)'exprimer durant tout ce procès sauf devant le tribunal ». « Nous avons attendu 11 ans, 11 ans d'instruction. Tout le monde va se défendre, va argumenter, la justice se fait aux yeux de tous, ce n'est pas la peine que j'en rajoute », a-t-il dit. Il s'est porté partie civile et son avocat, Me Jean-Pierre Mignard, a estimé que « tous les Français comprendront l'enjeu de ce procès puisqu'il s'agit d'une lourde atteinte à un droit fondamental ».

Tf1 (17 novembre 2004) « Les petites oreilles » de l'Élysée à la barre

Au troisième jour du procès dit « des écoutes de l'Élysée » en correctionnelle à Paris, le président Kross s'est attaché à mieux connaître ses autres prévenus.

La veille, il avait entendu le chef, Christian Prouteau, à la tête du cabinet noir, cette cellule antiterroriste voulue par le président Mitterrand pendant son premier septennat. L'ancien patron du GIGN commandait alors une douzaine de personnes, aujourd'hui accusées d'avoir participé à un vaste système d'écoutes illégales sur de nombreuses personnalités dont le président de la République soupçonnait qu'elles le menaçaient.

Les excuses de la « secrétaire » font rire toute la salle

Prouteau et son numéro deux, le capitaine Barril, avaient alors constitué leur équipe. Un recrutement particulier, comme en témoigne par exemple le profil de Marie-Pier Sajous, 45 ans, une grosse dame dont personne ne se méfierait.

Comment cette ancienne étudiante en lettres a-t-elle bien pu passer d'obscure employée à l'Institut de dessalement de l'eau de mer à la cellule où elle était supposée faire des synthèses sur le terrorisme ?

« J'ai envoyé des CV », répond-elle. Le président cassant : « Ah oui, alors qu'on sait dans la procédure que votre père était militaire et que votre mère était secrétaire au ministère de la Défense, au GIC ! » Le GIC, fameux groupe interministériel de contrôle qui justement réalisait les écoutes...

« Mes parents ne parlaient pas de ça à la maison », lâche alors Marie-Pier Sajous, suscitant l'hilarité dans la salle tout entière. Nouvel éclat de rire quelques instants plus tard, lorsqu'on apprend au détour d'une question qu'elle était salariée de Gaz de France, comme d'autres membres de la cellule, qui bénéficiaient « d'emplois fictifs » de la Poste ou d'Air France.

« Et les lettres MP, MPier ou MPS, qui figurent sur nombre d'écoutes ? » insiste le président Kross, qui sait que les initiales apposées étaient celles des petites mains qui dépouillaient et analysaient les écoutes transcrites au GIC : « On a pu utiliser mes initiales », se défend-elle : « Je ne m'occupais que de dépouiller la presse, je faisais des photocopies d'articles pour des dossiers, c'est tout. »

« Et vous n'avez jamais vu passer une écoute ? » lui lance une avocate des parties civiles. La dame nie. Prouteau vole à son secours : « Elle ne devrait pas être là, elle n'était qu'une secrétaire », proteste-t-il.

Le Parisien, jeudi 18 novembre 2004, « Dès le départ, il y a eu des dérapages »

Comme une échelle un peu raide qu'on grimpe marche après marche, le président Kraus, qui dirige les débats du procès dit des écoutes de l'Élysée, essaie de comprendre la chaîne des responsabilités pour établir le rôle des douze prévenus, accusés d'avoir mis sur écoutes des dizaines de personnes, avocats, hommes politiques, journalistes et vedettes de cinéma, entre 1984 et 1986.

Hier (24 novembre 2004), il s'agissait de savoir ce « qu'en haut » on faisait exactement des branchements illégaux. C'est-à-dire à Matignon, lieu centralisateur de toutes les autorisations d'écoutes, où s'apposait la dernière signature, feu vert aux « grandes oreilles » du GIC (groupement interministériel de contrôle) chargé de l'enregistrement proprement dit.

Avant de recevoir les explications des deux « politiques » prévenus, à savoir Christian Delebarre et Louis Schweitzer, successivement directeurs de cabinet à Matignon, le tribunal a entendu l'ancien Premier ministre Pierre Mauroy, cité comme témoin.

Une audition instructive puisque l'on y a su que le « premier Premier ministre de François Mitterrand de 1981 à 1984 » avait appris à son proche collaborateur Delebarre « un petit jeu taquin ». « Lorsque mon directeur de cabinet est venu me voir, excédé par une demande d'écoutes de l'Élysée, je lui ai dit : « La première fois, tu ne réponds pas, la seconde non plus. Et à la troisième... bon ben, il y a une hiérarchie dans la République, on était obligés d'accepter », soupire Pierre Mauroy, en levant les bras avec l'air de celui qui en a vu d'autres.

Par exemple, accepter « sans plaisir » qu'après la vague d'attentats terroristes en France en 1982 son projet de loi sur la légalisation des écoutes soit abandonné (il sera repris par Rocard). Ou encore avaliser « avec réticence » la création de la cellule de Prouteau et Barril, que le témoin assassine d'un mot : « Dès le départ, il y a eu des dérapages, des dysfonctionnements manifestes ! »

Les responsables de toute cette affaire ? demande le président : « Ceux qui ont signé les cartons d'écoutes, qui ont voulu un branchement et qui doivent savoir expliquer pourquoi. Ne me faites pas le coup de la responsabilité du directeur des chemins de fer obligé de démissionner parce que le garde-barrière a provoqué un accident ! » tonne Mauroy, pour qui la responsabilité est clairement du côté des soutiers.

Louis Schweitzer : « Il y a eu un effort pour me masquer la réalité »

Puis vient le tour en soirée de Delebarre et Schweitzer, qui avaient par délégation la signature de Matignon sur cette délicate question des écoutes. Une tâche pas facile. « Lorsqu'il s'est agi de renouveler l'écoute de Jean-Edern Hallier, raconte pour sa part Louis Schweitzer, pour moi c'était un cas limite. Alors j'en ai parlé au Premier ministre, puis j'ai vérifié que c'était bien une demande du président de la République, en questionnant directement Jean-Louis Bianco à l'Élysée, je crois.

Lorsque j'ai eu la confirmation que c'était une demande du président, je me suis renseigné sur la légitimité des motifs. Puis j'ai autorisé le renouvellement. » Mais l'actuel PDG de Renault d'expliquer, amer, les limites du système : « Les motifs invoqués étaient parfois succincts : trafic d'armes ou proxénétisme. Et j'ai aussi l'impression que lorsqu'on a utilisé un autre nom que celui de la cible, c'était pour me tromper. Il y a eu un effort pour me masquer la réalité. »

Le Parisien, jeudi 25 novembre : Le commandant Beau tient sa revanche

Pour cette troisième semaine du procès dit des écoutes de l'Élysée, il sera fidèle au poste. Assis au deuxième rang, à droite, sur les bancs des victimes, le militaire à la retraite Jean-Michel Beau veille au grain. Pas une seule explication des témoins ou des prévenus ne lui échappe.

Et si d'aventure l'un d'entre eux avance une imprécision ou marque une hésitation, il se lève aussitôt, rectifie *in petto*. Le colonel a imposé au fil des audiences, qui doivent durer jusqu'en février, sa présence intempestive, sa large stature enveloppée de costumes gris, et sa grosse voix de fumeur de brunes. Le président Kross, qui mène les débats fermement, a bien compris qu'il avait là un « adjoint » de choix dans la recherche de la vérité. Ce qui ne l'a pas empêché de lui rappeler discrètement, par l'intermédiaire de son avocate, Me Courregé, qu'il lui fallait se montrer parfois moins agressif.

L'affaire des Irlandais de Vincennes refait surface

Il faut dire que cet ancien gendarme de 61 ans tient là une revanche trop longtemps attendue contre Barril et Prouteau, les principaux prévenus de ce procès, qui l'ont manipulé dans la fameuse affaire des Irlandais de Vincennes, première dérive des deux super-gendarmes de l'Élysée.

À l'époque, en 1982, le commandant Beau, de la section de recherches de Paris, est appelé sur les lieux lors de l'arrestation de trois terroristes de l'Inla[93] dans un appartement de Vincennes, opération

[93] *Irish national liberation army* (Armée irlandaise de libération nationale) est une dissidence marxiste de l'Irish Republican Army (Ira, l'Armée républicaine irlandaise). Elle est apparue en 1975.

menée par Barril. À la demande pressante du duo alors tout auréolé de sa proximité avec le président Mitterrand, et parce qu'il croit faire son devoir de militaire, Beau accepte de cacher à la justice le fait que la perquisition ne s'est pas déroulée dans les formes procédurales.

Il ignore alors que l'interpellation elle-même et les armes saisies étaient un coup monté par le capitaine Barril, qui avait lui-même déposé l'arsenal dans l'appartement. Résultat de cette bavure gendarmesque ? Prouteau relaxé, Barril jamais poursuivi. Seul le soldat Beau, le « cocu », comme il l'a dit alors, trinque : douze mois avec sursis. Carrière brisée, déshonneur assuré, ce fils de militaire plonge dans l'amertume. Et il enquête — ce qui lui vaut semble-t-il de faire partie des « écoutés » de la cellule — pour découvrir la vérité sur les Irlandais de Vincennes, qui finit par éclater dans la presse, à défaut de venir dans les prétoires.

Pour voir Prouteau et Barril rendre des comptes à la justice, Beau devra attendre des années que le « dossier des écoutes », autre gros scandale lié à la cellule, arrive enfin devant des juges. Il tient donc aujourd'hui sa dernière « chance » : voir ses anciens compagnons d'armes répondre de leurs actes. Son honneur depuis longtemps perdu lui donne des ailes, il connaît le dossier par cœur : ses questions incisives, documentées, fouillent dans la mémoire de ceux qui viennent à la barre.

Mercredi dernier, l'audience a fait un saut décisif. Le témoin du jour, outre l'ancien Premier ministre Mauroy, était surtout le capitaine Marie, qui suivait les autorisations d'écoutes à Matignon et qui s'est souvenu que la production de la cellule était vraiment faible, ne se rappelant avoir vu presque aucun nom de la longue liste des « écoutés ». Laissant entendre que la cellule avait mis au point un circuit pour déjouer les procédures habituelles.

Beau a préparé ce procès comme si sa vie s'y jouait. C'est un peu ça d'ailleurs. Il n'est sorti de la dépression qui le ronge que pour assister à la dernière scène d'un drame qui l'a broyé il y a vingt ans et obtenir enfin la vérité. On ne se méfie jamais assez d'un militaire injustement humilié.

Le Parisien, lundi 29 novembre 2004, Écoutes : Quilès n'a rien vu, rien entendu

Au procès sur les branchements élyséens, l'ex-ministre de la Défense se défausse.

Ministre de l'Equipement envoyé à la Défense le 20 septembre 1985, Paul Quilès découvre des « constructions particulières » sur les lignes téléphoniques des terroristes ou des trafiquants d'armes. Mais pas seulement.

Jean-Claude Kross, le président du procès des écoutes de l'Élysée, a rappelé hier à ce prétendu « novice » en la matière, qui signe sans barguigner « des piles de fiches » d'autorisation, que les « constructions » interdites sur les avocats, les journalistes et parlementaires ont été édifiées en masse sous son règne de six mois, achevé le 20 mars 1986. Joël Galipapa et Gérard Ecorcheville, amis politiques de Charles Pasqua, ont été espionnés avant l'alternance, les journalistes Edwy Plenel, Hervé Brusini, Michel Cardoze et Jean-Marie Bourget ont été souvent surveillés pour traquer les auteurs de fuites dans l'affaire Greenpeace.

Mais Paul Quilès n'a rien vu, rien entendu.

Il a débarqué « à l'improviste » à la Défense pour remplacer Charles Hernu, limogé à cause du sabotage par des agents de la DGSE du bateau de Greenpeace en Nouvelle-Zélande, « sans connaître ce milieu » et sans un brin de curiosité. Paul Quilès se familiarise vite fait avec les us et coutumes de la Maison, chausse les bottes de son prédécesseur Hernu, apprend du chef du bureau réservé de son ministère que vingt lignes d'écoute sont dévolues à l'Élysée, sans s'en étonner outre mesure et sans même soi-disant connaître l'existence de « la cellule » : « Sur le coup, j'ai pris le système tel qu'il était. Mes préoccupations majeures étaient l'état de déliquescence de la DGSE et le rapatriement des deux agents de Nouvelle-Zélande. »

Sondages.

Donc, « dix minutes à un quart d'heure par semaine », le ministre de la Défense Quilès paraphe à la chaîne les demandes d'écoute de ses services et de « l'Élysée », et « pose de temps en temps une question

par sondage pour savoir pourquoi » telle ou telle personne « inconnue » de lui se retrouve surveillée. Sans plus. Il ignore que la construction au nom de Lapierre visait Edwy Plenel qui a révélé dans *le Monde* l'existence de « la troisième équipe » de la DGSE ayant coulé le Rainbow Warrior.

Une note de son bureau réservé retrouvée dans les archives de Christian Prouteau, ex-chef de la cellule, indique pourtant que « M. Plenel vit avec Mme Lapierre », souligne Me Francis Szpiner. Mais cela aussi a échappé à Quilès. Sinon, il aurait « fait cesser » ce branchement « instantanément ».

Jean-Edern Hallier.

Il n'est pas plus au courant de « la maladie de François Mitterrand et de l'existence de Mazarine » : « J'ai appris tout cela par la presse », rétorque ce témoin fort mal tuyauté pour un ex-ministre des services secrets.

La révélation imminente de la vie privée du Président par Jean-Edern Hallier a pourtant suscité des écoutes tous azimuts sur l'écrivain. Dans l'hypothèse où Paul Quilès serait responsable de quelque chose dans ces affaires de plomberie et de constructions, ce serait éventuellement « de [sa] signature », dit-il. À l'en croire, il s'agit d'une simple formalité, d'un gribouillis au bas d'un carton blanc qui... permet des écoutes : « C'est un des éléments, un des maillons de la chaîne », minimise-t-il. Certes, feu son prédécesseur Charles Hernu ne s'est pas contenté de jouer au sourd et à l'aveugle, signant à tour de bras et approuvant en connaissance de cause tous les desiderata de la cellule présidentielle ou de son complice François Mitterrand.

Mais Hernu et Mitterrand ne sont plus.

Et Quilès se défausse. Me Olivier Metzner, qui défend Pierre-Yves Gilleron, ancien de la DST reconverti à la cellule, toujours bouche cousue par le secret défense, ne comprend pas bien : « Vous avez une aversion pour les écoutes, pourquoi n'avez-vous pas cherché à contrôler plus ? » « Vous n'imaginez pas l'emploi du temps d'un ministre de la Défense ! » Les douze prévenus pour « atteinte à l'intimité de la vie privée » boivent du petit-lait et ironisent en aparté : « Bel exemple de courage politique ! »

Liberation, mercredi 01 décembre 2004, Écoutes : au service secret de sa majesté Mitterrand

Le général Esquivié, alias Aramis, a nié toute activité répréhensible.

Les « mousquetaires » de l'Élysée qui ont espionné des gens de la presse, du barreau, de la politique et du spectacle pour le compte de François Mitterrand de 1983 à 1986 manquent de panache. Vingt ans après l'épopée tragi-comique de la « cellule » dite antiterroriste installée à demeure rue de l'Élysée par le président de la République, les huit anciens serviteurs du « roi » jugés pour « atteinte à l'intimité de la vie privée » entretiennent encore un indécrottable culte du secret, même sur des combines minables et des pseudo bidons.

Ainsi, le général Jean-Louis Esquivié, 63 ans, habit gris passe-muraille, cheveux crantés poivre et sel, refuse encore d'admettre qu'il a signé *Aramis* une tribune dans *le Monde* en 1985, plaidoyer pro domo en faveur de la police parallèle de l'Élysée : « Il s'agit bien d'une nouvelle aventure des légendaires mousquetaires, écrivait Aramis. Ils servaient le roi, ils servent aujourd'hui le chef de l'État. Ils étaient chassés par les gardes du cardinal, ils sont aujourd'hui la cible de tous ceux que le pouvoir du Président dérange [...] Ils étaient fidèles, ils sont aujourd'hui toujours fidèles, n'ont aucun état d'âme [...] » Il comparait la cellule à « la cote de maille du Président », à un indispensable « entourage-rempart ».

Riposte.

Patelin mais mordant, l'homme de robe Jean-Claude Kross, qui préside à Paris le procès des écoutes de l'Élysée, croise le fer avec Aramis. Quatre prévenus ou témoins, son supérieur Prouteau, le capitaine Barril, le général Gervais et même le journaliste Edwy Plenel ont désigné Esquivié. « Je sais comment a été construit le texte mais je ne suis pas propriétaire d'Aramis, M. Plenel peut se tromper comme sur le financement du PS », riposte Esquivié.

Voilà que son voisin à l'audience, Gilles Ménage, accusé lui aussi d'écoutes illégales, le dénonce sur-le-champ. L'ex-directeur de cabinet de François Mitterrand explique qu'à l'époque il avait été pris à tort pour Aramis, et qu'il avait essuyé les « reproches épouvantables » du ministre de l'Intérieur, Pierre Joxe. « Je pense qu'Aramis se trouve à côté de moi », accuse Gilles Ménage. Le président jubile, « cinq à zéro, monsieur le général Esquivié », et sort du dossier d'autres « détails » qui, mis bout à bout, attestent le rôle majeur de Jean-Louis Esquivié, numéro 2 de la cellule et chef de l'informatique.

Fiches.

À la barre, Aramis sert des explications fumeuses : il travaille dans le bureau de Christian Prouteau « à cause du manque de place ». Il ratifie des ordres de mission et des demandes d'écoute : « J'ai signé les yeux fermés et par gentillesse pour mes camarades, en l'absence de Prouteau. » Sans rien regarder du tout. Il n'a pas non plus installé le logiciel Filing d'IBM[94] à la cellule pour intégrer les transcriptions d'écoutes téléphoniques et ficher les gens par centaines en 1983.

Pourtant, dans une note datée du 27 avril 1984 et exhumée des archives de Prouteau, la cellule demande à l'Élysée une audience pour le dirigeant d'IBM qui « a élaboré son informatique gracieusement, efficacement et dans la plus grande discrétion ». Esquivié n'en démord pas. L'informatique, ce n'est pas son truc. Lui, il multiplie les missions de lutte antiterroriste, monte des « opérations très secrètes » en Corse et au Pays Basque, œuvre à la libération des otages français au Liban : « J'ai rencontré tout ce qui bouge, le chef du Hezbollah, le patron des pasdarans, négocié dans la plaine de la Bekaa, ramené des messages en arabe pour le Président, et ça, c'est écrit nulle part, j'ai même une petite blessure au pouce. »

« Actif ».

Le mousquetaire se fait moins flamboyant lorsqu'il s'agit de répondre de la protection à outrance de la vie privée du chef de l'État et de « la tranquillité personnelle de Mme Mitterrand », dixit le président Kross, de sa note sur l'homme politique Philippe de Villiers (« un Rastignac de province »), de ses « dîners » hebdomadaires avec Jean-Edern Hallier et de ses signatures pour reconduire des branchements interdits. Le président le sermonne : « On attend de serviteurs de l'État la vérité d'un dossier, vous devez ça à votre justice, si on cumule tous ces éléments, vous n'êtes pas un obscur et un sans-grade. » Esquivié : « Il n'y en avait aucun à la cellule. Je me suis investi un maximum. » « Vous aviez un rôle important. » « Actif », corrige Aramis. « Quelle affaire de haute trahison de l'État alliez-vous traiter ? » demande le

[94] Révélée par Hervé Gattegno, l'affaire est digne d'un scénario de film policier. Mi-janvier, donc, une femme se présente devant les grilles du Palais de Justice de Paris et remet à un gendarme en faction une enveloppe à l'attention du juge chargé du dossier des « écoutes de l'Élysée », qui, un mois auparavant, a mis en examen, pour « atteinte à la vie privée » Gilles Ménage, ancien directeur de cabinet du président de la République et actuel président d'EDF ; le préfet Christian Prouteau, ancien chef de la cellule antiterroriste de l'Elysée ; le général de gendarmerie Jean-Louis Esquivié ainsi que le capitaine Pierre-Yves Guézou et l'ancien commissaire de la DST Pierre-Yves Gilleron.

À l'intérieur de l'enveloppe, le magistrat instructeur — bien en peine, malgré tout, de détenir des éléments imparables sur les pratiques de la cellule —, trouve 5 disquettes d'ordinateur portant chacune la mention « backup », et étiquetées de 1 à 5. Le 16 janvier, il confie à un expert informaticien la tâche de les décrypter. Ce qui ne va pas le plus simplement du monde, car leur contenu n'est pas directement lisible à l'aide d'outils logiciels standards ou de grande diffusion. Le juge Valat doit alors se souvenir d'une information rapportée par « *le Monde* », partie civile dans cette affaire après que l'un de ses journalistes, Edwy Plenel, eut été écouté. Il suggère à l'expert de recourir à un programme de traitement de texte élaboré par IBM, le logiciel *Filing*, utilisé par la cellule pour enregistrer ses données.

Miracle des technologies : là, grâce à *Filing*, l'expert voit apparaître sur son écran d'ordinateur 5.184 fiches, réparties en 26 fichiers, dont 23 sont constitués d'écoutes téléphoniques concernant autant d'individus. Selon le rapport d'expertise, « la quasi-totalité de ces fichiers auraient été créés avant le 25 octobre 1985, et au plus tard le 21 mars 1986 ». La thèse du maquillage, invoquée par les différents protagonistes de l'affaire depuis la publication, dans « *Libération* », de 16 comptes-rendus d'écoutes effectuées par ce service, prend un sérieux coup dans l'aile. Elle est carrément anéantie. Difficile maintenant de soutenir qu'il s'agit d'une grossière manipulation tendant à discréditer le gouvernement socialiste de l'époque, en lui attribuant des pratiques de fichage politique.

président. Aramis baisse la garde : « Plenel. Heuh, je ne devrais pas dire cela, Farewell » (du nom d'une taupe au sein du KGB).

Une révélation : « Actez, Mme la greffière ». Fine mouche, maître Christine Courrégé, pour une partie civile, demande à Esquivié « si la question de Mazarine relevait du secret défense ». Affirmatif : « Le souci d'un père pour sa fille, ça, c'est de l'intimité. Imaginez un chantage sur le Président qui peut déclencher l'atome, l'arme nucléaire, oui, ça relève du secret défense. » L'avocate du gendarme Beau, lui aussi victime d'écoutes, décoche une dernière flèche : « Vous n'avez pas eu l'occasion de vous poser des questions sur les limites ? »

Remercié pour ses bons et loyaux services à la cellule présidentielle par un galon de général de division, Esquivié persiste et signe : « Non. Je n'ai jamais douté personnellement ».

Libération, vendredi 03 décembre 2004, Écoutes de l'Élysée : Joxe charge Mitterrand et pleure

L'ex-ministre de l'Intérieur puis de la Défense témoignait hier au procès. Tout d'un coup, Pierre Joxe s'est mis à sangloter.

L'ancien ministre de l'Intérieur puis de la Défense de François Mitterrand est interrogé comme témoin par Me Olivier Metzner, avocat de l'un des anciens membres de la cellule antiterroriste de l'Élysée, en quatrième semaine du procès des écoutes.

Jusque-là, Joxe avait fait du Joxe. Politique, critiquant Mitterrand tout en faisant mine de respecter sa mémoire : « Occasionnellement, il recommandait de respecter la loi. (...) J'ai essayé parfois de l'empêcher de commettre des choses illégales, sans réussir, mais le pourcentage est faible. » Erudit, citant Sophocle : « Il existe des lois ineffaçables mêmes si elles ne sont pas écrites. » Protestant rigoureux : « Cette cellule ne pouvait provoquer que des ennuis, et on aimerait employer un autre mot. »

Mais on s'attendait à tout sauf à ce que Pierre Joxe verse une larme au terme de sa déposition. On en était à une digression sur l'affaire Ben Barka, indépendantiste marocain enlevé en 1963. Joxe évoque son karma personnel, son père Louis, ministre de De Gaulle, lui jeune militaire chargé de renseignements. « Ben Barka, je l'avais vu quelques jours avant sa mort. J'aurais pu l'éviter, car j'avais des informations. Le Sdece [les services secrets, rebaptisés DGSE] faisait ce qu'il voulait. C'est en me rappelant le passé que je sais qu'un service de renseignement, s'il n'est pas tenu, peut mal tourner. »

« Système bâtard »

Auparavant, Joxe était revenu sur la création en 1982 de la cellule de l'Élysée, composée de policiers et de gendarmes en dehors de tout cadre légal. « J'ai prévenu Mitterrand que ce système était bâtard, tordu, parallèle, sans hiérarchie claire. » Il dit son peu de goût pour les écoutes téléphoniques : « Il est tentant de s'en servir, tentant d'en abuser. » Charge la barque : « Il n'y a pas seulement les écoutes, mais l'archivage des fichiers ; là, c'est contraire à toute déontologie policière. » Revient sans cesse à l'ancien président de la République : « C'est malheureux à dire, mais ce truc a été organisé par Mitterrand. »

Le tribunal visite l'histoire sombre du mitterrandisme, notamment l'affaire du *Rainbow Warrior,* bateau de Greenpeace coulé en 1985 à Auckland (Nouvelle-Zélande) par des agents de la DGSE, avec mort d'homme à la clé (un photographe portugais de l'association écologiste, en lutte contre les essais nucléaires français dans le Pacifique).

Pierre Joxe revient sur la personnalité de Charles Hernu, ministre de la Défense en perdition : « Un vieil ami qui a perdu la tête. Je lui disais pourtant que les services spéciaux, par construction, peuvent conduire à des bavures, qu'il y en avait déjà eu dans le passé et qu'il y en aurait encore. Contre tout bon sens, de bonne ou mauvaise foi, Hernu a tout nié en public. »

Joxe relate son propre rôle au ministère de l'Intérieur : « On a su très vite que la DGSE était dans le coup. C'est malheureux à dire, mais je m'occupais de retarder les mesures d'identification de nos agents. » Il n'est pas peu fier des résultats de son « inertie feinte » vis-à-vis des autorités néo-zélandaises : « D'autres [agents] n'ont pas été arrêtés. »

Le tribunal cherche surtout à savoir en quoi l'affaire Greenpeace, après l'affaire des Irlandais de Vincennes, a motivé l'écoute de journalistes en charge de ces affaires qui fâchent, la cellule de l'Élysée, délaissant sa mission initiale antiterroriste, se focalisant désormais sur la traque des fuites.

Joxe joue sa propre partition : « L'important, ce n'était pas les fuites, mais les faits. Un mort, un crime » Justement, il est soupçonné, à tort ou à raison, d'avoir informé la presse au nom d'une sombre manœuvre intragouvernementale. Joxe réfute l'honneur : « Il était fatal que l'affaire Greenpeace soit totalement publique un jour.» Il évoque pourtant ses liens avec Edwy Plenel, journaliste au *Monde* qui a levé de nombreux lièvres sur ces affaires. « Il écrivait alors du bien de ma politique policière, mais ce n'est qu'ultérieurement qu'on est devenus amis. »

Mousquetaires

Retour sur certaines obsessions de François Mitterrand : « Pour des raisons que je n'ai jamais pu éclaircir, il était braqué contre Plenel, enragé contre *le Monde*. François Mitterrand, malgré tout mon dévouement à son égard, a quand même commis quelques erreurs dans sa vie.

À cette époque, il avait une mentalité obsidionale contre tout ce qui était imprimé dans la presse, pour des raisons politiques et personnelles. C'était pourtant contraire à tout ce qu'était et nous disait François Mitterrand, ancien avocat. Une part d'ombre. » Puisqu'il est question d'obsession, Pierre Joxe en revient à la sienne, en concluant sur la cellule de l'Élysée : « On ne peut pas concilier efficacité policière et respect des droits de l'homme avec une équipe de mousquetaires. C'est incompatible. »

Libération, 23 février 2005 Le procès des écoutes de l'Élysée, Les oreilles de Mitterrand ne rougissent pas

Défense, hier à Paris, de Christian Prouteau, ancien chef de la cellule.

Pour Christian Prouteau, Me Francis Szpiner a plaidé hier « l'honneur du soldat » contre « la lâcheté de l'État et l'hypocrisie du parquet ». Le procès des écoutes devant le tribunal correctionnel de Paris s'est achevé avec la défense de l'ancien chef de la cellule élyséenne, jugé pour 33 écoutes illégales entre 1983 et 1986.

Dans sa plaidoirie, Me Szpiner dénonce l'absence sur les bancs des prévenus de Pierre Mauroy et Laurent Fabius, anciens Premiers ministres ; il parle même de ces morts qui ont « joué un rôle central, François Mitterrand et Charles Hernu », ex-ministre de la Défense. Ne reste donc que le commandant de gendarmerie Prouteau, « homme de devoir et de courage », chargé d'une « mission » de lutte contre le terrorisme en 1982, après l'attentat de la rue des Rosiers. « Il ne s'agit pas d'une structure illégale ou d'une police parallèle, Prouteau a été régulièrement installé à la présidence de la République et a reçu 20 lignes d'écoutes sur les 924 effectuées au GIC », le centre officiel du gouvernement. Un petit nombre de lignes « facile à contrôler » par Matignon, qui signe les demandes d'autorisation de branchement. Il conteste tout détournement de procédure pour abuser les services des Premiers ministres successifs. Il ne voit « pas de dissimulation » des véritables identités des « cibles » d'écoutes lorsque la cellule indique les noms de leurs compagnes, Nicole Lapierre pour masquer le journaliste Edwy Plenel ou Blandine Vecten pour l'avocat Antoine Comte, « mais parce qu'elles sont titulaires des lignes ».

« Pas écouté, ni enregistré, ni transmis »

Très en verve, Me Szpiner dégaine un argument juridique massue. Poursuivi pour « atteinte à l'intimité de la vie privée », Christian Prouteau n'a pourtant « pas écouté, ni enregistré, ni transmis » de transcriptions, ce que punit le Code pénal, « c'est le GIC, c'est l'État qui l'a fait, Prouteau n'avait pas le casque sur les oreilles ». Il a certes demandé des branchements aux directeurs de cabinet de Matignon qui les ont signés et permis. « Il n'est pas complice par fourniture de moyens ni par instructions données », assène Szpiner, pour qui « les poursuites auraient dû être engagées » pour l'exploitation et la conservation de documents issus d'écoutes illégales.

« Car, en 1993, tout était prescrit »

Il évoque la question de la prescription qui se pose pour les multiples branchements de Jean-Edern Hallier jusque dans son bistrot de la place des Vosges et son restaurant de prédilection, *la Closerie des Lilas*. Car les conversations téléphoniques piégées du polémiste indiquent « non seulement qu'il se savait écouté », a souligné mardi Me Olivier Metzner, avocat de Pierre-Yves Gilleron, membre de la cellule, « mais aussi par qui ». L'écrivain provocateur contacte en effet, en 1983, le colonel Gervais, discrètement chargé à Matignon de réceptionner les comptes rendus d'écoutes, pour s'entretenir avec lui de ce sujet qui le vise directement. Une affaire de date essentielle, car, en matière d'atteinte à l'intimité de la vie privée, la prescription démarre le jour où la victime apprend le délit. Or, feu Jean-Edern Hallier n'a déposé plainte qu'en 1993, après la révélation du scandale par *Libération*. Tout comme le journaliste du *Monde*, Edwy Plenel.

À son tour, Me Patrick Maisonneuve, pour l'ex-directeur de cabinet adjoint de l'Élysée Gilles Ménage, a recensé « 23 interceptions » de Plenel en 1984 et 1985, « permettant de penser raisonnablement que M. Plenel est informé de l'écoute ». Ainsi, l'investigateur explique à sa compagne : « Ménage, c'est le conseiller de Mitterrand, c'est celui qui nous écoute là. »

Or, si l'enquêteur du *Monde* et le polémiste Hallier se savaient espionnés à l'époque, ils auraient dû porter plainte dans un délai de trois ans, « car, en 1993, tout était prescrit ». Au fil des 32 audiences, Plenel a objecté que ces allusions au téléphone ont valeur de « plaisanteries », qu'il n'y croyait « pas vraiment ».

Troisième problème.

Edwy Plenel s'est désisté en fin de procès de sa plainte contre Louis Schweitzer, ancien directeur de cabinet à Matignon. Une bourde juridique. Me Szpiner s'en empare et signale que, dans deux cas, « la diffamation et l'atteinte à la vie privée », ce sont les plaintes des victimes qui déclenchent les poursuites, pas le procureur. Le retrait de plainte de Plenel à l'égard d'un prévenu entraîne, selon lui, « l'extinction de l'action publique à l'égard de tous ses coauteurs et complices ». Contre les douze qui risquent aujourd'hui entre quatre et douze mois de prison avec sursis, assortis d'amendes.

Libération, Novembre 2005 Le procès des écoutes de l'Élysée

Prison avec sursis pour les grandes oreilles de Mitterrand

Pour le tribunal correctionnel de Paris, c'est l'État qui doit être tenu pour responsable.

Faute de pouvoir condamner François Mitterrand en personne, le tribunal correctionnel de Paris a distribué hier des peines symboliques aux anciens membres de la cellule de l'Élysée.

De la prison avec sursis pour ses principaux responsables (huit mois pour le commandant Prouteau, six mois pour le général Esquivié, trois mois pour le commissaire Gilleron), relaxe pour les moins gradés.

Dans la même veine, deux anciens directeurs de cabinet à Matignon, Michel Delebarre et Louis Schweitzer, sont condamnés, mais dispensés de peine.

Décédés.

Rendant à César ce qui lui appartient, le jugement est très clair : « Les faits ont été commis sur ordre soit du président de la République, soit des ministres de la Défense » (notamment Charles Hernu, également décédé). Mieux, il précise que les éventuels dommages et intérêts dus aux victimes d'écoutes sauvages devront être réclamés devant le tribunal administratif, les fautes commises par la cellule n'étant « pas détachables du service », compte tenu de sa « soumission à la volonté présidentielle ».

C'est donc l'État (donc les contribuables) qui devra réparer les basses œuvres mitterrandiennes.

L'ancien directeur de cabinet de Mitterrand, Gilles Ménage (six mois avec sursis), est le seul de son entourage à payer.

Le tribunal a également réduit considérablement le nombre de personnes placées sur écoute téléphonique (150 personnes et 1 368 interlocuteurs, dont de nombreux journalistes) pouvant exiger répara-

tion. Son jugement note bien « le caractère intolérable d'une réelle atteinte à la liberté de presse du fait de la dérive de la cellule de l'Élysée », théoriquement chargée de la lutte antiterroriste, mais de plus en plus obsédée par ce qui se disait de Mitterrand dans les journaux.

Cela ne relèverait pas d'une atteinte à l'intimité de la vie privée (le délit formellement poursuivi), mais seulement d'une ingérence dans leur activité professionnelle.

Au final, seuls quatre écoutés ont été retenus, avec leur proche entourage respectif: l'avocat Antoine Comte, défenseur des Irlandais de Vincennes, le pamphlétaire Jean-Edern Hallier, qui menaçait de révéler l'existence de Mazarine, le journaliste du *Monde* Edwy Plenel, en pointe dans l'affaire Greenpeace, et Joël Galipapa, collaborateur de Charles Pasqua aujourd'hui décédé.

Ce tri sélectif fait hurler Jean-Michel Beau, ancien colonel de la gendarmerie, partie civile, qui crie vengeance « depuis vingt-trois ans », plongeant seul dans l'affaire des Irlandais pour avoir protégé d'anciens membres de la cellule.

Sa voix de ténor a brusquement interrompu la lecture du jugement : « Je sors de la salle devant cette injustice inique et je vous emmerde. Poursuivez-moi donc pour outrage à magistrat. » Dans les couloirs, le général Esquivié philosophe : « Tout agent qui travaille dans l'antiterrorisme doit accepter de se retrouver un jour devant un tribunal. On devrait l'apprendre aux nouvelles recrues. »

Venger.

Le grand perdant est le capitaine Barril, condamné à six mois de prison avec sursis. On lui reproche d'avoir voulu se venger de la cellule, avec laquelle il était en conflit, en piratant sa mémoire informatique sous forme de disquettes et en la diffusant anonymement (dans la presse et auprès du juge d'instruction) pour se venger.

Les juges n'ont pas de preuve formelle contre lui, le parquet ayant même requis la relaxe. Ils se sont quand même fait une religion fondée sur ses « mensonges manifestes qui ne peuvent avoir pour finalité que de tromper le tribunal ».

Libération, jeudi 10 novembre 2005, Écoutes téléphoniques : les leçons d'un procès

Après trois mois d'audience, le procès des écoutes téléphoniques touche à sa fin. Entre dénégations et faux semblants, les débats auront permis d'établir quelques vérités sur l'histoire de la fameuse cellule antiterroriste de l'Élysée.

Comme l'affaire du Watergate, le scandale des écoutes montre donc à quel point les contrôles hiérarchiques et administratifs sont nécessaires dès lors qu'il s'agit de protéger l'exécutif du pouvoir (sans limites ?) qui l'anime. Mais le parallèle s'arrête là. En France, ni la presse, ni les parlementaires, ni les juges n'ont été en mesure de mettre en cause les politiques. Comme si l'avertissement lancé en 1965, dans le *Coup d'État permanent*[95], restait valable quarante ans plus tard. En dénonçant le cabinet noir du général de Gaulle, François Mitterrand constatait : « Ce qui sort en surface est peu de choses au regard de ce qui reste caché. »

Le jugement

Douze ans après l'ouverture de l'enquête judiciaire, le Tribunal correctionnel de Paris, dans son jugement du 9 novembre 2005, a exposé les motivations de sa décision judiciaire :

[95] Dans ce livre, F. Mitterrand dénonce la pratique du pouvoir personnel par le général de Gaulle. Il ne se contente pas de critiquer la lettre de la Constitution : il reprocherait plutôt au général de Gaulle d'avoir trahi la promesse de 1958, selon laquelle le président est un arbitre. Le chef de l'État est devenu tout-puissant. Il montre la faiblesse du gouvernement et du Parlement, marginalisés par le président de la République. François Mitterrand insiste aussi sur les abus en matière de justice et de police. Il dénonce par exemple l'utilisation de provocateurs, la multiplication des bavures et brutalités policières, les officines en tous genres (comme le SAC et les réseaux Foccart), les tribunaux d'exception (la Cour de sûreté de l'État, supprimée dès l'été 1981 par la gauche), le mépris du Conseil constitutionnel et du Conseil d'État, le recours abusif au délit d'offense au chef de l'État, etc.

Le tribunal releva ainsi que le président François Mitterrand s'était montré soucieux de protéger divers éléments de sa vie personnelle, notamment l'existence de sa fille naturelle Mazarine Pingeot (dont l'écrivain Jean-Edern Hallier, menaçait de révéler l'existence si le président n'effaçait pas son lourd redressement fiscal) — voire, selon la dépêche de l'agence *Reuters* rapportant la décision judiciaire, le cancer diagnostiqué fin 1981 et son passé à Vichy pendant la guerre (affirmations qui n'avaient pas paru jusqu'alors). C'est pour des « motifs obscurs » (dixit le tribunal) également que le compagnon de Carole Bouquet est écouté à cause de ses relations au Proche-Orient tout comme Edwy Plenel, journaliste au Monde ou encore l'avocat Antoine Comte.

Dans ses attendus, le tribunal a encore pointé du doigt François Mitterrand : « Les faits avaient été commis sur ordre soit du président de la République, soit des ministres de la Défense successifs qui ont mis à la disposition de (Christian Prouteau) tous les moyens de l'État afin de les exécuter ».

Selon le Tribunal, François Mitterrand a été « l'inspirateur et le décideur de l'essentiel ». Le dossier a montré que le ***président avait ordonné lui-même certaines écoutes et avait laissé faire pour d'autres***.

Le tribunal néanmoins souligna que les autres écoutes administratives réalisées par les services secrets et la police n'avaient pas plus de cadre légal que celles de la cellule antiterroriste.

Sept anciens collaborateurs du président sont finalement condamnés dont :

— Gilles Ménage, ex-directeur de cabinet adjoint (six mois de prison avec sursis et 5 000 euros d'amende pour « atteinte à l'intimité de la vie privée »)

— Christian Prouteau, dirigeant de la cellule antiterroriste (huit mois de prison avec sursis et 5 000 euros d'amende)

— Louis Schweitzer, ancien directeur de cabinet de Laurent Fabius à Matignon, pour le placement sur écoutes de l'écrivain Jean-Edern Hallier (dispensé de peines)

— Michel Delebarre, ex-directeur de cabinet de Pierre Mauroy à Matignon, pour le placement sur écoutes de l'écrivain Jean-Edern Hallier (dispensé de peines)

— l'ancien gendarme Paul Barril, condamné pour le recel des données secrètes de la cellule à six mois de prison avec sursis et 5 000 euros d'amende.

Quatre autres employés de la cellule ont été relaxés ainsi que le général Pierre Charroy, patron de 1982 à 1999 du Groupement interministériel de contrôle (GIC), organisme qui réalise pour le compte du gouvernement l'ensemble des écoutes téléphoniques administratives (extrajudiciaires).

Seules sept parties civiles sont ainsi reconnues comme victimes parmi lesquelles l'ex-journaliste du *Monde* Edwy Plenel, en pointe dans l'affaire *Greenpeace*, l'avocat Antoine Comte, défenseur des Irlandais de Vincennes, Jean-Edern Hallier (décédé) ainsi que sa famille et Joël Galipapa (décédé), collaborateur de Charles Pasqua aujourd'hui décédé alors que 22 autres plaintes sont jugées infondées dont celles des journalistes Hervé Brusini et Michel Cardoze et celle de l'actrice Carole Bouquet.

Par ailleurs, le tribunal déclara que les fautes n'étaient pas « détachables du service de l'État ».

Aucune partie n'ayant fait appel du jugement, il a eu force exécutoire, mais les sanctions seront amnistiées en vertu de la loi votée après l'élection présidentielle de 1988, et donc non inscrites au casier judiciaire, si les condamnés paient les amendes.

Constantin Melnik, conseiller de Michel Debré à Matignon, qui coordonna les services secrets entre 1959 et 1962 expliqua en octobre 1996 dans *Le Monde* que les écoutes pratiquées sous François Mitterrand lui apparaissaient comme « des jeux d'enfants improvisés par rapport à ce qui était pratiqué systématiquement durant les premières années de la V^e^ République », en pleine guerre d'Algérie.

Le 13 mars 2007, la Cour d'appel de Paris a accordé à l'actrice Carole Bouquet un euro de dommages et intérêts et au lieutenant-colonel Jean-Michel Beau 5.000 euros, pour atteinte à l'intimité de leur vie privée dans cette affaire

Djokhar Doudaev tombe dans le piège

Le 9 avril 1996, cela fait presque seize mois que la sale guerre de Tchétchénie se poursuit dans le Caucase, lorsque Djokhar Doudaev, ex-général de l'Armée rouge et dirigeant de la résistance tchétchène, annonce à quelques journalistes réunis pour une conférence de presse improvisée dans les montagnes du sud de la Tchétchénie, qu'il n'est disposé à négocier qu'avec le président Bons Eltsine lui-même. Il va être entendu... Dans la nuit du 20 au 21 avril, il réunit quelques fidèles dans une ferme du village de Gekhi-Tchou où il attend une communication, par téléphone satellitaire, avec l'un des médiateurs proposés par Bons Eltsine. A l'heure prévue pour cette communication, ses gardes du corps déploient, dans un champ proche de la ferme, l'antenne parabolique nécessaire à l'établissement de la communication. Quelques minutes plus tard, Doudaev est tué dans un bombardement.

Depuis le début de la guerre, le FSB cherchait le moyen d'éliminer le rebelle. Plusieurs tentatives d'assassinat s'étaient déjà soldées par un échec, mais les hommes de la Loubianka ne renoncent jamais. Et, une nuit de printemps, leur heure était enfin venue. Chamil Bassaeiv, l'un de ses adjoints, responsable des forces spéciales de la résistance tchétchène, prétendra quelques jours plus tard que ce sont des missiles guidés par les ondes émises par son téléphone cellulaire qui ont tué le président et mettra en cause une puissance occidentale qui aurait placé ses satellites au service du FSB pour cette opération.

Une explication passionnante, mais fausse. Car si le schéma d'ensemble est bien réel, les choses se sont cependant déroulées un peu différemment. Et pour cause le missile anti-téléphone, comme des experts français de la guerre électronique le déclareront au journal Le Monde, n'existe pas : "S' il existe des missiles antiradars qui se guident sur les ondes émises par leurs cibles, le missile anti- téléphone n'a pas encore été inventé" (23) L'activation du téléphone portable du président tchétchène aurait, en revanche, permis sans beaucoup de problèmes à un Illiouchine 76 équipé de matériel ELINT (Electronic Intelligence) de repérer en quelques secondes l'origine de l'émission du signal. Il suffisait dès lors de dépêcher sur place un ou plusieurs hélicoptères de combat en vol dans la région pour éliminer Doudaev en tirant quelques missiles air-sol. Mais l'important, en ce qui nous concerne, n'est pas là. Ce qui importe, bien entendu, c'est que le FSB ait jugé bon d'utiliser le prétexte de négociations au plus haut niveau pour attirer le loup tchétchène dans le piège qui lui sera fatal. Un procédé qui a porté ses fruits, mais qui discrédite dangereusement le pouvoir politique russe. Il y a fort à parier que, placés dans des circonstances identiques dans un avenir plus ou moins loin tain, d'autres rebelles y regarderont à deux fois avant de croire à la sincérité de leurs interlocuteurs se réclamant du Kremlin...

Quelques affaires de plus...

Cambriolage à France Télécom

Le 3 mars 2000, il a été constaté qu'il y avait eu des visiteurs dans un dans un immeuble de France Télécom, et que les clés du responsable avaient été utilisées. Comme il n'y avait eu aucun vol, la gendarmerie et autres services d'investigation n'avaient pas été alertés.

Le lundi de Pâques, 24 avril, la direction de la téléphonie mobile à Montrouge dans les Hauts de Seines, Avenue de la Marne, s'est fait là, carrément piquer un coffre fort de 50 kg. Il contenait 360 fiches téléphoniques classées *Secret Défense*. Il y avait aussi un autre listing de demandes d'interceptions en cours, et 200 fiches d'écoutes datant de mi-décembre 1999, qui auraient dû être détruites et ne l'avaient pas été. Elles concernaient des écoutes de téléphones portables dont les demandes émanaient de services comme la PJ, DST, DGSE, gendarmerie, les douanes, mais aussi DPSD[96]... Elles sont roses pour la DST, jaunes pour la PJ...

Le cambriolage de France Télécom a été réalisé visiblement par des professionnels, qui en plus connaissaient très bien les lieux.

La sécurité de l'immeuble est réalisée par deux sociétés, une de télésurveillance, et l'autre de maîtres-chiens. Ce lundi matin de Pâques, il y a d'ailleurs eu une intervention pour programmer le système de contrôle d'accès en jour férié. Un peu plus tard, un véhicule avec trois personnes arrive et rentre dans le parking souterrain en utilisant un badge magnétique. Ils évitent les caméras du rez-de-chaussée, puisqu'ils ne s'y arrêtent pas. Elles ne sont de toute façon pas branchées sur le réseau, et on peut même se demander s'il y a un magnétoscope qui enregistre ce qui se passe en permanence dans l'immeuble. Ils utilisent l'ascenseur pour monter directement du sous-sol au premier étage, qui n'a pas de caméra. Ils passent le sas avec leur badge, pour rentrer dans le service des écoutes. Il y a seulement 20 personnes qui peuvent y pénétrer avec un badge. Les cambrioleurs vont vers le bureau des deux responsables des écoutes habilités *secret défense*. Ils ne fracturent pas la porte blindée, mais démontent la paroi vitrée de côté.

C'est paradoxal à France Télécom, mais on va « durcir » quelque chose en y mettant le prix, et avec des cabinets d'études qui pensent à tout, alors qu'en passant par derrière si je puis m'exprimer ainsi, n'importe qui peut neutraliser un moyen qui a été coûteux à la réalisation.

Ensuite ils n'ont pas fait de détail, ils ont carrément embarqué le coffre avec eux, car il n'était pas scellé. Là, plus moyen de faire autrement, France Télécom a été obligée d'informer la gendarmerie. L'enquête a été confiée à la DST. C'est la preuve que la sécurité à France Télécom a de sérieuses lacunes. Ce n'est pas une grande surprise, quand on sait comment fonctionne et sont dirigés certains départements. Cette opération commando rappelle le cambriolage de la brigade financière sur les documents de l'affaire ELF, rue Château des Rentier dans le treizième.

Le feuilleton continue, un salarié découvre le jeudi 27 que son tiroir a été forcé durant la nuit. À la suite d'une fuite, le *Journal du Dimanche* du 30 avril 2000 a révélé ce cambriolage. Ce cambriolage a été confirmé le 3 mai 2000 par le secrétaire d'État Christian Perret.

Des opérateurs non contrôlés :

Un opérateur peut mettre n'importe qui sur écoute en toute impunité.

Il y a des naïfs qui pensent qu'il s'agit d'un cambriolage crapuleux, dont le but était de voler des cartes téléphoniques. Soyons sérieux. Mieux on peut aussi lire que des concurrents avaient peut-être un but qui était celui de porter atteinte à l'image de France Télécom. La plaisanterie est quand même un peu grosse.

[96] Direction de la Protection et de la Sécurité de la Défense.

Mais on peut se demander aussi si le dirigeant d'un groupe ou d'une société concurrente à une des filiales du groupe France Télécom, n'a pas voulu vérifier tout simplement par ses propres moyens, s'il n'avait pas été mis sur écoute par l'opérateur. Cette hypothèse vaut aussi bien la précédente.

On peut aussi se dire qu'un très haut politicien, un ministre par exemple, ou un diplomate a voulu vérifier si son numéro de portable n'était pas sur écoute, en faisant cambrioler France Télécom par un service secret. Autre hypothèse qui tient aussi la route.

Il faut savoir que des chercheurs qui travaillent sur les effets du téléphone portable sur la santé, peuvent aussi avoir été mis sur écoute. De là à penser qu'il en est de même pour les politiciens qui travaillent sur des sujets qui dérangent les opérateurs, on peut se demander qu'est-ce qui peut empêcher ce dernier de les écouter en France.

N'importe quel politicien par exemple qui voudrait faire passer un texte de loi qui irait contre les intérêts des opérateurs pourrait se retrouver mis sur écoute sans le savoir, et sans que les services de l'État ne le découvre, puisqu'il n'existe aucun moyen, ou aucune structure officielle de contrôle, capable de vérifier ce fait et l'éthique de nos opérateurs. Ils peuvent faire des écoutes en toute impunité, puisqu'il n'y a aucune commission de contrôle pour vérifier leurs agissements. Ce fait est valable pour tous les opérateurs sans exception, y compris pour ceux d'internet, pour le courrier électronique.

Le CNCIS épingle les officines et opérateurs :

Actuellement n'importe qui peut faire des écoutes quand ce n'est pas les opérateurs eux-mêmes qui commettent des actes illégaux en se livrant à des interceptions illégales. En Effet, des actions réalisées en marge de la légalité par des opérateurs ont été dénoncées par la CNCIS[97] en 1998, qui s'est plainte de ne pas pouvoir les sanctionner. Le journal *le Parisien* du 30/04/98 publiait un article de Fabrice Lhomme sur le contenu du sixième rapport de la CNCIS. On retiendra que les écoutes clandestines sont estimées à 100.000 par an. Mais on apprend surtout :

« La CNCIS redoute qu'une insuffisante coopération institutionnelle avec les opérateurs de télécommunications et les industriels, conduise à la multiplication d'initiatives en marge de légalité ».

On ne peut être plus clair. Le CNCIS a jugé utile par exemple de retirer en début d'année 1998 à certaines sociétés, l'habilitation dont elles disposaient pour faire des écoutes, en raison du non-respect de la loi. Cette commission a aussi regretté, ce qui est tout à son honneur, que des poursuites ne soient pas engagées à l'encontre de ceux qui avaient violé cette législation en vigueur. On peut donc s'étonner que dans une république, que des politiques puissent accepter sans engager de poursuites, la violation de la constitution française, des droits des citoyens, l'atteinte à la vie privée, mais aussi de leurs droits. Il n'y a en effet aucun service de l'État qui vérifie si les opérateurs de téléphonie ou Internet ne réalisent pas des interceptions illégales pour leur propre compte. Début avril une réunion a eu lieu au CNCIS en présence :

— du Conseiller d'État, Dieudonné Mandelkern,

— du Député PS Jean-Michel Boucheron,

— du Sénateur Centriste Pierre Fauchon,

Dans les coulisses, on déclare un certain agacement à l'égard de France Télécom Mobile, dont on dit volontiers qu'il se préoccupe plus de son chiffre d'affaires que de la sécurité des écoutes. Dans le rapport public du 8 juin, un chapitre concerne les problèmes liés à la téléphonie mobile. À partir de 1995, il a été imposé que les opérateurs prennent les dispositions nécessaires, pour permettre les écoutes sur les mobiles. Elles coûtent 5 fois plus cher que les écoutes filaires. Chez certains opérateurs comme Bouygues, on attend que l'État paye ses dettes avant de refaire d'autres écoutes. Il est vrai que quand l'État vous réclame les impôts, il n'est guère patient.

[97] Commission Nationale de Contrôle des Interceptions.

Et c'est toujours d'actualité...

Voici le tableau figurant dans le 14e Rapport d'activité du CNCIS pour l'année 2005 :

Les demandes initiales d'interception

État des demandes initiales d'interception, années 2004 et 2005

	Demandes initiales		Dont urgence absolue		Accordées	
	Année 2004	Année 2005	Année 2004	Année 2005	Année 2004	Année 2005
Totaux	3 787	4 144	633	854	3 744	4 067

État comparatif sur cinq ans

Motifs	2001	2002	2003	2004	2005
Sécurité nationale	509	486	526	548	625
Potentiel scientifique et économique	49	38	42	66	43
Terrorisme	1 203	1 103	1 126	1 292	1 468
Criminalité organisée	1 400	1 511	1 668	1 881	2006
Groupements dissous	0	0	0	0	2
Totaux	**3 161**	**3 138**	**3 362**	**3 787**	**4 144**

Les « grandes oreilles » de la France

Le Ministère de la Défense se dote de satellites espions capables d'intercepter les communications téléphoniques, fax, e-mails... pour écouter le monde entier. Par Serge BROSSELIN

Milieu des années 90 au siège parisien d'un groupe industriel français. Tous les hauts responsables ont été convoqués par leur président qu'accompagne le directeur de la sécurité. Aucune des « huiles » conviées à la réunion n'a préalablement été informée de la raison de ce surprenant rendez-vous matinal. Le chef de la sécurité met en marche un magnétophone. Stupeur des invités ! Ce sont leurs propres communications téléphoniques, interceptées à partir de leurs téléphones portables, qu'ils entendent !

Depuis, ces cadres dirigeants appelés à traiter les informations stratégiques sont sensibilisés aux risques des interceptions électromagnétiques. Car, inutile de le préciser, ce que les « grandes oreilles » du ministère de la Défense français ont intercepté, le réseau d'écoute américain Echelon de la National Secutity Agency (NSA), dont le siège est à Fort Meade, dans le Maryland, en a eu également connaissance. Interception de mobiles, de télécommunications civiles (courrier électronique, fax, téléphone...) et militaires, recueil des caractéristiques des fréquences de fonctionnement des radars militaires ou des conduites de tir de batteries de missiles, tout s'écoute à partir de l'espace !

« Gouverner c'est prévoir », donc plus que jamais à l'ère de la communication généralisée, c'est avant tout, savoir. Voilà pourquoi le ministère français de la Défense va mettre en service en 2003 (voir dans la section traitant du réseau mondial d'écoute Echelon) un système d'écoute électronique spatial que seuls les États-Unis et la Russie possèdent aujourd'hui.

Les moyens d'enregistrement téléphoniques :

La justice peut se demander légitimement pourquoi et dans quel but des opérateurs de télécommunications filaires ou portables, s'équipent avec des systèmes d'enregistrement aussi sophistiqués, que même nos services officiels ne peuvent se payer. On peut douter que ces derniers sous-traitent ce genre d'activité sensible à des opérateurs, sinon on retomberait une fois de plus dans des contingents d'écoutes non déclarées, donc une fois de plus dans les écoutes illégales.

Il serait certainement très instructif d'écouter les justifications des uns et des autres. Les nouveaux équipements disponibles chez divers constructeurs, permettent d'horodater et d'enregistrer 2 MICs simultanément. Cela correspond à 60 conversations téléphoniques et les deux canaux D respectifs. On peut sélectionner les conversations par les numéros des appelés ou appelants, par bornage d'une date et d'un créneau horaire. Toutes ces informations sont en effet contenues dans les canaux D.

En utilisant un dispositif externe de reconnaissance vocale, on peut extraire une communication à partir d'une empreinte vocale pour déclencher un enregistrement à partir de ces derniers. L'autre moyen possible consiste à utiliser les mots clefs pour déclencher une action. Comme exemple, nous pouvons prendre le logiciel Voice-Assist qui était livré à une époque avec la carte sonore SoundBlaster pour les ordinateurs IBM/PC. Après avoir enregistré des mots clefs sous une ou plusieurs intonations, on programme pour chacun, une action ou fonction particulière interne ou externe au système. L'ordinateur reconnaît ensuite le mot prononcé et déclenche l'action appropriée.

Pour en revenir aux enregistreurs, ils peuvent utiliser des cassettes S-VHS, DAT dont la durée pourra atteindre 500 heures en fonction du temps d'utilisation des canaux du MIC. Certains de ces appareils sont assez bien conçus pour n'autoriser qu'un accès sélectif à plusieurs techniciens qui auront chacun un mot de passe et leur propre journal d'accès au système horodaté. On peut autoriser ainsi un technicien à n'écouter que certains numéros. Ils comportent aussi bien évidemment un mot de passe ingénieur système ou encore appelé super-utilisateur. Plusieurs appareils peuvent être gérés en réseau à partir d'un seul ordinateur. Ils peuvent fonctionner en mode cyclique ou ping-pong ou dès l'apparition d'une communication sur un canal. Quand la bande est terminée sur un, un autre appareil prend la relève et enregistre. Le nombre de constructeurs pionniers pour ce type de matériel est assez limité.

Le problème, c'est que si les services officiels ont acheté ce type d'équipement, ils n'ont malheureusement pu que les acheter en nombre réduit. En effet si on considère que le prix d'une unité est de l'ordre de 200 à 270 KF en fonction des constructeurs, tout le monde comprendra qu'il est impossible d'en installer dans chaque ville. Alors qu'en est-il dans ce cas pour les téléphones portables, réseaux auxquels la gendarmerie n'a pas accès. Ce qui est contraire aux opérateurs qui peuvent faire ce qu'ils veulent sans le moindre contrôle en plus. Leurs ennemis n'ont plus qu'à bien se tenir ou changer de mode de communication. C'est ce qui a peut-être justifié l'apparition de système de cryptographie pour le GSM à une époque. Les politiciens et services officiels, éditeurs journalistes, concurrents n'ont pas en effet à être écoutés par ces curieux d'un nouveau genre. Le nombre de constructeurs étant très limité, un juge n'aurait aucun problème à définir la liste des clients et compter le nombre vendu aux opérateurs.

Le principe de fonctionnement est le suivant : plusieurs abonnés sont reliés sur un central PABX. Les communications des suspects sont réorientées, par programmation vers un faisceau MIC sortant qui sera transmis vers le PABX d'un centre d'écoute officiel comme le GIC. Car en effet contrairement à un lien physique dédié à chaque fois à un seul abonné, ici on peut enregistrer 100 ou 300 abonnés différents sur le même enregistreur. Il ne faut seulement pas dépasser la limite de 30 communications simultanées. S'ils téléphonent donc chacun à tour de rôle, c'est ce qui permettra d'augmenter le nombre des suspects sur un seul système. Pour les téléphones portables, cela est plus complexe en raison de la mobilité des utilisateurs. Rien ne peut se faire sans passer par les divers opérateurs. Le groupe se retrouve donc automatiquement directement informé des actions engagées contre les dirigeants d'une de ses filiales. Voilà pourquoi la justice, les juges, les services de police auront plus de difficulté qu'avant pour faire leur travail.

Système d'interception ou d'écoute électronique téléphonique automatique :

C'est ce que nous pouvons appeler des écoutes automatiques. Il n'y a aucune intervention physique sur les installations. Elles sont totalement indétectables. Le principe consiste à réorienter dès la détection

de mots clefs préprogrammés ou à partir d'une reconnaissance vocale les conversations automatiquement vers un centre d'écoute.

Le développement de ce genre d'autocommutateur téléphonique a commencé a être étudié et réalisé à partir de 1980 par la firme *Pressley*. Elle travaille pour le Département de la Défense Américain qui est un de leur client. Il permet précisément de tout numériser, tout sauvegarder, tout réorienter vers un centre pour une écoute et un traitement ultérieur ou voire même immédiat. Ce genre d'installation est disponible et opérationnelle chez *British Telecom* en Angleterre. Quand un opérateur s'installe sur notre territoire, il vient avec son propre matériel, avec ses PABX, ses logiciels de base et options plus ou moins connues. Nous n'avons aucune garantie que des opérateurs n'utilisent pas ou n'utiliseront pas ce genre de système en France permettant de réorienter certaines communications de diverses firmes françaises vers leur pays. J'attire l'attention de notre gouvernement sur ce point particulier. Il n'y a en effet aucune différence matérielle ou modification, tout est géré et traité au niveau des logiciels. Je ne vois donc pas comment on découvrirait la supercherie sauf en espionnant tout ce qui transite sur les tuyaux en direction de l'étranger et encore. Si le traitement se fait sur place avec un système d'analyse en langage pivot, que l'on compresse et l'on crypte le tout, on n'y verra que du feu.

Des informations capitales pour notre économie ou nos recherches peuvent ainsi transiter. Il en est de même sur le réseau Internet. Un message que j'expédie à mon voisin peut très bien se retrouver à la NSA à Fort Meade tout simplement parce que j'aurai utilisé des mots dans mes phrases sans le savoir qui auront été programmé dans leur système. On ne peut que conseiller à nos industriels des très hautes technologies d'être très prudent sur l'utilisation des réseaux comme Internet.

Nouveau service France Telecom : l'espionnage gratuit !

Article paru dans *Le Virus Informatique* 26 (juin 2004)

Qui n'a pas au moins une fois rencontré la Messagerie Vocale ? C'est un service gratuit de France Telecom qui, à l'instar d'un répondeur téléphonique, enregistre les appels. Il s'active au bout de quatre sonneries dans le vide ou lorsque votre téléphone est déjà occupé par une autre communication. Pour prendre connaissance des messages déposés, l'abonné doit simplement composer le 3103 depuis son combiné. Il connaîtra au surplus, la date d'appel et le numéro de téléphone de l'appelant. Mais, le saviez-vous ? L'offre Messagerie Vocale comprend en outre des options pratiques, notamment l'alerte par e-mail. Elle vise en première ligne les gros consommateurs du net ou les itinérants.

Chaque jour, dès qu'un message est laissé sur votre répondeur France Telecom, un mail vous informe que « *vous avez reçu dans votre messagerie 0142xxxxxx au moins un nouveau message le 09/06/2004 à 17:26:06* ». Pour l'activer, rien de plus simple : il suffit soit de téléphoner à un automate, soit d'envoyer un mail à l'adresse lamessagerievocale.3103@francetelecom.com. Dans l'objet, indiquez seulement votre numéro de téléphone et laissez le corps vide. Si tout se passe bien, un mail de confirmation vous annoncera dans les 48 heures la mise en route du système. Mais, grosse surprise, il n'y a aucune vérification de la légitimité des demandes !

Quiconque peut envoyer la demande d'inscription depuis n'importe quelle adresse e-mail et, surtout, mentionner le numéro de téléphone de n'importe quel abonné ! En toute discrétion, une personne mal intentionnée peut donc savoir si son voisin, ami, ennemi, patron, collègue, conjoint (etc.) a reçu des appels sur sa ligne. Il saura du même coup si, à l'heure indiquée dans le mail, il était absent ou occupé, car en week-end ou en vacances ! Les seules contraintes, aussi maigres que naturelles, consistent à connaître le numéro et espérer que la victime soit abonnée à la Messagerie Vocale... Bref, un bien bel outil d'espionnage offert par France Telecom !

Contactée, la société nous a remerciés, mais a également relativisé, car « très peu de clients utilisent l'avis de message par mail » (sic). Elle souligne, un peu gênée, que la procédure normale exige bien une validation par téléphone « mais trop souvent les clients oubliaient cette étape et se plaignaient que cela ne

fonctionnait pas ». Pour « faciliter cet usage, le service compétent procédait lui-même à l'activation, dans la foulée de la réception du mail. Nous allons donc restaurer la procédure initiale ». Virus, le premier magasine qui pourrit la vie des abonnés France Telecom ! (Source : David F. Gallagher)

Marc Rees

Le Busch à oreilles...

Bush défend les écoutes téléphoniques (Article publié le 20/12/2005 dans RFI Actualités)

Patriot Act ou écoutes électroniques, le président américain continue à justifier des mesures exceptionnelles par la guerre contre le terrorisme.

Le président des États-Unis, George W. Bush, continuera à autoriser les agences d'espionnage à faire de l'écoute électronique aux États-Unis sans mandat de la justice. Samedi, dans son message radio hebdomadaire, il avait admis avoir autorisé plus de 30 fois des opérations d'écoute de plusieurs centaines, voire plusieurs milliers de personnes aux États-Unis. La loi interdisant aux États-Unis d'espionner des conversations d'Américains, le président a assuré qu'il s'agissait d'appels internationaux faits depuis les attaques du 11 septembre 2001.

Dans sa conférence de presse de lundi, George Bush a assuré que ces mesures étaient légales, relevant de sa « responsabilité constitutionnelle » de protéger le pays. Revendiquant le secret ayant protégé l'opération, il a annoncé l'ouverture d'une enquête pour déterminer l'origine des fuites qui ont révélé la pratique de ces écoutes dans les colonnes du *New York Times*. C'était un « acte honteux » selon lui que de révéler les opérations d'écoute « en temps de guerre » allant jusqu'à assurer que « le fait qu'on discute de ce programme aujourd'hui aide l'ennemi ». Il a dressé un parallèle avec la responsabilité de la presse qui aurait révélé la façon dont Oussama Ben Laden communiquait par téléphone portable, ce qui, après publication, aurait poussé le chef d'Al-Qaïda à changer ses habitudes.

Un appel pour le Patriot Act

C'est encore au nom du 11 septembre et de « la guerre contre le terrorisme » que le président américain s'en est vigoureusement pris aux sénateurs qui bloquent le renouvellement du *Patriot Act*, une loi d'exception étendant les pouvoirs des forces de l'ordre dans le cadre de la lutte contre le terrorisme. Lorsque la loi avait été adoptée dans la foulée des attentats du 11 septembre, tous les sénateurs sauf un l'avaient soutenue. Quatre ans plus tard, la quasi-totalité de l'opposition démocrate, rejointe par quatre élus du Parti républicain du président Bush, émet des réticences à sa reconduction dans la forme actuelle. George Bush leur a rappelé leurs contradictions : « La plupart des sénateurs qui bloquent actuellement le Patriot Act l'avaient adopté en 2001. Ces sénateurs doivent expliquer pourquoi ils pensaient que le Patriot Act était un outil crucial après les attentats du 11 septembre et pourquoi maintenant ils pensent qu'il n'est plus nécessaire. » Interrogé sur la chaîne ABC lundi soir, le vice-président Dick Cheney est allé un peu plus loin dans les accusations vis-à-vis des sénateurs opposés à sa prolongation : « Ce qui me préoccupe, c'est qu'à mesure que l'on s'éloigne du 11 septembre, il semble que certains soient de moins en moins engagés à faire le nécessaire pour défendre le pays. »

Tensions entre la Maison Blanche et le Congrès

Ces remarques ont remis de l'huile sur le feu entre la Maison Blanche et le Congrès. En ce qui concerne les écoutes controversées, le président a fait valoir qu'il avait eu l'aval du ministre de la Justice pour les écoutes, mais il n'a pas mentionné l'autorisation du Congrès. Tout comme pour l'existence de prisons secrètes à l'étranger, ses élus (à l'exception des chefs de file qui n'ont pas été autorisés à partager l'information) n'ont pas été informés des écoutes. « Le président croit qu'il a le pouvoir de passer outre les lois que le Congrès a votées », s'est plaint le sénateur démocrate Russell Feingold, « le président ne choisit pas quelles lois il décide de suivre. Il est le président, pas un roi. »

Pour les démocrates, l'affaire des écoutes est symptomatique des libertés que le président s'autorise vis-à-vis du pouvoir législatif. Ils reprochent à la majorité républicaine de ne pas laisser le Congrès jouer son rôle de contre-pouvoir et d'avoir signé des chèques en blanc au président Bush, sans lui avoir demandé de compte sur 14 dossiers, allant du scandale des fuites sur la couverture de l'espionne Valerie Plame, aux attributions de contrat en Irak à *Halliburton*, l'entreprise dont le vice-président Dick Cheney était employé.

Ces prérogatives que s'est attribué George Bush font aussi grincer des dents sur des bancs conservateurs traditionnellement méfiants vis-à-vis du pouvoir du gouvernement fédéral et de son intrusion dans la vie privée des Américains.

Les portables aussi...

Les radiotéléphones :

Il existe à ce jour divers systèmes comme le Radiocom 2000 dont l'activité devrait s'arrêter dans très peu de temps. Le plus répandu aujourd'hui étant le cellulaire ou GSM. Il y a aussi le Bi-Bop qui n'a pas connu le succès du GSM. Il semble que ce dernier ne soit pas la solution en terme de confidentialité. Sinon pourquoi des industriels ont-ils estimé nécessaire de produire des systèmes de cryptographie pour ce mode de communication ?

Il y a une raison. Il ne faut pas oublier que pour réparer ou régler ces appareils, des bancs radiotéléphone ont été créés. Même s'ils sont coûteux, en matière d'espionnage industriel, on ne regarde pas à la dépense. Ce type de banc à un coût qui oscille entre 100 et 200 KF, mais comporte une multitude de protocoles de communication numériques ou analogiques. Ces appareils permettent normalement de régler tout ce que l'on veut à condition d'y mettre le prix. Mais on peut aussi écouter en faisant quelques modifications, et en le couplant à une informatique assez lourde.

Mais il faut aussi avoir des complicités chez les opérateurs pour connaître certains numéros. Ce n'est évidemment pas à la portée du premier venu. Le problème c'est que les portées radio des portables sont réduites, donc l'écoute est possible pour un sédentaire, pour un pigeon voyageur, il est sûr que l'interception est beaucoup plus délicate. Il faudrait autant de systèmes d'interception radio qu'il y a de cellule. Par contre, l'opérateur pourra lui écouter tout ce qu'il veut au niveau des MSC[98], même s'il n'en a pas le droit, qui ira le contrôler ?

Aussi aberrant que cela paraisse, il n'y a en effet aucun organisme de contrôle qui vérifie si nos opérateurs respectent une certaine déontologie, et n'y dérogent pas pour effectuer des écoutes pour leur propre compte, sur les portables de leurs concurrents, des personnalités politiques gênantes, juges, ou brigade financière qui pourraient les déranger. Ils peuvent s'aménager en toute tranquillité un autre sous-sol, ni vu ni connu, faire en sorte que l'ascenseur ne puisse jamais l'atteindre sans un code spécial et une clef, et y installer tous leurs dispositifs d'enregistrement. Il installera des systèmes de traitement destinés à extraire les conversations à partir de mots-clefs, d'empreintes vocales, ou des numéros des abonnés appelants ou appelés. Ce n'est pas sans raison que Matra Communication a développé le Matracom 9600 présenté à Millipol 96, qui est un réseau cellulaire numérique sécurisé et crypté, destiné aux services gouvernementaux.

1-Micro espion GSM (Fiche du revendeur)

« *Micro espion* »dernière génération conçu à partir d'un téléphone mobile cellulaire. À la différence des « Micro Espions » ordinaires qui utilisent les ondes radio classiques, l'émetteur GSM

[98] Le MSC (Mobile services Switching Center ou Mobile Switching Center) est un équipement GSM en charge du routage dans le réseau, de l'interconnexion avec les autres réseaux (réseau téléphonique classique par exemple) et de la coordination des appels.

transmet sans limites de distance (couverture de la téléphonie mobile) ; il n'est plus nécessaire de posséder un récepteur scanner pour capter les émissions. Indétectable par les appareils anti-micro espion. Allumé, il peut être utilisé comme un téléphone portable ordinaire qui permet d'effectuer ou recevoir des appels téléphoniques .

Lorsqu'on l'éteint après avoir composé un code un secret il se transforme en redoutable micro espion GSM capable de transmettre les sons captés dans un rayon de 7 mètres. Pour effectuer une écoute, il suffit d'appeler le numéro de la carte SIM (non fournie) à partir de n'importe quel téléphone (fixe, cabine, mobile) dans le monde ; l'appareil décroche automatiquement sans aucune sonnerie ; l'écran reste éteint. Sans attirer l'attention il est alors possible d'écouter l'activité et les conversations du local où l'appareil a été installé.

Recommandé pour la surveillance audio d'un local, d'une cible en mouvement (une voiture ou caravane par exemple), d'une marchandise. Appareil d'investigation idéal pour détective privé ou pour usage personnel (surveillance audio de la maison par exemple), recherche de preuves, filature...

Livré avec batterie et chargeur.

Autres systèmes en vente libre

INTERCEPTEUR PASSIF GSM MULTIBANDE
IP-GSM-06

Ce système d'Interception de la téléphonie mobile convient pour travailler avec tous les réseaux GSM car il opère dans toutes les bandes attribuées (850/900/1800/1900 MHz).- Il intercepte passivement les objectifs, pouvant registrer tous les appels et messages de texte (SMS) émis ou reçus.-

Ce système opère avec les données extraites de la MSC du réseau à explorer, donnant les données d'interception dans l'air (IMSI/TMSI). L'algorithme y est incorporé COMP128 pour l'encryptement A5.0, A5.1, et A5.2, qui va effectuer le désencryptage en « temps réel ».-

Il génère les registres d'activité des cellules explorées, avec les données correspondantes aux usagers registrés, permettant de « capturer » ceux-ci en tant qu'objectifs.-

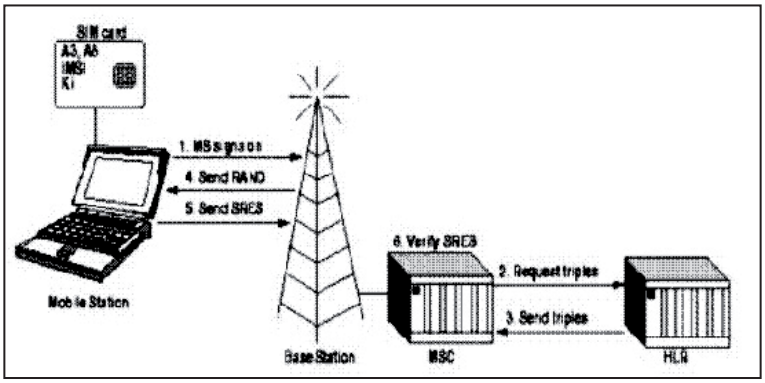
Il génère tous les registres d'activité des objectifs, tant des conversations effectuées, comme des SMS interceptés, avec registre de date, heure, durée, trant/sortant, identification d'abonnées, etc.

Il permet un « suivi en ligne » et la possibilité de convertir en fichiers MP3 (compressés) encryptables avec la possibilité d'être envoyés par courrier électronique.-

Le système basique permet d'explorer en simultané 2 Cellules avec 4 canaux audio d'opération, apte pour 2 objectifs en simultané, et ce système peut « augmenter » jusque 12 Cellules (24 canaux audio), 12 objectifs.-

Forme de travail :

Le système permet de contrôler plusieurs récepteurs selon la configuration et de visualiser sur l'écran l'activité des cellules explorées, obtenant ainsi les données d'interception : IMSI et KI de l'objectif,



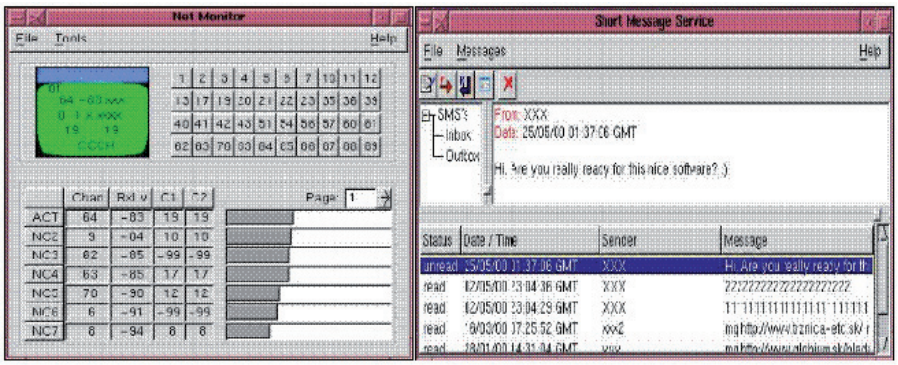
sans devoir utiliser sa SIM (puce) car ils s'obtiennent par le biais d'une application API de manière entièrement passive dans l'air.-

Le système permet d'observer sur l'écran l'activité des cellules, les canaux et l'identification des usagers se trouvant temporellement dans la cellule explorée et par le biais d'une application on peut déterminer que l'un de ces usagers devient « objectif » ou charger dans la base d'objectifs, ceux en mode « spécifique ».

La configuration physique du système Basique (2 cellules 4 canaux audio) est autocontenue dans une valise où le « contrôleur » est un ordinateur du type Laptop (Notebook), Pentium IV, de nouvelle génération, contenant les programmes de contrôle du système et un module de RF et logique contenant le reste de logiciel, les plaques DSP et les récepteurs spécifiques multibandes, plus batterie, source d'alimentation et autres éléments.-

Tout le système est facile à opérer et nous avons des plates-formes en base à Windows et Linux, selon demande expresse et possède une procédure d'utilisation permettant à un opérateur de pouvoir travailler avec tous les paramètres principaux en quelques heures d'apprentissage.

Quelques écrans du système :



Dans l'un on peut apprécier le suivi du Réseau et dans l'autre le suivi du Centre de SMS.-

On peut aussi appliquer un logiciel spécifique pour la localisation de l'objectif par le biais du système LAI, que les réseaux GSM incorporent afin de minimiser les tâches de recherche de l'objectif.

Ce logiciel est supplémentaire et permet de pouvoir retrouver un « objectif » dans le Réseau GSM avec une précision allant entre 100 et 300 mètres, suffisant pour s'approcher et faire la capture.-

On dispose aussi de dispositifs accessoires permettant d'augmenter considérablement la zone d'opération de ce système d'interception, par le biais d'un écran de cellules portatif « IC-GSM-01 », antennes directionnelles de gain élevé et amplificateurs d'antennes.-

Comment fonctionne le Système :

Le système d'interception « multi-cellule », est basé sur le principe du besoin et de l'opérabilité d'un système efficace pour les propos destinés a ces fins, devant couvrir les expectatives quant à leur réalité de fonctionnement d'un Réseau GSM.

Le diagramme de couverture d'un Réseau GSM est basé sur les principes basiques de besoins d'un système d'« interconnexion » entre les usagers de ce réseau, où les devises suivantes règnent :

— Densité d'usagers par zone géographique
— Situation réelle de zone géographique
— Réseaux d'alternative (concurrence)

Tout réseau GSM a un maximum de capacité allant jusque 992 usagers (canaux) par cellule, cela veut dire qu'il ne pourra jamais donner plus de 992 interconnexions sans fil avec les téléphones mobiles (usagers), et si on prend aujourd'hui par exemple la zone d'un « centre commercial », avec la grande

incorporation de « nouveaux usagers » au système de téléphonie mobile, on peut même avoir une zone de +/- 40.000 m² (quatre hectares) quelques 600/700 usagers actifs.-

Tout système d'interconnexion (API) en un réseau GSM envisage que chaque BTS (cellule) n'admet pas plus de 60% de sa capacité, ce qui donne quelques 595 usagers maximum par cellule, cela veut dire qu'une zone de 40.000 m², où l'on dépasse le nombre d'usagers présents, « automatiquement » le réseau partage ces usagers avec les 2 cellules les plus proches. Ces usagers sont « répartis » spontanément et de manière « aléatoire », car l'attribution la donne la BCCH (qui désigne chaque canal à chaque usager), qui désigne la MSC, à chaque cellule, sur un rang ne dépassant pas 40.000 m², quelques 600/700 usagers.-

Si on essaie d'interpréter cette situation, un système « approprié » pour travailler sur un rayon d'action appréciable où on considère qu'on aura toujours le « uplink » ou le « outgoing », c'est-à-dire que le signal généré par le « mobile » ou « station mobile » (on considère la voix de la personne propriétaire du mobile), qui sera toujours limité à un rayon ne dépassant pas les 500/800 m. Dans les meilleures conditions ce système devrait avoir la possibilité d'intercepter avec une capacité minimum de 3 cellules pour un rayon de +/- 200/300 m ou de 6 cellules pour la limite de rayon +/- 500/800 m de notre objectif.

Dans ces conditions, on considère une limite de capacité du réseau GSM, cela veut dire qu'on s'approche de la limite de sa capacité d'interconnexion. Cela ne se passe pas dans les zones où le nombre d'usagers diminue et une cellule ne peut pas recevoir pas plus de 150 ou 200 usagers permanents et pas plus de quelques 200 usagers qui « passent » par la zone c'est-à-dire qu'ils font « roaming » et n'occupent que de manière transitoire la cellule leur donnant service.

Dans les conditions les plus favorables (très peu d'usagers registrés) et avec une très faible densité, on pourra obtenir d'un objectif le maximum de capacité d'interception qui sera proche des 2 km dans les zones urbaines et de plus de 5 km dans les zones sous-urbaines.-

Conception d'un système :

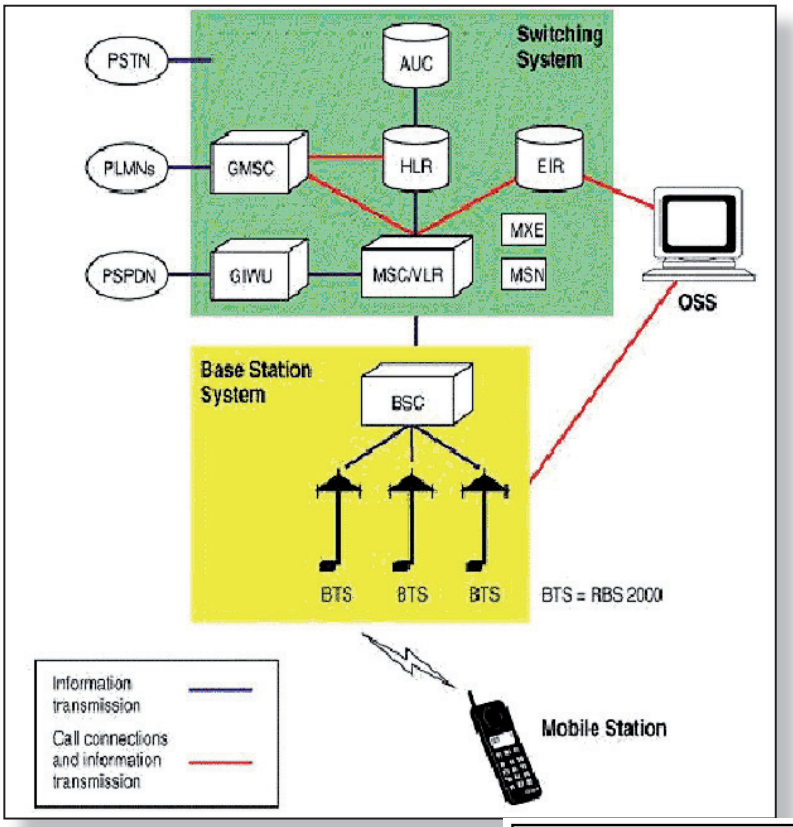
Si nos objectifs se maintiennent tous dans une zone géographique de moins de 50000/60000 m², avec un système de 6 cellules on pourra avoir l'interception simultanée de jusque 2 objectifs dans 100 % des appels car dans le rang des possibilités, on va toujours disposer de plus de 6 récepteurs pour le début de l'interception, 4 d'entre eux travaillant tout en interceptant et 2 autres explorant les cellules restantes pour ne pas perdre la communication.-

Avec ces devises, la conception d'un système multicellule doit envisager les caractéristiques suivantes :

1. Nombre d'objectifs
2. Emplacement géographique des objectifs
3. Mobilité des objectifs (déplacements)
4. Nombre d'usagers dans la zone à opérer
5. Mobilité du système intercepteur

Analysant selon le besoin de chaque situation en particulier on pourra penser un système nous permettant d'intercepter le plus efficacement possible, car avec un système passif, il est impossible d'intercepter à plus de distance ou avec grand pouvoir d'interception, car pour cela il devrait s'agir d'un système d'interception actif ou « enkysté » dans le réseau ou si on peut intercepter massivement la totalité des usagers sans importer les distances du système vers les objectifs.

Diagramme d'un réseau simple de GSM

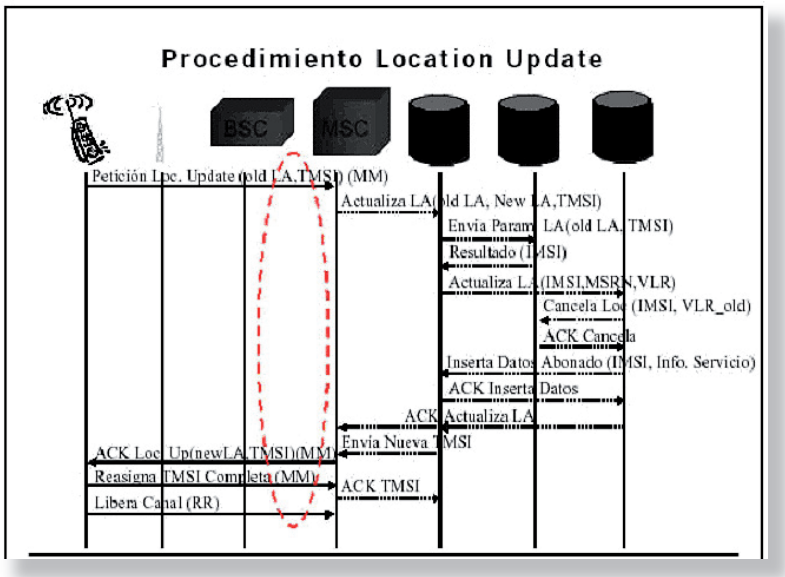


On observe ici où on peut intercepter, de manière active, un objectif et pour cela, on doit compter avec l'approbation de la partie prestataire et une autorisation judiciaire pour le faire.-

C'est différent lorsqu'on opère avec un réseau comme le GSM de manière passive, car l'action doit rester sans évidence de l'interception et donc sans avis au prestataire du service.-

Comment opérer un système d'interception passif :

Dans la zone délimitée, on peut observer où travaille un « intercepteur passif » et toute l'information extraite et capturée, il le fait depuis l'air de manière complètement invisible.



Fonctionnement :

L'Intercepteur actif « IA-GSM4 », tel qu'énoncé par le modèle, est un Intercepteur des réseaux GSM capable d'intercepter les conversations téléphoniques de jusqu'à quatre (4) téléphones cellulaires de façon simultanée, permettant en outre d'activer le microphone de ce téléphone pour pouvoir écouter les conversations qui se déroulent aux alentours, d'intercepter tous les messages de texte — aussi bien ceux reçus que ceux émis par chaque téléphone — et, finalement, de recevoir des messages de texte (SMS) avec toutes les données enregistrées chaque fois que le téléphone est éteint ou allumé, ou chaque fois qu'une quelconque donnée est ajoutée dans le carnet d'adresses.

Toute cette activité est totalement invisible puisqu'elle ne laisse aucune trace dans le téléphone cellulaire « espionné » et son propriétaire ignore totalement que l'ensemble de son activité est enregistrée anonymement, de façon permanente et sans limites de distance.

Ce systèle d'interception utilise le même réseau GSM que celui de la cible sans laisser de traces, peut importe si la cible se trouve dans une ville ou un pays différent, puisqu'à partir du moment où il utilise le service, il peut être intercepté.

Ce possède des qualités uniques puisqu'il dispose des quatre (4) bandes de fréquence utilisées par le système mondial de communication avec les mobiles, et qu'il est possible d'étendre son activité à l'ensemble de la planète. Pour couronner le tout, peut importe le protocole de cryptage utilisé, le système s'adapte à toutes les normes de tous les pays possédant des réseaux GSM (A5.0, A5.1, A5.2 et A5.3).

Composition du système :

Le système se compose des matériels suivants :

— Un PC équipé d'un processeur PENTIUM 4 double cœur à 2,4 GHz, de 512 Mb de mémoire RAM, d'un disque dur de 140 GB, d'un écran plat TFT 17', d'une carte d'interface RS232 (4 ports COM RS232) exploitant le bus PCI, d'une carte son (4 canaux actifs), d'un clavier, d'une souris, d'un jeu d'enceintes puissantes, d'auriculaires, de câbles d'interconnexion et d'accessoires.

— Un module GSM à 4 canaux actifs quadribande, programmables, livré avec interface audio et signal d'activité, batterie rechargeable, antennes multibandes, câbles et accessoires d'interconnexion, chargeur de batterie automatique et logiciel d'activation intégré (firmware).

— Un logiciel de contrôle « IA-GSM4 » codé et personnalisé pour chaque utilisateur, encapsulé dans une clé USB de 1 GB et avec blocage électronique.

— Un manuel d'utilisation du système (incluant la maintenance préventive), qui est remis à chaque client avec un cours de formation personnalisé.

— Quatre (4) logiciels de contrôle pour téléphones cellulaires tournant sous Symbian OS 7.0, 8.0 ou 9.0, personnalisés avec le numéro IMEI de chaque appareil.

Fonctions du système :

Le système IA-GSM4 permet de mener un registre total de toute l'activité de chaque téléphone cellulaire « objectif », en générant des registres de tous les messages texte et un registre de toutes les conversations ou écoutes ambiantes réalisées. Toute l'activité peut être stockée dans la clé USB fournie, dans un CD-RW ou dans un CD simple ; elle peut aussi être renvoyée de manière automatique par courrier électronique partout dans le monde.

Les registres du système se présentent sous forme de fichiers .txt pour les messages de texte (SMS) et sous forme d'archives .wav ou .mp3 compressés pour les fichiers audio.

Tous les registres sont générés automatiquement, mais la décision d'intercepter va dépendre directement de l'action de l'opérateur du système. Pour cette raison, notre entreprise prépare efficacement l'opérateur du système, qui devra en outre être informé sur le travail d'intelligence mené sur l'objectif.

Les écoutes officielles :

Elles sont réalisées le plus souvent au niveau des centraux téléphoniques. Les communications sont réorientées vers le Groupement Interministériel de Contrôle (GIC) dont l'essentiel des installations se situe sous les Invalides. Son existence officielle a été légalisée le 10/07/91. La durée normale d'une écoute est de 4 mois renouvelable. Il est relié à une cinquantaine de centraux téléphoniques de Paris par une trentaine de MICs (1 MIC=30IT) minimum, ce qui donne l'équivalent de 900 lignes téléphoniques. Le reste est complété par des lignes analogiques pour arriver en 92 à un total de 1180 lignes donc d'écoutes simultanées. Pour Paris il y avait 680 lignes et la proche province en comportait 530. Aujourd'hui on

peut penser en raison des risques terroristes que ce centre a multiplié le nombre de lignes par 4 en raison de la miniaturisation des équipements et de ses performances.

La salle d'enregistrement disposait de 4 rangées de 200 enregistreurs minicassette et de 2 de 120. Une autre rangée comportait 6 ordinateurs serveurs équipés chacun avec 1 MIC permettant d'intercepter un total de 192 lignes de télécopieur. Un système de gestion et de traitement permet l'horodatage, l'archivage, la destruction et l'extraction des fax utiles par repérage de mots-clefs programmés. Je suppose que le principe de traitement est similaire au système *Taïga*. Cinq cents personnes permettent à ce site de fonctionner 24 h sur 24.

En 1992, le ministère de l'Intérieur devait utiliser 950 lignes, 300 pour la PJ, 300 pour la DST, 300 pour les RG approximativement. Le ministère de la Défense a environ 250 lignes et les finances utilisent celles qui restent, une quarantaine peut-être. Ces chiffres ne prennent pas en compte les infrastructures non officielles comme la cellule élyséenne qui n'existe plus normalement aujourd'hui. Dire qu'il dispose de moyens assez importants est faux, parce que beaucoup de ces équipements sont dépassés. Mais un gouvernement ne peut se permettre de le renouveler annuellement en raison du coût de telles installations. On peut dire que nos services officiels, du moins pour certains, sont moins bien équipés que les groupes industriels de notre pays. Sinon comment expliquer que la presse télévisée, a, elle, pu donner le nombre de 100 000 à 200 000 écoutes illégales. D'où vient cette information ? Des services officiels eux-mêmes ? Ce chiffre est-il estimé à partir des ventes de matériel ?

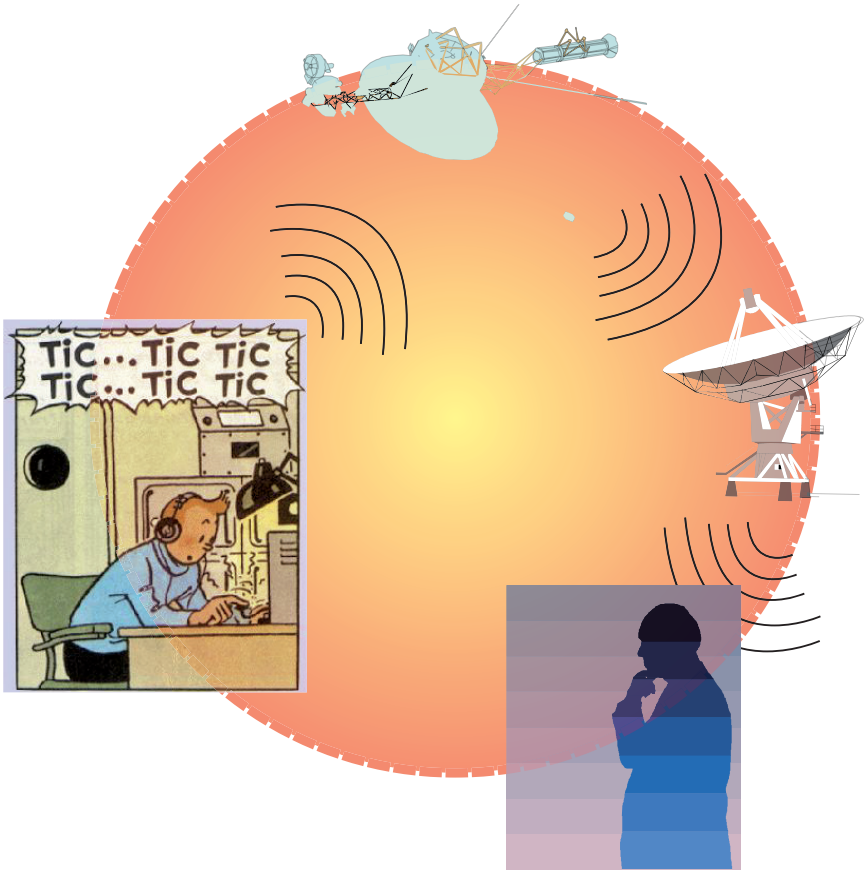
En réalité, il n'y a pas que le GIC qui fait des écoutes. Les militaires, les divers services spéciaux, certains groupes industriels, ont leurs propres centres d'écoute téléphonique ou radio, à divers endroits toujours planqués dans des sous-sols. Certains services n'ont pas d'existence légale de même que leur personnel. C'est pour cette raison qu'il dispose de double, triple, ou quadruple identité, toutes plus vrai l'une que l'autre. Même le numéro de matricule de certains véhicules, ne permet pas de connaître les utilisateurs ou services véritables. Les services sont tellement cloisonnés, que les hiérarchies peuvent ignorer qu'elles sont aussi surveillées parfois. Ils ont leurs propres codes, leurs propres réseaux de communication filaire, fibres optiques, ou radio comme *Tigre, Panthère, Syracuse, Rita* pour les militaires, *Saphir* pour la gendarmerie, etc. Chaque armée a ses structures indépendantes des unes des autres tellement la confiance règne. Si entre services de l'ordre, on s'écoute, il en est de même avec, et entre les militaires, les politiques, ou polices politiques. La guerre des polices est loin d'être inexistante. Ce qui m'intrigue le plus dans cette histoire, c'est comment et par quel canal, la presse a pu affirmer qu'il y a plus de 100.000 écoutes illégales par an. Même s'il y a forcément des officines gouvernementales inconnues, on ne peut affirmer un tel chiffre, alors qu'il n'y a aucune trace, aucun recensement ni organisme de contrôle.

Les écoutes illégales tombent sous le coup de l'article 114 du Code pénal pour entrave aux libertés. Mais les preuves étant impossibles à avoir, aucune plainte n'arrive en justice. Les plaintes déposées finissent sans suite, quand la victime ne se retrouve pas elle-même poursuivie pour dénonciations calomnieuses. Dans ce cas, il ne reste qu'une solution, pour quelqu'un qui a de gros moyens, la Cour Européenne de justice des droits de l'homme. La France est un tel désordre dans ce domaine, qu'il a fallu faire passer un autre décret au journal officiel pour réglementer le contrôle des 40 sociétés privées s'occupant d'écoutes téléphoniques. Le business du renseignement comporte 50.000 personnes au minimum, et continue à se développer. On serait d'ailleurs plus près de la vérité en disant 100.000 personnes, si on compte les anciens policiers, les détectives, les électroniciens, les petits installateurs en téléphonie, les gardiens, tout ce beau monde qui arrondit ses fins de mois au noir.

Conclusion :

Les opérateurs de téléphonie n'ont pour mission que d'acheminer correctement ce qui est envoyé sur leur réseau. La sécurité et le secret de vos conversations, c'est VOTRE affaire !

À l'écoute des ondes



Les moyens hertziens et la perte de confidentialité des communications :

Les ondes, le moyen le moins sûr de communiquer.

À l'évidence, n'importe qui peut capter une émission radio, quelle que soit la fréquence utilisée. De plus, l'écoute et l'enregistrement d'un signal radio ne laisse pas de traces et est parfaitement indétectable.

L'histoire, en particulier la Deuxième Guerre mondiale regorge de faits de « Renseignement ». La possibilité de localiser un émetteur par goniométrie obligeait les résistants à des émissions de courte durée. Le codage est de rigueur, nous développerons ce sujet plus loin, mais relisons quelques pages d'aventure vécue...

La tragique affaire Szek

Si les parents d'Alexandre Szek n'avaient pas vécu en Angleterre, le jeune radio n'aurait sans doute pas trahi l'Allemagne. Et le cours de la guerre aurait pu en être changé... D'origine autrichienne, fils d'un familier de l'empereur, parlant couramment cinq langues, Alexandre Szek est un jeune ingénieur brillant. Le déclenchement de la Première Guerre mondiale ne l'empêche pas de poursuivre, à Bruxelles où il se trouve alors, des recherches sur les communications par voie hertzienne. Indirectement, sa passion le perdra.

Le 27 novembre 1914, en effet, une panne généralisée paralyse les moyens de transmission de la Kommandantur allemande de la capitale occupée. Pour déceler les origines de l'incident et remettre en état le matériel défectueux dans les meilleurs délais, l'état-major réquisitionne tous les spécialistes radios sur lesquels il est possible de mettre la main, et Szek est bien entendu du nombre. Les qualités dont il fait montre, autant qu'une de ses récentes inventions dont le commandement a eu vent un appareil de réception radiotélégraphique capable de s'adapter à toutes les longueurs d'onde — incitent le gouverneur militaire de Bruxelles à recruter le jeune homme et à l'affecter définitivement au service de T.S.F. de son quartier général. Chaque nuit, jusqu'en février 1915, Szek dirige donc, depuis ses bureaux situés rue de la Loi, non loin du Palais Royal, dans le centre de Bruxelles, l'interception du trafic radio allié.

Londres écoute

Nous savons tous à quel point ce sont s'affrontés les services secrets allemands et anglais. Et nous avons pu comprendre l'importance de l'interception et du décodage des communications allemandes par le S.R. britannique. Cette opération, menée sur une grande échelle, sera l'un des secrets les mieux gardés de la Grande Guerre (il ne sera d'ailleurs révélé qu'en 1931). C'est au cœur de la Naval Intelligence Division — le S.R. de l'amirauté — dirigée par l'amiral Hall que se niche la section que l'on désigne par le numéro de son bureau : Room 40, Old Building ou 40 O.B. C'est dans ces quelques pièces que travailleront, quatre années durant, les briseurs de code anglais. Dès le début de la guerre, la marine britannique a dépêché au large du continent quelques discrètes unités navales chargées d'une mission qui l'est tout autant : l'Opération cisaille. En une ou deux nuits, les câbles télégraphiques sous-marins allemands ont été remontés à la surface, coupés et rendus à leur vie sous-marine. Désormais, les communications de l'Allemagne avec le reste du monde ne peuvent plus passer que par les câbles sous-marins des pays neutres ou, en T.S.F., par la voie des airs. Il devient donc possible de les intercepter.

Encore faut-il les déchiffrer. C'est là le rôle de la brillante équipe d'universitaires rassemblée par sir Alfred Ewing au 40 O.B. Un coup de chance va considérablement faciliter leur travail : au début de la guerre, la flotte russe a récupéré, sur le corps d'un officier du croiseur allemand Magdeburg, coulé dans la Baltique, le code de ce bâtiment qui a permis de découvrir la clé de chiffrage de l'amirauté. D'autres récupérations, entre autres celle menée à Bruxelles par Alexandre Szek, vont permettre aux Anglais, durant

toute la guerre, de déchiffrer la quasi-totalité des dépêches envoyées ou reçues par l'état-major, le ministère des Affaires étrangères et les autres services officiels allemands : « On établit des stations d'écoute le long des côtes britanniques » écrit sir Basil Thomson dans ses mémoires, « leur moisson nocturne était envoyée à la Chambre 40 O.B. à l'amirauté pour y être déchiffrée : apprendre les plans secrets de l'ennemi de sa propre bouche valait mieux qu'une tonne de rapports envoyés par l'armée d'espions employés par les Alliés. Peu de gens connaissaient l'existence de 40 O.B., on la cacha même aux ministres mariés. Les messages déchiffrés qui se montaient parfois à 2 000 par jour étaient soigneusement gardés et même les chefs des gouvernements qui profitaient de ces nouvelles ne connaissaient pas toujours leur source »

La Radio et la Résistance

À Londres, le deuxième bureau du Général de Gaulle se transforme progressivement, sous l'impulsion du Colonel Devawrin ,en Bureau Central de Renseignement et d'Action, le BCRA. Le BCRA a pour mission de fournir à la Résistance Française le soutien extérieur et les moyens de coordination dont le plus urgent à résoudre consistait à établir des liaisons radioélectriques France-Londres.

Les premières étapes.

— 1940 : Le Capitaine de Frégate d'*Estienne d'Orves* réalise la première tentative de liaison en Bretagne. Il est arrêté le 22 janvier 1941 et fusillé le 29 août de la même année.

— 1941 : Les opérateurs parachutés « blind »(sans comité d'accueil au sol) sont presque tous arrêtés. Fin 1941,12 postes de radio établissent des contacts. On compte trois opérateurs en entraînement en Angleterre.

— 1942 : Jean Moulin est parachuté accompagné de son radio « Monjaret » le premier janvier, c'est la naissance de « l'Action ». Des opérations d'atterrissages et de parachutages sont de plus en plus nombreuses. D'abord limitées à quelques maquis, ces opérations s'élargissent à l'ensemble des deux zones avec arrivée de radios recrutés en France groupés en un pool nommé « WT », (Wireless Transmission).

Arrestation de Jean Moulin et « WT » décapité, c'est une longue période de silence entre Londres et la France alors que l'effectif des maquis grossit du fait des appels au STO (Service du Travail Obligatoire) pour lequel la défection est totale.

La maturité.

— 1943 : juillet, Jean Fleury réorganise les transmissions et ,avec l'aide de Jean Roy, met en œuvre de nouvelles structures.

— La séparation de l'émission et de la réception qui raccourcit beaucoup le temps des vacations réduit le risque de repérage par la radiogoniométrie allemande. La réception en France est assurée par la procédure « Broadcast » sur appareils de TSF ordinaires ou récepteurs miniatures « Biscuit » spécifique maquis. Ce poste permettait de recevoir toutes les gammes d'ondes par changement de bobines. Il était livré avec une pile offrant basse tension et haute tension dans le même élément avec 30 heures d'écoute.

Récepteur Biscuit

— Instauration de nouveaux plans d'émission radio avec grand nombre de fréquences, horaires, endroits, indicatifs indéchiffrables. Mise en place de « quartz » interchangeables qui stabilisent les fréquences avec plan de fréquences.

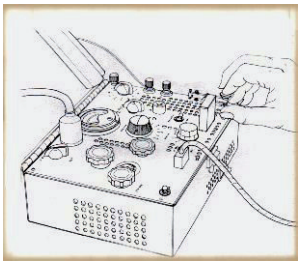
— Une Inspection Nationale des Transmissions est créée avec un inspecteur et un adjoint.

— 2000 émetteurs et 1000 quartz sont fabriqués et parachutés sur la France où Claude Wolf (« Indien ») assure le recrutement et la formation des opérateurs radios.

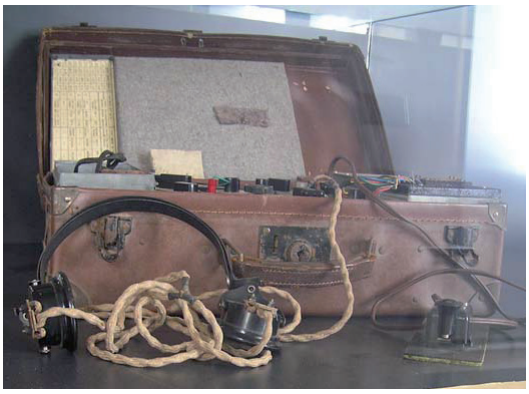
Les opérateurs radio.

— On compte 159 opérateurs qui ont travaillé depuis la réorganisation avec un pseudonyme représentant qui une ville, qui une nation, qui un peuple, etc. Plus de la moitié a été recrutée en France. Pour la période 1940-1942, plus de 75 % ont été arrêtés alors que pour la fin de guerre seulement 25 % ont subi l'allemand. Dans les deux cas, 50 % ne sont pas revenus des camps de la mort.

— Le volume du trafic passe de quelques câbles quotidiens en 1940 à 150 par jour en 1943. Pendant la dernière année de guerre, 50000 messages sont transmis...



POSTE BP3 : construit à partir de 1943 il équipe les centres secrets de l'I.S. Appelé aussi poste polonais, il était de facture robuste et puissant. Bien qu'encore un peu lourd, il permettait des liaisons intercontinentales.



Radio-valise utilisée par les résistants

Le 31 mai 1942 à 2 heures du matin...

Quel vacarme après le silence du ciel ! Je reste caché dans l'herbe haute, pistolet à la main — une balle dans le canon, cran d'arrêt ôté — scrutant l'ombre des haies, tendu, prêt à défendre chèrement...

Il n'y a là rien de méchant, seulement les hôtes naturels de l'endroit, que mon arrivée n'impressionne pas, à leur aise et célébrant l'Amour dans la tiédeur du Printemps, et qui s'appellent sous la lune : « Cigale chérie, je suis ici ! Grillon de mon cœur, viens ! Ma grenouille, ah, je meurs ! »

Il me faut détacher la valise des suspentes. Les instructions sont de faire un paquet du parachute, de la combinaison de saut et du rembourrage de protection de la valise, puis d'enterrer le tout : j'ai même la pelle idoine attachée à la jambe de ma combinaison de saut.

Mais la terre est bien dure et il fait bien chaud. La gare de Romanèche-Thorins doit être à une dizaine de kilomètres. Creuser un gros trou dans ce sol sec, puis traîner ma valise dans la chaleur de la nuit sur une telle distance, va m'épuiser et me faire remarquer : ça ne me semble pas raisonnable. Il vaut mieux cacher le tout et revenir chercher mon bagage plus tard.

Je fais une boule de l'ensemble — ayant, bien sûr, retiré le Paraset[99] de la grosse valise : avoir un poste émetteur au bout des doigts est ma raison d'être ici — bien recouvert de tissu camouflage, que je fourre au plus profond d'un buisson, pas trop près, en prenant soin de ne pas laisser de trace qui puisse relier la cachette à l'herbe écrasée par mon atterrissage.

La route est là, à côté du pré. Une borne : Thoissey 3 km. Chapeau pour la navigation !

La route serpente à travers Thoissey. La lune et les étoiles éclairent le chemin. Chiens stupides qui aboient, malgré mes semelles de crêpe. Volets clos de la gendarmerie. Je m'en voudrais de déranger le sommeil de ses occupants.

Des champs s'étendent de part et d'autre de la route. Je marche dans la nuit chaude, les yeux et les oreilles aux aguets, entouré par le bruit des conversations des bestioles, mon Paraset toujours à la main. Une autre borne me dit que la gare de Romanèche-Thorins est à cinq kilomètres. N'est-il pas bien tôt pour y arriver ? Et si je dormais un peu dans ce petit bois ?

[99] Le Paraset était un émetteur récepteur simple construit par les alliés pendant la 2e Guerre Mondiale. Il était utilisé par les services secrets britanniques ainsi que par les résistants belges, hollandais et français.

Il fait jour, c'est dimanche. Déjà on travaille dans les champs à étaler les meulettes du foin entassé pour la nuit. Petit déjeuner avec une ration de survie : il y a là une tablette d'un mélange de chocolat et d'extrait de bœuf déshydraté, sans doute très nourrissant. Ce métier exige une grande largeur d'esprit.

L'auteur à Lyon 1942/43

Je traverse la Saône. Soleil radieux. La gare de Romanèche-Thorins. « Un billet aller pour Uzès, s'il vous plaît. » Arrivée de la locomotive : gros soupirs de vapeur. Le wagon est plein de gens avec des colis, des sacs, des valises : tous parlent ravitaillement, de toute évidence le sujet de première importance.

Il me faut changer de train à Lyon. Dans la gare de Perrache, une équipe de gendarmes scrute la foule, demande l'ouverture d'une valise particulièrement grosse, ou les papiers de celui qui a vraiment l'allure trop louche. Moi, j'ai l'air d'un bon petit et ma valise est pas grosse : je passe sans encombre avec le flot. Il me faut aussi changer à Nîmes, mais là, pas de train pour Uzès avant le lendemain.

Lorsqu'au matin on frappe à la porte de ma chambre d'hôtel pour me réveiller, je réponds : « Come in ! » Ça n'est pas perçu.

À Uzès, je trouve mon contact, un ami d'André Diethelm qui me donne l'adresse de celui dont je dois être le radio : Jacques Soulas — SALM — chef d'une mission pour le Commissariat à l'Intérieur, et dont l'objet est de prendre contact avec des personnalités de la vie politique française pour essayer de les persuader de rejoindre le général de Gaulle, qui se trouve un peu seul en Angleterre.

J'ai connu Jacques Soulas à Londres. Il était de ceux qui, prisonniers de guerre dans l'Est de l'Allemagne, s'étaient évadés vers l'URSS proche, d'où ils avaient rejoint les FFL en Angleterre, et qu'on avait surnommés : Les Russes.

La plupart des chefs de mission en France : renseignements politiques, économiques ou militaires, organisation de parachutages et d'atterrissage, de sabotage, de propagande, d'évasion, etc., étaient accompagnés d'un opérateur radio — dans la mesure où, denrée rare, il y en avait de disponible — pour assurer les communications avec leur base en Angleterre.

Jacques Soulas habite Lyon, 10 Montée des Carmélites, avec sa femme et ses enfants. Il a repris son travail aux Câbles de Lyon, une couverture impeccable. Retrouvailles. Des télégrammes arrivés par le truchement d'un réseau polonais lyonnais lui avaient annoncé mon arrivée.

Je cherche une chambre meublée. J'en trouve une du côté de Bron, au deuxième étage d'un pavillon de banlieue tout en hauteur. J'achète un vélo d'occasion, objet rare, mais indispensable, payé son poids d'or, que j'utilise aussitôt pour aller chercher la valise cachée sous son buisson de mon terrain d'atterrissage près de Thoissey. Je la retrouve sans difficulté.

J'achète aussi un poste de TSF, qui sera l'alibi pour demander à mon propriétaire la permission d'installer un fil d'antenne en travers de son jardin : « La réception est tellement meilleure, n'est-ce pas, avec une antenne. »

Pour lui, je suis étudiant en droit. J'essaie, sans grande conviction, de m'inscrire en faculté, mais mon manque de connaissance de l'université me fait craindre d'y être trop maladroit et de me faire remarquer.

Émotion lorsque je vais au service du Ravitaillement. Je présente la carte qui me donne droit à ma ration de tickets mensuels de ravitaillement. Elle a été imprimée à Londres, mais il est écrit dessus qu'elle a été délivrée à Paris. « Quelle drôle de couleur ! » dit la préposée. « Vous trouvez ? Elles sont toutes comme ça à Paris. — Ah bon ! » dit la dame. Et me donne mes tickets.

Aussitôt installé dans ma chambre, j'essaie d'établir le contact radio avec l'Angleterre. En vain. J'appelle à tous les rendez-vous, six fois par semaine, trois de jour, trois de nuit. C'est décourageant. Soulas, via le réseau polonais, signale à Londres mes efforts infructueux. Le 20 juin, l'opérateur de la Centrale se réveille : les premiers télégrammes passent dans les deux sens.

Le Paraset , le poste émetteur-récepteur que j'utilise, a pour principales qualités d'être petit et léger. La partie récepteur, d'un type dit « à réaction », est sensible et permet de recevoir des signaux faibles, mais son réglage, un peu acrobatique, varie au gré des fluctuations du voltage de la ligne du secteur électrique, et de la proximité de la main de l'opérateur. Il est peu sélectif : une station puissante, voisine de la longueur d'onde de votre correspondant, matraque facilement vos tympans et rend difficile la lecture du Morse.

L'émetteur a une faible puissance : 4 watts. Sur ondes courtes, ça n'est pas un gros inconvénient, d'autant plus que mon correspondant en Angleterre dispose de récepteurs sophistiqués et des immenses antennes de la Centrale, la « Home Station », STS 53A, située à Grendon.

Écoute rituelle, aussi et toujours, de la BBC, pour entendre les nouvelles de la guerre, sur ondes courtes aussi, bien sûr, malgré le brouillage intense des Allemands. Merveilleuses ondes courtes qui permettent aux faibles de se jouer des puissants !

Pas grand-chose à faire. Le travail de mon patron génère peu de trafic radio : environ cinq télés par semaine. Grandes balades à vélo dans la campagne alentour. Mes muscles à bicyclette, inutilisés depuis l'été 40, fonctionnent toujours bien. Les routes sont vides et je transpire sous le soleil. Je vais me rafraîchir sur les plages de la Saône : j'y retrouve parfois mon patron, sa femme, ses enfants.

Je découvre Lyon, les Lyonnais à l'abord grincheux, les ouragans de poussière de la place Bellecour, les tramways antédiluviens et leurs rails néfastes aux cyclistes, les splendides chevaux de Carpeaux sur la place des Terreaux, la Tour Eiffel à courtes pattes, et sa voisine Notre-Dame de Fourvière qui, comme le Sacré-Cœur de Montmartre, ressemble à un éléphant sur le dos ; et les petits restaurants où, avec un peu d'argent, guerrier sans vergogne, je mange au marché noir et à ma faim.

Vie sur une autre planète qui a pour nom solitude. Rares rencontres avec mon patron, la sécurité exige le cloisonnement, on communique par « boîtes aux lettres ». Je vais bientôt avoir 22 ans, je n'ai aucun ami, aucune amie. Je ne peux, je ne dois parler de rien à personne. Comment esquisser un début d'amitié, d'intimité en se tenant sans cesse sur ses gardes ?

Vigilant, l'esprit doit veiller à ce que rien de ce que je fais ne dépasse de la norme, qu'aucun objet, aucune attitude ou parole puisse susciter la curiosité des autres. Et sans cesse il doit déceler, évaluer dans l'environnement les signes que livrent hommes, voitures, mouvements, anticiper les situations, et m'éviter la confrontation, me guider vers le calme. Mais la solitude...

Par une belle journée du mois d'août, devant la librairie Flammarion, Place Bellecour : Daniel Cordier. Nous étions ensemble à la STS 52, l'école des radios de *Thame Park*. Je revois, un dimanche qu'un groupe de Français Libres étaient allés déjeuner au George, un excellent restaurant d'Oxford, le chic fou de l'uniforme — bleu, filet jonquille — et du képi d'officier de chasseurs, faisant sillage dans la mer des battle-dress kaki. Esprit vif, sens de l'humour, original, la parole un peu zozotante, c'était un des plus agréables compagnons.

Chacun sur son vélo, un pied-à-terre, on se regarde, on regarde alentour, visages de joueurs de poker, le temps de peser la chose, de déceler ce qu'il pourrait y avoir d'inquiétant dans l'environnement.

La sécurité aurait voulu que l'on ne se reconnût point. Le plaisir de se revoir, de rompre la solitude méfiante de notre vie — enfin quelqu'un à qui parler sans crainte de faux pas ! — on rit, on déjeune ensemble chez Colette, place Antonin Poncet, un petit restaurant tenu par une blonde opulente. Colette a un ami inspecteur de police, ce qui assure la quiétude du lieu. On s'y retrouve souvent.

Daniel Cordier — BIP W — a été parachuté à la lune de Juillet 1942. Destiné à être le radio de Georges Bidault — BIP — il est kidnappé par Jean Moulin — REX — qui discerne en lui les qualités qui en feront le secrétaire sans pareil de la Délégation du Général de Gaulle en France jusqu'en mars 1944.

Il m'emmène rôder parmi les rayons de la librairie Flammarion. Orgie de lecture. Daniel me fait découvrir *Les Thibault*, *La Chronique des Pasquier, Les Hommes de Bonne Volonté, Les Copains, À la Recherche du temps perdu, le Journal d'André Gide*, etc., etc.. Quel monde je rencontre là !... Moi à qui, enfant, on interdisait de lire *Poil de carotte* !

Au théâtre antique de Vienne, on joue Antigone. Nous allons voir un soir, mais nous n'osons quand même pas aller souper chez Point[100]...

Le Secrétariat manque de moyens. Daniel a si peu d'argent qu'il a faim. C'est souvent moi qui paie nos steaks-frites de marché noir, puisque mon patron dispose de fonds plus abondants.

Un jour, place de l'Opéra, nous sortons d'un restaurant : Horreur ! Tragédie ! Le vélo de Daniel a été volé. Oiseau à qui on vient de couper les ailes, il contemple, effondré, le désastre. Circuler est vital au secrétaire de REX, le prix d'une bicyclette au marché noir est exorbitant, quelles acrobaties en perspective pour en trouver une autre...

Le Secrétariat manque de liaisons radio. Deux opérateurs : Jean Holley — LEO W — parachuté d'Angleterre, et un radio — BIP Y — recruté en France, essaient en vain de prendre contact avec Londres. Hervé Monjarret — SIF X — le radio de Raymond Fassin — SIF — qui avait été le premier radio à transmettre des télégrammes pour REX — a quitté les transmissions pour être officier de liaison auprès de Francs-Tireurs.

Gérard Brault — KIM W —, un autre ancien de *Thame Park*, arrivé en Juin 1942, pour être le radio de Paul Schmidt — KIM — , officier de liaison auprès du mouvement de résistance LIBERATION, reste seul à assurer le trafic de son patron et celui du Secrétariat de Jean Moulin : jusqu'à six heures d'émission par jour ! Il est surmené au-delà du raisonnable et obligé de prendre des risques absurdes. Situation saugrenue : au même moment, j'écoule mes télés en quelques minutes par semaine. Si peu que je ne m'inquiète pas d'un avertissement venu de Londres : une équipe allemande de radiogoniométrie s'installe dans la région.

Des messages échangés entre Londres, Jean Moulin et mon patron, Jacques Soulas, organisent mon transfert du Commissariat à l'Intérieur vers le BCRA. À la mi-septembre, l'écheveau bureaucratique londonien se démêle, et je passe au service de la Délégation du Général de Gaulle en France, où je commence par soulager Gérard Brault des télés de Georges Bidault, nombreux et longs.

Émission plusieurs heures par jour, parfois jusqu'à cinq ou six, de ma chambre à Bron, le jour. Les cristaux de quartz qui devraient me permettre d'utiliser mes fréquences de nuit sont défectueux. REX est conscient du danger ainsi couru par son nouvel opérateur, et donc par ses transmissions. Il voudrait bien améliorer mes conditions de travail, mais n'y parvient pas.

Il faut que le trafic passe. Il passe. Depuis l'âge de seize ans, radio amateur, je pourchasse les signaux rares et lointains sur des postes de ma fabrication. J'aime ce jeu qui allie l'acuité de l'ouïe à la subtilité technique, et lorsqu'en face de moi se trouve un opérateur de haut vol pour capter les quelques micro volts que je lui lance, écouler les télégrammes est un plaisir : satisfaction du travail bien fait, plus celle de David qui fait un pied de nez au Goliath Chleuh.

L'expansion fantastique des services radioélectriques en Angleterre crée une demande de personnel difficile à satisfaire. Il faut du temps pour former un opérateur. C'est une chose de lire le Morse dans une salle de classe, et c'en est une autre d'extraire ce minuscule signal de la jungle électromagnétique. Tous, l'armée, la Royal Air Force, la Royal Navy, les services secrets, se battent sauvagement pour avoir des radios. Notre centrale parfois bouche les trous avec des apprentis : rendez-vous manqués, répétitions las-

[100] Qui avait la réputation d'être le meilleur restaurant de France.

santes, dangereuses — plus longue est l'émission, plus facile le repérage — dialogues de sourds, erreurs. La température monte, la patience diminue : « La gonio est dans la rue et ces cons-là prennent le thé ! »

On décoche des télégrammes furibonds à l'adresse de la Home Station : « Je ne veux plus travailler avec l'opérateur du 2 août ses signaux sont illisibles ! » — « L'opérateur d'hier ne savait pas manipuler les chiffres 2, 3 et 4... » Moulin s'impatiente : « Voulez vous demander aux Anglais s'ils se moquent de nous ? »

De l'autre côté, ils ne sont pas contents non plus : « Réduisez la durée de vos émissions qui sont beaucoup trop longues. Rappelons qu'EEL[101] ne doit pas prendre contact tous les jours ni plus d'une heure... »

Ils n'ont pas tort : le principe, enseigné à l'entraînement en Angleterre, d'une demi-heure trois fois par semaine est devenu ici la pratique de plusieurs heures par jour. Je proteste bien auprès de ceux qui me submergent de télégrammes. « Il faut que ça passe ! Tu serais dans une tranchée avec une mitrailleuse en face de toi, tu refuserais d'aller à l'assaut parce que c'est trop dangereux ? » Je suis meilleur radio que dialecticien, alors je continue à émettre trop longtemps.

De Londres, début octobre l942 : « BRANDY est en panne, aidez-le. » BRANDY est un réseau d'évasion conçu par le lieutenant d'aviation Christian Martell[102], qui est parti pour l'Angleterre en décembre l941. Se rendant compte du grand besoin en mécaniciens de la Royal Air Force, il offre de revenir en France pour en recruter. Parachuté en avril 1942, il établit, avec l'aide de ses amis d'avant la guerre, une filière d'évasion qui part de Paris et va en Espagne. Avec le premier groupe de mécanos, il retourne en Angleterre rejoindre son escadrille, et laisse la direction du réseau à son frère Maurice (SIMON), qui ajoute au recrutement de mécaniciens d'aviation l'évacuation d'aviateurs alliés rescapés après que leurs appareils eussent été abattus lors de missions au-dessus de l'Europe.

L'adresse est Cours Gambetta. Il y a là un jeune radio, Jean-Louis Mérand, parachuté de Londres en août 1942, et qui ne parvient pas à prendre contact. Le poste qu'il possède est défectueux. Son plan d'émission — microphoto où figurent ses heures de rendez-vous, ses fréquences et ses indicatifs d'appel — a pour nom de code AMBRE. Je l'essaie sur mon poste. Cette fois encore, c'est évident, la Centrale n'est pas au rendez-vous. J'envoie les télés de SIMON sur mon plan.

Chez les radios, il ne s'est rien passé d'inquiétant depuis longtemps. La pression pour transmettre les télégrammes est intense. Le soutien logistique nécessaire — réseau de lieux pour émettre chaque fois d'un endroit différent, équipes de protection pour surveiller les alentours — est inexistant. Les comportements imprudents glissent vers l'absurde. Pendant ce temps la gonio Chleuh écoute et s'approche...

Radiogoniométrie.

Les Allemands sont entrés en zone « libre » avec un service spécial pour la détection des émetteurs clandestins, le *Sonderkommando Kurzwellenüberwachung*, le KWU[103]. DONAR est le nom de code de l'opération, Donar, dieu de la foudre dans le Walhalla, a été bombardé saint patron de la chasse aux radios clandestins. Cent six hommes, sept appareils de gonio mobiles montés sur camion ou sur quelques-unes de leurs 35 voitures. Leur « protection » est assurée par des inspecteurs de la Sureté Nationale française.

L'appareil de radiogoniométrie est muni d'une antenne spéciale qui permet de relever la direction d'où provient une émission. Trois appareils, travaillant ensemble, mais éloignés les uns des autres per-

[101] EEL est le nom de code de mon plan d'émission, et par extension. est devenu le mien.

[102] De son vrai nom Christian Montet. De nombreux volontaires, en Angleterre, changeaient de nom pour ne pas attirer de représailles sur leur famille en France.

[103] Gottlieb Fuchs, l'interprète de Klaus Barbie, dans son livre *Le Renard*, p. 61, écrit que le Sonderkommando KWU dépendait de l'Abwehr, mais qu'avec l'installation de Barbie à Lyon, il était passé sous contrôle du SD. – Dans son *Histoire de la Gestapo*, p. 382-4, Jacques Delarue écrit que le service de l'Abwher avait pour nom Fahndungfunk, et qu'un deuxième service existait : Wehrmacht Nachrichten Verbindung Funk. Delarue écrit aussi qu'un accord entre deux officiers français et l'Abwehr, à l'hôtel Lutetia à Paris au début de septembre 1942, permit l'entrée en zone Sud le 28 septembre 1942 de l'opération DONAR.

mettent de porter sur une carte trois relèvements qui se recoupent et dont l'aire de rencontre dessine un triangle. C'est là qu'est l'émetteur recherché. Les chasseurs s'en rapprochent, réduisant peu à peu la taille du triangle où se trouve leur proie. Finalement, gonio légère à la main, ils font du porte-à-porte, et c'est la curée.

Aux alentours du mois d'octobre 1942, les Allemands repèrent, et les policiers français arrêtent, dans la région lyonnaise, un radio polonais et deux anglais. Le 16 octobre, c'est le tour de Gérard Brault — KIM W.

Un autre jour d'octobre, vers 17 heures, au cours d'une liaison, alors que je passe à l'écoute de la Centrale après lui avoir transmis un télé, je l'entends, à peine, me dire qu'elle ne m'entend plus du tout. La propagation est chamboulée.

La propagation des ondes courtes est aléatoire. On peut, en général, compter sur elle pour franchir une certaine distance, si on choisit bien son heure et sa longueur d'onde. Mais de temps à autre un phénomène, exceptionnel — aurore boréale, tache solaire, orage magnétique, etc. — peut brutalement tout modifier.

Les instructions reçues en Angleterre m'ordonnaient de toujours conduire mes émissions comme si je menais une station commerciale. Habituellement respectueux de ces règles, j'aurais dû, puisque la liaison n'était plus possible, envoyer le signal : QRT de WNG[104], et fermer la station. Paresseux ? Sixième sens ? Ce jour-là je n'ai rien transmis.

Le Paraset rangé, puis caché sur le haut d'une armoire — comme on m'avait appris à le faire à l'école de radio — l'antenne transférée sur le poste de TSF-alibi, qui me donne un peu de musique, et je m'allonge sur le lit, un livre à la main.

Cavalcade dans l'escalier. Grands coups cognés dans la porte, qui s'ouvre violemment. « Police ! Haut les mains ! » Une dizaine de mecs, pistolet au poing. On se croirait dans un film. Il est évident qu'ils ont l'air surpris d'avoir devant eux un môme, qui du lit où il était allongé, se redresse, l'air étonné, un bouquin au bout d'un de ses bras levés. Avec mon visage rieur, je fais plus jeune que les 18 ans de mes papiers d'identité. Ils fouillent, me fouillent, feuillettent les livres, cherchent sous le lit, sous le matelas, sous l'armoire, dans l'armoire...

On voit bien à leur figure qu'ils se sont trompés. La plupart ont l'air allemand, certains sont Français. Un des Chleuhs ne me quitte pas des yeux, des yeux gris, durs. Je n'ai vraiment pas l'air d'un espion, avec mes shorts, mon grand col ouvert et mon sourire de bonne volonté : « Que cherchez-vous donc ? Je peux peut-être vous aider ? » L'un d'eux a trouvé un papier sur ma table. Menaçant : « Ach ! Qu'est-ce que c'est, Monsieur ? — Ben, heu, vous voyez, c'est la liste des postes avec l'heure où ils donnent des nouvelles. Là, *Radio-Paris, la Suisse romande, Stuttgart, la BBC*... » Mais ils cherchent autre chose qu'un auditeur de la radio anglaise. Après un dernier coup d'œil, ils s'en vont.

Si je suis novice et naïf à ce jeu, eux aussi. Sur ma table : un quartz — ce cristal qui sert à stabiliser l'émission sur sa fréquence — oublié lors du rangement... Petit parallélépipède noir, qui leur faisait un clin d'œil qu'ils n'ont pas perçu.

Assis sur le lit, un tremblement irrépressible me saisit. Piégé par mes multiples infractions aux règles de sécurité (infractions obligées par le manque de soutien logistique : émissions beaucoup trop longues, beaucoup trop fréquentes, toujours du même endroit, sans personne pour surveiller les abords), j'ai été

[104] QRT signifie : j'arrête mes transmissions, et WNG était l'indicatif de ma station.

sauvé par une autre infraction, à la règle qui voulait que l'on se donne l'attitude d'une station commerciale : Dans la rue, l'équipe du KWU attendait, pour affiner son relèvement, que je revienne sur l'air. Pendant ce temps je rangeais. Si j'avais, selon la règle, annoncé la fin de mon émission, ses hommes auraient aussitôt bondi, sans me laisser le temps de rien cacher. Ainsi retardés, les Chleuhs fouillent, sans certitude, une demi-douzaine de maisons le long de la rue.

En bas, dans sa cuisine, mon propriétaire est en proie à sa propre trouille : il vient de rentrer un sac de 50 kg de blé acheté au marché noir et il croit être la cible de ces messieurs. Comme ça lui donne l'air coupable, ils lui démontent quelques meubles.

Le calme revient. Je sors faire le tour du voisinage. Ils sont bien partis. Je descends le Paraset et mon pistolet du haut de l'armoire. Les sacoches pleines, j'enfourche mon vélo, pour ne plus jamais revenir.

Le cloisonnement avec le secrétariat est excellent. Nous n'avons de contact que par boîte aux lettres interposée, lorsque je n'ai pas de rendez-vous avec Daniel Cordier. Ils ne connaissent pas mon adresse, je ne sais pas la leur. Seuls endroits où je pourrais me réfugier : chez Jacques Soulas — SALM — mon ex-patron, ou chez Maurice Montet — SIMON — dont je viens de dépanner les transmissions. C'est lui que je choisis, car aller faire des vagues chez Soulas et déranger son excellente couverture, sa femme, ses enfants, ne me paraît pas indiqué. Pour être sûr de n'être pas suivi, je tourne, virevolte et traboule dans Lyon. Atterrissage cours Gambetta, accueil, épluchage et examen des événements. Pour l'instant, je peux manger et dormir là.

Au Secrétariat, on n'est pas heureux. Après l'arrestation de Gérard Brault, et mon esquive de la gonio, ils n'ont plus de liaison radio avec Londres. Un rendez-vous de repêchage — mis en place, justement, pour se retrouver lorsque les choses dérapent — me permet de reprendre contact avec Cordier. Mais ils n'ont toujours pas le moyen de me fournir un lieu sûr où habiter, ni des emplacements d'émission. La Résistance à qui on les demande, est sans doute occupée à répandre ses tracts.

Je passe un accord avec Maurice Montet, le patron du réseau BRANDY. J'assure ses transmissions, pas lourdes, mais qui lui sont précieuses, et il me fournit des points d'émission le long de sa filière d'évasion. Nous avons, son groupe et moi, des atomes crochus : j'habite avec eux. Leur ravitaillement est bien organisé, ce qui évite de s'exposer dans les restaurants.

En vérité, il n'est pas très orthodoxe de mélanger ainsi deux réseaux. Mais il faut faire avec ce que l'on a. Les volontaires aux côtés des Français Libres sont encore rares. Les gens ne croient guère à cette chimère qui nous agite : foutre dehors le tout-puissant Grand Reich.

« Ils ont battu tout le monde, pensez donc, même les Français ! » et « Pétain est un grand bonhomme ! », sont les clichés qui permettent de ne rien faire avec bonne conscience. Il faudra le débarquement américain en Afrique du Nord, et surtout la dérouillée de Stalingrad, pour que commencent à se réveiller ceux que leur bon sens avait engourdis.

La filière BRANDY traverse la ligne de démarcation près de Chalon-sur-Saône, avec l'aide de l'équipe d'André Jarrot, garagiste, ancien coureur motocycliste, de Raymond Basset, capitaine des sapeurs-pompiers, et de Pierre Guilhemon.

Je descends du train à Tournus. Dédé Jarrot est là. Je monte derrière lui sur sa moto, la valise du poste émetteur entre nous. On part à travers la campagne. Une ferme. Accents bourguignons : « Je vous ai apporté la chambre à air[105] que vous vouliez pour le vélo de la p'tite. On pourrait pas s'installer une demi-heure dans un coin ? »

(Copyright (c) Maurice de Cheveigné)

[105] En dehors de son charme bourguignon débordant, Dédé Jarrot savait la façon de s'attirer la bonne volonté des populations. Etant garagiste, il pouvait importer de zone occupée des pièces détachées de vélo, à condition d'y exporter ensuite la quantité de vélos assemblés correspondante. Ce qu'il faisait consciencieusement.
Mais dans le noir de la nuit, quittant sa casquette de garagiste pour celle de contrebandier, il ramenait quelques vélos en zone libre. Puis plus tard, redevenu garagiste, il les représentait une deuxième fois à la ligne de démarcation, obtenant ainsi, avec les mêmes bicyclettes, un nouveau crédit de pièces détachées ! Un excellent matériau d'échange...

Piratage et écoute d'une base TSF :

Beaucoup de français moyens utilisent des téléphones sans fil en le raccordant tout simplement sur une prise téléphonique. Il est possible de le raccorder aussi sur le joncteur d'une ligne analogique derrière un PABX. Que ces appareils soient homologués ou non, le principe de fonctionnement est le même pour tous sans exception.

La généralisation de ce type de matériel pose un grand problème en matière de confidentialité des communications. Les utilisateurs non avertis ignorent bien souvent que tout ce qu'ils disent à leur correspondant peut être intercepté par des récepteurs de surveillance radio larges bandes. Ils comportent souvent un dispositif, qui permet de déclencher un magnétophone automatiquement. On peut se demander légitimement aussi, si la généralisation de ce moyen de communication, n'est pas une volonté de nos gouvernements. Le but est de permettre aux grandes oreilles (stations de surveillance radioélectriques gouvernementales), d'espionner la vie des citoyens moyens, afin de connaître leurs aspirations ou préoccupations du moment, ou même leurs opinions politiques. Ces écoutes anodines, permettent de savoir à la veille d'élection, ce que la population pense de ses politiciens et de compléter les sondages.

En dehors des écoutes, il existe d'autres aspects encore plus sournois. Des particuliers peuvent appeler leur banque pour connaître la position de leur compte. Il peuvent aboutir sur des serveurs vocaux qui peuvent leur demander de composer leur mot de passe et code confidentiel. Le téléachat à distance à travers ces serveurs commence à se développer en France. Les particuliers non techniques imprudents peuvent ainsi transmettre le numéro de leur carte bancaire par T.S.F. pour commander quelque chose.

Un individu en possession de ce type de récepteur, voire même d'un poste CB fonctionnant sur la bande A (ce qui correspond au double inférieur) peut intercepter de multiples communications téléphoniques. C'est ainsi que l'on peut voir des pirates en possession de numéros de carte bancaire qu'il ne devraient pas avoir. Ils peuvent ainsi passer des commandes pour leur propre compte qui seront payées par d'autres à leur insu.

Il faut savoir qu'aucun T.S.F. homologué en France ne peut être crypté. Ceux qui le sont viennent de l'étranger et sont interdits d'utilisation. Pour l'instant, on peut supposer que les écoutes systématiques ne sont pas utilisées par les groupes, ou seulement de façon occasionnelle. Mais rien n'interdit ce développement illicite.

Alors est-il normal que les vendeurs de ces matériels n'informent pas les acheteurs potentiels des risques possibles. On ne voit pas pourquoi il n'existerait pas un décret obligeant les fabricants à écrire sur leurs notices que la confidentialité des communications n'est pas assurée sur ces appareils. Pourquoi il n'est pas déconseillé ou même interdit d'utiliser ces appareils pour des transactions que l'on peut qualifier de financières. Par exemple, pour les jeux vidéo une mise en garde figure sur toutes les notices afin de mettre en garde les épileptiques sur les effets secondaires. Ce moyen de communication est le pire qui puisse exister. Il a en effet permis sur Paris un grand nombre de fuites dans tous les domaines, qu'ils soient politiques, financiers, industriels, scientifiques, voire même militaires. Il ne faut pas oublier que les ambassades sont des grandes oreilles en puissance. Certaines disposent d'antennes assez remarquables, pour que l'on en devine leur utilisation.

Transmissions informatiques radio sans fil :

Les fonctionnaires de Bruxelles viennent de définir la norme IEEE802.11 pour l'Europe). Elle consiste à autoriser les ordinateurs ou autres systèmes à communiquer entre eux de 0,3 à 1,35 Mbit/s dans la bande de fréquence de 2446,5 / 2483,5 MHz.

Deux techniques sur cette bande se dégagent. L'une est a fréquence fixe (DSSS) et l'autre à sauts de fréquence (FHSS). Cette dernière paraît un peu plus sûre que la précédente contre un risque d'écoute. Mais de toute façon quoiqu'en disent les divers constructeurs du marché, ces solutions seront toujours moins sûres qu'une liaison par câble face à des espions.

Il faut en effet savoir que la cryptographie lourde est assimilée à une arme de guerre en France, comme dans beaucoup d'autres pays et est donc interdite. Les communications transiteront donc en clair et pourront être interceptées par n'importe qui utilisant un récepteur fonctionnant sur la bonne fréquence. Utilisé conjointement avec un analyseur de protocole ou encore ces nouveaux équipements appelés *sniffeurs*, un pirate pourra intercepter les adresses IP, les informations transitant sur un réseau.

La norme ETS300-652 (Hiperlan: Hight Performance Radio Lan) disponible depuis 97.

Ces systèmes utilisent les 5 et 17 GHz avec un débit de 10 à 20 Mbit/s.

Ces moyens présentent les sérieux inconvénients d'être écoutés sans aucune restriction comme pour les téléphones sans fil. Le pire, c'est que l'on ne saura jamais si effectivement toutes les données ont été captées par un espion. On peut donc supposer ici aussi qu'il y a une volonté des gouvernements, d'espionner ce qui transite sur les systèmes informatiques, sans connexion physique.

Le danger vient surtout de la possibilité de leurrer le correspondant initial et d'émettre à sa place un signal HF qui pourra comporter sous-programme invisible d'espionnages. Ce type de programme généralement en assembleur ira se camoufler quelque part sur le disque dur et demeurera invisible même lors du listage du contenu du disque. Il attendra le moment opportun pour se charger automatiquement de lui-même. Il transmettra tout seul vers son propriétaire la première fois tout le contenu du disque dur. Les fois suivantes, il se contentera de transmettre les nouveaux fichiers qu'il a réceptionnés d'un autre système informatique autorisé. Il émettra aussi les informations ou les ordres tapés sur le clavier qu'il stockera dans un fichier tampon en attendant l'heure d'émission.

Ce programme fera le nécessaire afin qu'il ne figure aucune modification ou trace dans le fichier historique. Il y a cependant deux problèmes qui permettent de visualiser ce genre de supercherie. Un autre ordinateur superviseur sur le site peut détecter l'activité du modem radio. L'autre problème peut apparaître lorsque le disque dur de l'ordinateur espionné est pratiquement plein. Si on souhaite enregistrer sur le PC un fichier 10 Mega-octets et, que ce dernier vous dit que c'est impossible, alors qu'il nous signale qu'il reste une capacité disponible de 20 Mega-octets, on peut se poser des questions. Il y a dans ce cas un ou des fichiers invisibles quelque part.

Matra Grolier Network se lance aussi dans la bagarre du sans fil, en proposant ici des moyens de communication Internet par satellite pour un débit de 500 kilobits avec un tarif très intéressant. La société israélienne RDC propose un système complet de communication sans fil pour Internet sur 2,4 GHz. Il permettrait d'évincer les opérateurs habituels du câble. Le fournisseur d'accès installe sur son serveur une passerelle qui est raccordée à une antenne omnidirectionnelle sur le toit. La portée possible serait un rayon de couverture de 35 km en fonction du relief avec un débit de 1 Mbit/s. L'abonné ou l'entreprise disposerait d'une antenne parabolique bidirectionnelle de 10 à 20 décibels avec un angle d'ouverture de 14 à 40° connecté sur une Unité de Communication Principale et raccordé à son réseau local. Il y a ici aussi des risques d'interception des transmissions avec des systèmes fonctionnant d'un côté en omnidirectionnel et de l'autre en bidirectionnel pour l'UCP, et omnidirectionnel pour les boîtiers. L'Internet par ces moyens, n'a qu'un objectif, court-circuité les opérateurs nationaux, en proposant des tarifs très bas. Malheureusement, tant que la cryptographie lourde ne sera pas autorisée, ces moyens sont voués à

l'échec pour les sites ou sociétés très sensibles, et c'est valable pour n'importe quel fournisseur français ou étranger.

Les faisceaux hertziens :

Les communications micro-ondes se généralisent de plus en plus. L'intérêt réside dans le fait qu'ils permettent de relier deux sites entre eux sans passer par des câbles. Ils permettent ainsi le transfert de grosses quantités d'information numériques et analogiques dans des zones isolées ou ayant un fort relief accidenté. L'inconvénient, ici c'est que ces types de faisceaux peuvent être écoutés surtout par les services d'espionnage de gouvernements étrangers. Dans ce cas précis, ils préfèrent enregistrer toute la largeur de bande du faisceau et procéder au triage par analyse, ou sélection de mots-clefs. Ils utilisent les fréquences ci-dessous :

-1,5 GHz / 8 voies,
— 4,5 GHz / 1 voie à 2 Mbit/s,
— 8,5 GHz / 1 voie à 2 Mbit/s,
— 10 GHz / 8 voies ou 2 Mbit/s
— 13 GHz / 4 voies à 2 Mbit/s,
— 23 GHz / tout type, distance : 20 km.
— 31 GHz / 4 voies à 2 Mbit/s,
— 38 GHz / 4 voies à 2 Mbit/s, distance : 08 km.

Une chose que l'on sait moins, c'est que ces interceptions peuvent se faire par des satellites très sensibles spécialisés dans ce domaine. Les micro-ondes ont la particularité de se propager en ligne droite. Il est évident qu'il ne s'agit plus ici de travail d'amateur avec quelques milliers de francs, mais d'organisations avec des millions pour ne pas dire des milliards de dollars d'investissement. Si nous restons sur un plan terrestre, il est possible d'intercepter ces faisceaux avec des moyens moindres et de procéder à des réacheminements. Les spécialistes comprendront la méthode, il est inutile que de rentrer dans les détails.

Transmissions informatiques infrarouges (IR) :

Ces systèmes répondent à la norme IrDA1.1 permettant un débit de 115,2 Kb/s. La nouvelle norme Fast IrDA1.1 autorise un débit de 4 Mb/s et est utilisée par l'ordinateur portable *Toshiba Satellite Pro 420*. Mais il a un coût qui est malheureusement dissuasif.

Elles sont suffisamment intéressantes pour être mentionnées. Elles présentent l'inconvénient de ne pas franchir les murs ou autres obstacles qui se trouveraient dans son champ de vision. Mais c'est peut-être aussi un avantage. Les signaux ne pouvant franchir ces murs ne pourront être interceptés illégalement par un concurrent. De plus, nous ne sommes pas confrontés aux interférences entre les divers systèmes.

Il faut se rappeler que la HF et l'informatique ne font pas bon ménage ensemble. Les systèmes sans fil les plus pratiques pour les utilisateurs sont pour commencer les souris, les tablettes et les claviers comme ceux de *Keytronic*. Ensuite on a des portables comme *Compaq* ou *Toshiba* qui intègrent un module de transmission IR autorisant un débit de 1 à 4 Mb/s.

La société *AB SOFT* vend des modules que l'on peut raccorder sur les prises séries des ordinateurs et sur les prises parallèles des imprimantes.

EXTENDED SYSTEM commercialise la gamme Jeteye qui comporte des modules IR pour Ethernet en 10base T, 10base 2, pour port série et parallèle.

Certains dispositifs utilisant le procédé infrarouge sont utilisés aujourd'hui à des fins d'espionnages. Ces systèmes permettent d'écouter les dialogues dans une pièce à condition que les diodes d'émission infrarouges puissent être orientées vers l'extérieur par une fenêtre. Ce type de signal contrairement aux ondes radio ne passe pas à travers les murs.

Les gadgets d'espionnage électronique

Les microémetteurs :

Il existe une multitude de moyens miniaturisés proposés dans les revues d'électroniques ou spécialisées dans la sécurité. Certaines boutiques dans des galeries situées sur les Champs Élysée proposent ce genre de matériel. Ils utilisent généralement une fréquence dans la bande FM. Ces gadgets peuvent être dissimulés dans les murs, le mobilier, l'installation électrique, téléphonique, informatique et même la plomberie. Pour ce dernier cas, je ne rentrerai pas dans les détails. Il n'est pas utile de donner des idées. On les trouve sous les formes les plus diverses et parfois inattendues.

— sucre sur ligne PTT, - sucre sur ligne EDF,
— pastille téléphonique, - stylos émetteur,
— calculatrice émettrice, - bague émettrice,
— livre émetteur, - bouton émetteur,
— agendas émetteur, - montre émettrice,
— téléphone émetteur, - ou même combiné émetteur,
— prise PTT émettrice, - multiprise émettrice,
— prise EDF émettrice, - horloge émettrice.
— câble dont l'émetteur est dissimulé dans la gaine.

Tous les systèmes ci-dessus existent. Le fin du fin consiste à disposer d'un microémetteur que l'on déclenche sur commande afin de rendre la détection de ce type de matériel plus délicate. Mais si pour déclencher l'émetteur, on utilise un récepteur de radio-télécommande si je puis dire, son oscillateur local s'il est mal blindé va rayonner lui aussi une infime énergie, qui risque de trahir sa présence. Dans le cas du téléphone, la dissimulation et la mise en route sont plus faciles. L'émetteur ne peut se déclencher que lorsqu'on décroche le combiné, si on ne souhaite intercepter que les communications téléphoniques. On intercepte ensuite les conversations jusqu'à une centaine de mètres ou plus, tout dépend de la puissance du sucre émetteur et des obstacles présents, avec un récepteur radio équipé d'un enregistreur minicassette. Ce dernier ne se déclenchera que si le sucre émetteur capte une voix dans le local ou il se trouve. Une autre méthode consiste aussi à piéger les équipements d'instrumentations destinés à un laboratoire. L'intérêt de ce moyen consiste surtout à réémettre numériquement vers l'extérieur en priorité les résultats des expérimentations en cours du laboratoire. Si on allume l'appareil, on assimile ainsi les signaux captés à la multitude d'oscillateurs, d'horloges du système. L'appareil stoppé, l'émetteur est indétectable.

Les caméras CCD :

La nouvelle technologie miniaturisée permet l'utilisation d'appareils photographiques, mais aussi de caméras CCD miniatures dont les dimensions n'excèdent pas un cube de 25 mm de côté. Il y en a de plus petites encore, mais plus rares à des prix exorbitants et réservées pour des applications spécifiques comme dans le domaine microchirurgical. Elles peuvent être couplées à un émetteur d'une portée de 50 à 300 mètres. Ce type de matériel est généralement dissimulé dans un objet d'ornement qui sera installé sur un bureau, une cheminée, un buffet. On les trouve aussi intégrés sous les formes ci-dessous avec un émetteur. Leur réalisation est évidemment plus complexe et coûteuse. Leur utilisation ne se fait donc que dans les cas vraiment extrêmes.

— pommeau d'une canne,

— dans une broche,
— dans une cravate,
— dans une montre,
— une horloge,
— une mallette,
— un livre,
— derrière un miroir sans tain,
— un objet d'ornement
— un radar infrarouge.
— caméra cachée dans un mur avec canne endoscopique,
— même dans des détecteurs incendie raccordés à une centrale de gaz halons[106], ce qui est ridicule et interdit, car ce type d'installation est soumis à des contrôles annuels obligatoires. D'ailleurs à plusieurs reprises des faux détecteurs ont été trouvés avec une caméra dans certaines entreprises déclenchant le mécontentement des syndicalistes. Ce qui est justifié.

Par contre, sur des sites sensibles, des centres de recherche, les accès aux laboratoires et non pas l'intérieur, ce genre de système me paraît parfaitement justifié. Ces espions optiques peuvent être repérés par un dispositif qui détecte le signal de balayage de ligne des caméras. Ce genre de matériel est plus rare, car il a un coût, un volume, et une consommation non négligeable malgré sa miniaturisation. Il faut cependant savoir que ce type de matériel existe. Nos dirigeants d'entreprises sensibles ne sont pas toujours préparés à ces nouvelles menaces, surtout face à des concurrents étrangers virulents dans le domaine militaire ou scientifique. Ce genre d'affaires n'est d'ailleurs pratiquement jamais dévoilé au grand public. La détection de l'émission HF se fait avec les mêmes moyens que pour les sucres émetteurs. Les spécialistes de ces activités sont souvent électroniciens et sont des as de la débrouille.

Des moyens variés :

D'autres méthodes consistent à utiliser des dispositifs d'émission et de réception infrarouge. L'inconvénient, c'est qu'il ne fonctionne qu'en portée optique, c'est-à-dire que si une personne passe devant ou qu'elle met un meuble sur la trajectoire du faisceau, elle coupe la transmission. Ils ont par contre l'avantage d'être indétectable, car même un radioamateur ne dispose pas de récepteur IR et il faut être dans l'axe de ce type de système. Bien que discret il est peut employé en raison de cette contrainte de portée optique.

Il y a aussi des moyens non électroniques originaux dont certains sont connus des Russes depuis longtemps. Il y a le principe de la résonance d'un matériau. Un cendrier de cristal réalisé avec le matériau approprié et taillé d'une certaine façon peut vibrer en fonction des sons générés dans le local où il se trouve. Il peut vibrer de la même façon qu'un diapason dont le son sera modulé par les personnes qui parleront à côté. La qualité et la portée sera médiocres évidemment, mais c'est le genre de truc que l'on peut trouver dans les cas extrêmes. Il est évident que les détecteurs habituels de micro ne servent pas à grand-chose. On peut aussi utiliser des matériaux ferromagnétiques très denses qui donneront un résultat équivalent.

Un moyen plus connu concerne la réflexion d'un faisceau laser sur la vitre d'une fenêtre. La vitre vibre en effet en fonction des bruits générés dans le local. Après traitement du signal réfléchi, on peut écouter ce qui se dit dans un bureau. Les paroles sont des vibrations sonores qui excitent les vitres modulant en même temps le faisceau du laser. Le petit problème c'est que dans le cas d'un double vitrage, le système devient inopérationnel. Un autre moyen repose sur l'utilisation des micro-ondes. Ce qui peut s'appliquer à un faisceau laser, peut aussi s'appliquer à des hyperfréquences dont une partie de l'énergie traversera

[106] Les halons 1211 (CF2BrCl) et 1301 (CF3Br) s'utilisent dans le secteur de l'extinction des incendies et comme anti-explosif.

les obstacles. Si entre deux obstacles il existe une vibration sonore, les micro-ondes récupérées de l'autre côté, auront subi une modification lors de ce passage. Je ne rentrerai pas plus dans les détails. Ce moyen n'est pas sans effet sur la santé.

Systèmes informatisés d'interception radio :

Nous arrivons ici dans la dernière génération d'équipement. L'évolution technologique, l'informatique, le traitement numérique, permettent l'intégration de plusieurs fonctions pour le même coût. C'est maintenant la qualité des logiciels intégrés qui permet de faire la différence surtout au niveau des tarifs.

L'élément primordial est un châssis d'ordinateur dans lequel on va intégrer des interfaces d'interception radio. Le tout sera piloté par un ou plusieurs sous-programmes. L'interface utilisateur standard de base est aujourd'hui le système Windows. Habituellement un système radio ou de mesure disposait d'une façade avant avec des boutons fixes immuables. Chaque appareil remplissait une fonction bien précise. Aujourd'hui, ce n'est plus le cas. Le principe modulaire permet de disposer d'un châssis dans lequel on rajoute des modules spécialisés. Le tout est ensuite piloté par une unité de traitement externe, un PC avec Windows sur lequel on fait apparaître les commandes nécessaires aux besoins du moment. La façade d'un récepteur radio, d'un mesureur de champ, d'un système gonio, se retrouve ainsi affiché sur un écran d'ordinateur.

Il est évident que tout le matériel de laboratoire cité ci-dessus, bien qu'il soit destiné à la mesure ou l'étalonnage des systèmes, permet l'interception de pratiquement tous les types de communications. Un groupe et d'autres, disposant de spécialistes peut être tenté d'utiliser tous ces moyens à des fins d'espionnage pour contrer la concurrence. Face à des marchés porteurs qui se chiffrent aujourd'hui à plusieurs centaines de millions de francs, le risque de ce genre d'activité va en grandissant et semble être utilisé en raison de la baisse des prix, de la disponibilité du matériel, de son ergonomie et ses facilités d'utilisation.

Les capitales qui ont des ambassades et des consulats, sont les plus exposées à ces interceptions. C'est pour cette raison que tous les moyens sans fil représentent un danger pour les utilisateurs, qu'ils soient des particuliers ou des officiels. Quel est le juge, policier ou avocat qui pense à demander à son correspondant s'il utilise un téléphone sans fil ou poste fixe. Les moyens sans fil utilisés dans les villes où sont installées des ambassades, sont à l'origine d'un très grand nombre de fuites.

Les moyens d'enregistrement radio :

Les systèmes sophistiqués de réception radio comportent tous des sorties, prise d'écoute et prise de magnétophone. Ils disposent aussi de plusieurs prises FI (fréquence intermédiaire) standardisées aujourd'hui à 30 KHz/ 75 KHz/ 1,44 MHz/ 10,7 MHz /2 MHz/ 21.4 MHz. Cela permet le raccordement d'enregistreurs audio de divers types avec des durées variables qui s'échelonnent de 1 à 25h par piste à diverses vitesses. Les baies conventionnelles d'ancienne génération équipées de deux magnétophones de 40 pistes chacune avaient des durées de 25h. Maintenant on trouve des systèmes moins volumineux capables d'enregistrer la même capacité sur une bande vidéo. D'autres systèmes plus sophistiqués permettent d'enregistrer à partir de la FI tout une partie du spectre radio. La sortie FI d'un récepteur radio est envoyé vers l'entrée d'un convertisseur qui permet d'abaisser la fréquence d'une partie du spectre pouvant atteindre de 1 à 10 mégahertz, ensuite ce signal arrive sur un enregistreur large bande. Cette solution permet de traiter les données ultérieurement sur place ou ailleurs. Il suffit de repasser la bande en reconvertissant le signal dans l'autre sens et de l'envoyer vers l'entrée FI d'un récepteur ou d'un système d'analyse. On utilise aujourd'hui des ordinateurs de plus en plus sophistiqués et rapides. On peut donc enregistrer du son ou de l'image sur disques durs à ou autres supports à condition qu'il dispose des interfaces d'entrées nécessaires, comme la reconnaissance vocale. Ensuite s'il dispose de logiciel de traitement ou d'analyse de la voix, on peut lui demander de mettre à part les communications téléphoniques ou radio contenant

des mots-clés particuliers. Il pourra au besoin transcrire la langue écoutée en texte. Ce texte pourra être classé dans un thème et traduit par un logiciel dans une autre langue. C'est dans ces cas précis que des logiciels d'analyses basés sur le langage-pivot comme Taïga trouvent leur intérêt. Il est en effet impossible à un opérateur d'écouter des centaines de conversations françaises ou étrangères sans des artifices. Ils permettent ainsi de faire un tri très sélectif et de ne retenir que l'essentiel. Il est aussi nécessaire de surveiller l'activité des opérateurs sur notre territoire.

Espionnage de tous les systèmes sans fil

Une mise en garde est aussi a effectuer sur tous les équipements sans fil :

— Clavier d'ordinateur sans fil,
— Téléphones portables, DCS, GSM, UMTS[107],
— Téléphone sans fil, analogique ou DECT[108],
— Boucle locale radio pour la téléphonie fixe,
— Boucle locale radio pour les échanges de données informatiques type *Tetra*
— Liaisons Wifi[109]
— Liaison Bluetooth[110]

Tous ces systèmes représentent des dangers d'espionnage très sérieux, surtout dans les grandes villes comme Paris. Nous avons pu constater une disparition des téléphones filaires dans les grandes surfaces, au profit des téléphones sans fil. Les dirigeants politiques en voulant encourager le tout sans fil surtout pour inciter la population à utiliser les systèmes ci-dessus, commettent une grave erreur, car ils vont favoriser l'espionnage à grande échelle. Non seulement ils vont se pénaliser eux-mêmes, mais vont aussi pénaliser notre économie et nos entreprises. De nombreuses ambassades dans les grandes capitales, disposent d'équipements d'interception radioélectriques destinés à faire de l'espionnage.

La bêtise des fanas du gadget, c'est l'utilisation des claviers sans fil. Pour une certaine marque d'ordinateur, on a découvert que celui-ci transmettait toutes les informations tapées au clavier jusqu'à une distance qui dépassait largement les 250 mètres. Ou alors, cet ordinateur a été sciemment vendu avec cette défaillance, pour permettre l'espionnage des transactions à l'intérieur de cette société.

Dans le synoptique ci-dessous, nous avons mis en évidence les différents points d'interception possibles. Les ambassades peuvent être dotées de moyens lourds, récepteurs à large bande et enregistreurs, permettant d'enregistrer tout un spectre de fréquence. En effet, contrairement à ce que peut penser le

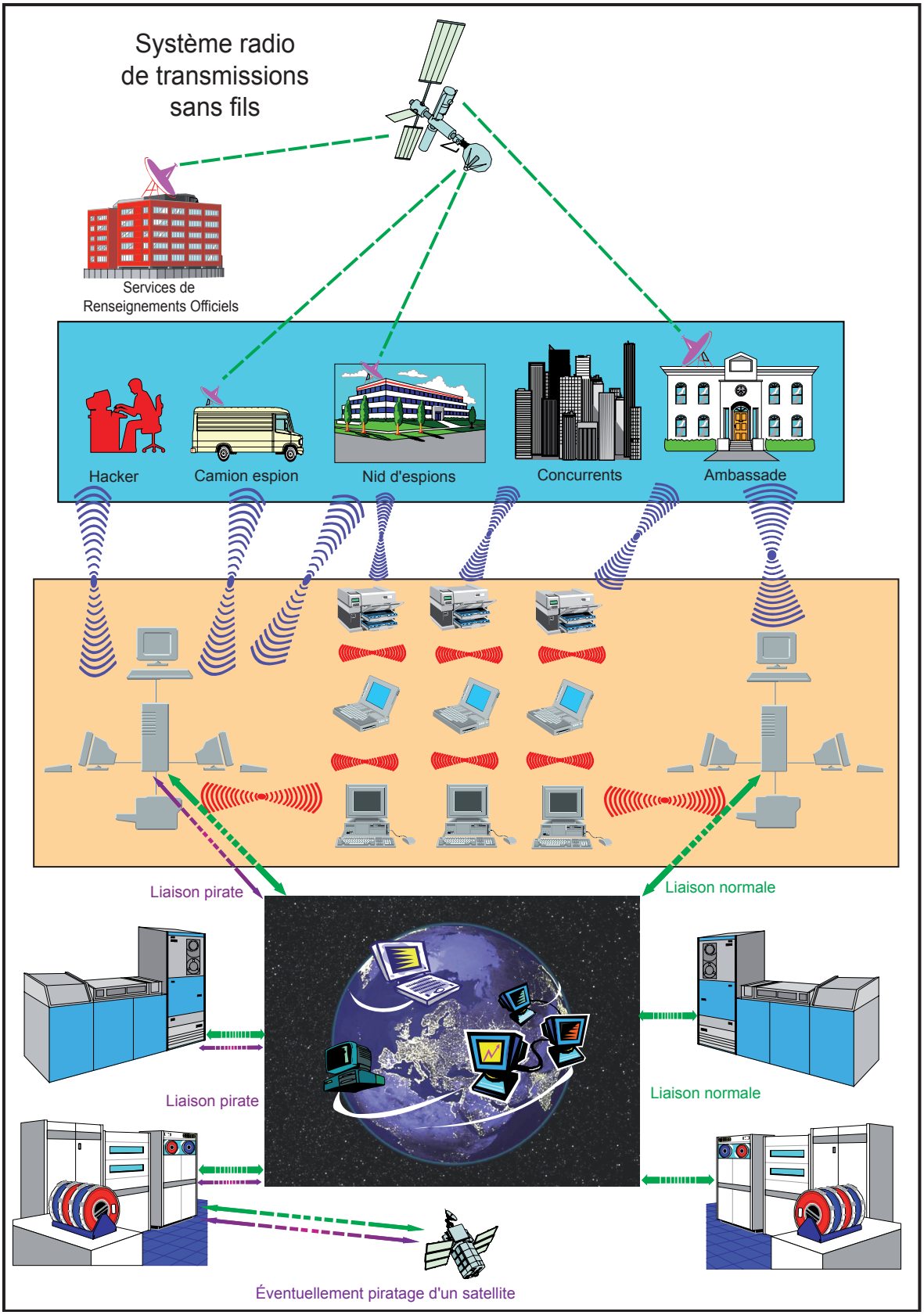
[107] Universal Mobile Telecommunications System (UMTS) est l'une des technologies de téléphonie mobile de troisième génération (3G). Elle est elle-même basée sur la technologie W-CDMA, standardisée par le 3GPP et constitue l'implémentation européenne des spécifications IMT-2000 de l'UIT pour les systèmes radio cellulaires 3G. L'UMTS est parfois aussi appelé 3GSM, soulignant l'interopérabilité qui a été assurée entre lUMTS et le standard GSM auquel il succède. On l'appelle également et plus simplement 3G, pour troisième génération.

[108] Digital Enhanced Cordless Telephone abrégé en DECT (Téléphone sans-fil numérique amélioré), anciennement Digital European Cordless Telephone, est une norme de téléphonie sans-fil numérique destinée aux particuliers comme aux entreprises sur la gamme de fréquence 1880 à 1900 MHz (micro-ondes). Cette norme, même si elle a été conçue pour une gamme large d'utilisations, est aujourd'hui principalement utilisée pour des communications vocales.

[109] Wi-Fi (également orthographié Wi-fi, WiFi, Wifi ou encore wifi, prononcé /wifi/) est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à Internet.

[110] Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les claviers, les souris, les téléphones portables, les PDAs et les appareils photo numériques.

néophyte, il n'est pas nécessaire de disposer d'un récepteur pour chaque fréquence que l'on souhaite écouter.



Il y a de plus en plus de moyens qui sont apparus et permettent de pirater les systèmes.
1°) au milieu des années 70, il suffisait de disposer d'un Minitel et d'une ligne téléphonique.
2°) à partir de 1990, il suffisait d'un PC avec un modem et une ligne téléphonique.
3°) à partir de 1995, il suffisait d'un PC avec un modem et une ligne téléphonique et Internet.
4°) à partir de 2000, il suffira d'un PC avec un dispositif radio pour accéder anonymement aux flux de données informatiques et aux gros systèmes, même les plus sensibles, via Internet.

Les boucles locales radio haut débit en 3,6 ou 26 GHz constituent une brèche importante que les services secrets étrangers peuvent exploiter contre les entreprises nationales françaises et autres. Il faut aussi rajouter les systèmes Tétra en 450 MHz.

Même s'il existe un système de protection des données, en réalité celui-ci est rarement activé par les administrateurs ou responsables informatiques, pour améliorer la compatibilité des transmissions entre le réseau informatique fixe de la société, et les ordinateurs portables des ingénieurs et commerciaux.

Les systèmes d'échange de données entre ordinateurs ou périphériques, permettent à n'importe qui disposant de bonnes compétences informatiques, de s'introduire localement dans les systèmes informatiques. Il est possible par exemple d'intercepter les fichiers destinés à un autre ordinateur ou même à une imprimante.

La cryptographie n'est pas fiable, ni les firewall[111], car la grande majorité a été testée par la NSA (entre autres), ce qui veut dire qu'ils connaissent les failles pour que leurs services de renseignement puissent pirater nos systèmes. De plus, comme nous le verrons par la suite, la réglementation en matière de cryptage est (en France en particulier) restrictive et limitante.

[111] Pare-feu : élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

« ECHELON »
Le réseau mondial qui vous écoute

La chronologie du Réseau

1941 : Après l'attaque japonaise de Pearl Harbor, le centre d'écoute de Bletchley Park est développé en Grande-Bretagne par les Anglais et les Américains pour intercepter et décoder les communications militaires des Allemands et des Japonais. C'est le projet ULTRA.

17 mai 1943 : L'accord Brusa est signé entre le Royaume-Uni et les USA : il s'agit d'une coopération en matière de renseignement électronique. Les cryptanalystes chargés par le gouvernement britannique de casser le code de chiffrement de la machine allemande Enigma, regroupés à Bletchley Park autour du mathématicien Alan Turing, étaient parvenus à de spectaculaires succès, et avaient accepté de faire part de leurs découvertes aux Américains.

2 septembre 1945 : Traité de Sécurité entre les États-Unis et le Japon.

5 mars 1946 : La Grande-Bretagne crée le *Commonwealth Sigint Organisation*, avec le Canada, l'Australie et la Nouvelle-Zélande. Le Pacte UKUSA est en gestation.

1947 : Création de la première station d'écoute à Hong Kong. Dirigée par les Britanniques, elle a permis de préparer les bombardements américains sur Hanoï et d'obtenir des précisions sur les rapports de force du Politburo Vietnamien lors des pourparlers de paix.

1947/48 : Le pacte UKUSA est prorogé. Ce pacte secret conclu, pendant la Seconde Guerre mondiale, entre la Grande-Bretagne et les États-Unis, organise la collaboration des services de renseignement des deux pays dans le domaine de l'espionnage des télécommunications. Le Canada (7 juin 1948, dans le cadre du pacte CANUSA avec les USA), l'Australie et la Nouvelle-Zélande se joignent à ce pacte de coopération et d'échange des informations recueillies. Cibles principales : l'URSS et les pays communistes.

24 octobre 1952 : Aux États-Unis, création de la NSA (National Security Agency) par une directive de huit pages (National Security Council Intelligence Directive N°9)[112] du président Truman en remplacement de l'AFSA (Armed Forces Security Angency). La NSA est chargée, au sein des services de renseignement, des opérations SIGINT (signal intelligence), c'est à dire de l'espionnage électromagnétique (surveillance des liaisons radios, des émissions radar, des télécommunications, etc.) et de la conception des systèmes de codage et de cryptage destinés à assurer la confidentialité des communications du gouvernement, des diplomates et des militaires américains.

1957 : Reconnaissance officielle de la NSA par le gouvernement américain.

25 août 1960 (ou 1961) : Naissance du NRO (National Reconnaissance Office), agence fabriquant des satellites-espions, suite à une controverse entre la Maison Blanche, la CIA et le DoD pour déterminer qui aurait la responsabilité des reconnaissances par satellite du pays. Son existence sera niée jusqu'en 1992.

1966 : La NSA prend le contrôle de la base de Menwith Hill (nord de l'Angleterre) qui était jusque-là dirigée par l'armée américaine. Elle en fera la plus grande station d'interception du monde.

8 Juin 1967 : Le navire USS Liberty est coulé par l'aviation israélienne qui l'avait confondu avec un bateau égyptien : le bilan fait état de 34 morts, 170 blessés.[113]

[112] Disponible sur Internet, archives déclassifiées de la NSA.

[113] Le 2 juillet 2003, l'agence de sécurité nationale (NSA) a libéré l'information additionnelle relative à l'attaque du 8 juin 1967 sur le « U.S.S. Liberty ». Ce document inclut trois enregistrements audio, et transcriptions (en anglais), trois rapports de suivi, et un rapport *Cryptologic* d'histoire des États-Unis intitulé « *Attaque sur un collecteur de SIGINT, l'USS. Liberty* » Les enregistrements sont en hébreu et contiennent des décomptes de temps, en anglais, qui ont été ajoutés par l'opérateur d'interception. Les rapports de suivi sont des résumés des trois transcriptions, avec omission des paroles hors action, et un rapport compilé qui récapitule l'activité et contient le texte des transcriptions. Le rapport *Cryptologic* d'histoire des États-Unis est une version moins développée du même document à l'origine, libéré en 1999.
Comment l'information a été obtenue : Une heure après avoir appris que le « Liberty » avait été torpillé, le directeur de la NSA, le LTG Marshall S. Carter, USA, envoie un message à tous les emplacements d'interception demandant une recherche spéciale de toutes les communications qui pourraient refléter l'attaque ou la réaction. Aucune communication n'était disponi-

Août 1968 : Lancement du premier satellite COMINT américain sous le nom de code CANYON, puis d'un second. Ils étaient contrôlés depuis la station de Bad Abling, en Allemagne, et visaient l'URSS. Ils furent placés à proximité d'orbites géostationnaires afin de couvrir en permanence les cibles sélectionnées. Cinq autres satellites de cette classe furent lancés jusqu'en 1977.

1970 : Création de la station de Yakima dans le Nord-Ouest des États-Unis, en même temps que la première génération de satellites INTELSAT. La station est dotée d'une grande antenne orientée vers le Pacifique.

Octobre 1971 : Le sous-marin USS Halibut, croisant dans la mer d'Okhost, au large de la côte Est de l'URSS, enregistre les communications passant dans un câble militaire reliant les quartiers généraux de l'armée à Vladivostock à la péninsule du Kamchatka. Il était équipé d'une capsule de plongée à très basse profondeur fixée à la poupe du bâtiment et décrite par la Navy comme « un canot de sauvetage à basse profondeur ». En 1972, il lâcha une nacelle d'enregistrement à haute capacité à côté du câble qui fonctionna jusqu'en 1982, quand un employé de la NSA informa les Soviétiques de l'opération IVY BELLS.

1972 : Le GCHQ commence à « exploiter » une nouvelle station secrète à Morwenstow, non loin de Bude en Cornouailles, Angleterre. Cette station, dotée de trente antennes satellitaires, permettait d'intercepter les communications satellites au-dessus de l'Atlantique et de l'océan Indien.

1972 : Création au sein de la NSA, par mémorandum présidentiel, du Central Security Service chargé de coordonner les activités de cryptologie, de gérer les procédures d'écoute et de sécurité électronique du DoD. Il assure également la liaison avec les autres organes de renseignement et de sécurité.

1974 : Construction à Menwith Hill de la première grande antenne satellitaire.

8 août 1975 : Le Directeur de la NSA, Lew Allen, reconnaît, devant la Chambre des Représentants, que « *la NSA intercepte systématiquement toutes les communications internationales, qu'elles soient vocales ou par câbles* », il s'agit de l'opération SHAMROCK.

Juin 1978 : Lancement du premier satellite CHALET, suivi par un second en octobre 1979. Après que le nom du premier satellite fut apparu dans la presse américaine, ils furent rebaptisés VORTEX, avant d'être rebaptisés MERCURY en 1987, à la suite d'une nouvelle fuite.

1978 : Le Congrès adopte une loi (Foreign Intelligence Surveillance Act) définissant les procédures d'écoute de la NSA.

Eté 1979 : Le sous-marin USS Parche, fait le voyage de San Francisco à la mer de Barents en passant au-dessous du Pôle Nord et installe un nouveau système d'enregistrement des informations par câbles près de Mourmansk. Il est toujours en activité et reçut de hautes récompenses, chaque année de 1994 à 1997.

1980 : Entrée en service de la station de Sugar Grove dans l'Est des États-Unis (cette station existait déjà pour écouter les communications russes) afin de s'adapter à la deuxième génération de satellites INTELSAT. Une autre station est installée à Hong-Kong .

1981 : La NSA et le GCHQ construisent le premier réseau global à grande échelle (Wan). Jusqu'au milieu des années 90, ce réseau international, qui permettait de relier les stations SIGINT et les centres de traitement, était plus important qu'Internet. Le réseau est constitué de câbles transocéaniques et de liaisons spatiales. La plus grande partie des capacités des satellites de communications militaires américains et britanniques, Milstar et Skynet, est consacrée à transmettre des données pour les services de renseignement.

1985/87 : Projet de création d'un réseau mondial de surveillance des télécommunications révélé par le journaliste britannique Duncan Campbell. Le principe du projet F 415 est de relier entre elles, grâce

ble. Cependant, une des plateformes aéroportées, le U.S. Navy EC-121, avait rassemblé des conversations entre deux pilotes israéliens d'hélicoptères et la tour de contrôle du terrain d'aviation de Hazor suivant l'attaque sur le « Liberty ».

à de puissants ordinateurs, les différentes bases d'interception des pays du pacte UKUSA qui sont disséminées à travers le monde.

Février 1983 : M. Thatcher fait surveiller par Echelon les conversations de deux de ses ministres (selon les informations de Mike Frost, ancien du CSE canadien).

1986 : Deux soldats américains étaient tués dans l'explosion d'une discothèque à Berlin-Ouest. L'attentat n'a pas été revendiqué. Pourtant, l'État commanditaire, la Libye, a été immédiatement identifié par les États-Unis : la NSA avait intercepté et décrypté les communications entre les ambassades de Tripoli à Berlin-Est et Rome. Quelques minutes après l'explosion, un membre des services secrets de Kadhafi disait : « *L'opération a bien eu lieu. Elle n'a pas laissé de traces*. » Quelques jours après, Reagan autorisait le bombardement de la capitale libyenne.

1988 : Lors d'une visite en Australie, Bob Tizard, ministre de la Défense néo-zélandais, révèle que deux nouvelles bases en construction ne sont pas destinées aux communications militaires, mais à intercepter les satellites de communications civiles lancés par les pays du Tiers Monde tels que l'Inde et l'Indonésie.

12 août 1988 : Ducan Campbell rédige le véritable premier article sur Echelon, publié dans l'hebdomadaire britannique « *News Statesman* ». Depuis lors, il ne cessera de réunir des éléments sur ce réseau.

1989 : La chute du mur de Berlin entraîne la redéfinition des priorités stratégiques des États-Unis. La conquête des marchés mondiaux est désormais l'objectif majeur.

1990 : La NSA intercepte les communications entre le fabricant japonais de satellites NEC et l'Indonésie pour la fourniture d'un contrat de 200 millions de dollars. Le président Bush intervient auprès de Djakarta. Le contrat sera partagé entre NEC et l'américain ATT.

1990 : Inauguration des nouveaux locaux de l'ambassade de Chine en Australie. Lors de la construction du bâtiment, des agents américains ont installé de multiples micros et des systèmes de surveillance des communications dans tous les murs. Les informations recueillies sont transmises directement par satellite au quartier général de la NSA dans le Maryland aux États-Unis.

Juillet 1990 : Les satellites Keyhole ont vu le déploiement des troupes irakiennes à la frontière du Koweït. Le 27, six jours avant l'invasion, les capteurs infrarouges ont repéré les camions militaires transportant de l'eau, du gasoil et des munitions.

19 août 1991 : Lors du putsch de Moscou, la NSA obtient des photos de Gorbatchev emprisonné dans sa maison ainsi que des enregistrements de toutes les discussions téléphoniques entre les chefs rebelles. Avant tout le monde, Bush sait donc que le coup d'État ne réussira probablement pas.

3 septembre 1991 : Un document, aujourd'hui déclassifié, précise la mission du centre de surveillance électronique de l'US Navy, à Sugar Grove (Virginie Occidentale), en liaison avec le 544ème groupement de renseignement.

1991 : L'émission britannique *World in Action* effectue un reportage sur le fonctionnement d'un ordinateur Dictionary situé dans la station londonienne du GCHQ sur Palmer Street, Westminster (station UKC1000). L'émission cita des employés du GCHQ, qui souhaitaient rester anonymes : « *Ici au troisième, [le GCHQ] a engagé un groupe de spécialistes de la sécurité de British Telecom... Ça n'a rien à voir avec la sécurité nationale. C'est parce qu'il est illégal d'intercepter tous les fax. Et pourtant ils prennent tout ce qui passe* : *ambassades, contrats, vœux d'anniversaire, tout y passe. Et ils mettent tout dans le Dictionary*. »

1991 : Plus de 12 tonnes de cocaïne sont saisies grâce aux informations fournies par la NSA qui intercepte, à partir du Venezuela, toutes les communications des membres du cartel de Cali.

8 avril 1992 : dans son discours d'adieu à l'état-major de la NSA, le vice-amiral William Studeman, alors directeur de la NSA, décrit comment les « *demandes pour un accès global accru [aux communications]se multiplient. La partie commerciale de cet accès global est une des jambes, qui, espérons-le, sera solide, sur laquelle la NSA devra s'appuyer au siècle prochain* ».

1992 : L'arrestation pour espionnage d'un attaché commercial de Crypto AG par le gouvernement iranien devait entacher la réputation d'indépendance de la firme helvétique, soupçonnée d'avoir fourni depuis des décennies les clés de cryptage à la NSA.

1992-93 : La NSA espionne les communications des officiels mexicains qui négocient l'ALENA (Accord de Libre-échange Nord-américain) avec les États-Unis et le Canada.

1993 : Au cours du sommet de l'APEC (forum de coopération Asie-Pacifique), la NSA et le FBI installent des équipements capables d'écouter les communications des 15 dirigeants des pays de la zone Asie-Pacifique conviés à Seattle, aux États-Unis, par Bill Clinton. Certaines informations collectées semblent avoir été transmises à des chefs d'entreprises qui ont financé la campagne électorale du président américain.

1994 : Début du démantèlement de la station de Hong Kong : les antennes sont transférées en Australie.

1994 : Lors du bras de fer entre les États-Unis et l'Union européenne dans les négociations du GATT, le réseau Echelon est utilisé par Washington pour connaître la position de chacun des 15 pays de l'UE et la stratégie de la Commission européenne. Des consignes seront données aux fonctionnaires de Bruxelles leur demandant de ne pas utiliser le courrier électronique, dont l'usage commence à se généraliser, pour transmettre des informations sensibles.

1994 : Interception des négociations entre le fabricant français de radars Thomson-CSF et les autorités brésiliennes. La NSA aurait donné le montant des « dessous de table » au Président Bill Clinton, qui serait par la suite intervenu auprès du gouvernement brésilien. C'est finalement la firme américaine Raytheon qui décrochera le contrat pour assurer la couverture radar de l'Amazonie.

1994 : Le directeur de la NSA, John Mac Connell, déclare : « *Il n'y a pas un seul événement de politique étrangère qui n'intéresse le gouvernement américain et auquel la NSA ne soit pas directement mêlée.* »

1994 : La NSA intercepte les coups de téléphone et les fax entre Airbus et les autorités saoudiennes. Le contrat de 6 milliards de dollars sera décroché par Boeing.

20 juillet 1994 : Bill Clinton renonce au projet de la NSA (remontant à la présidence de G. Bush) de doter chaque ordinateur ou chaque téléphone produit aux USA d'une *clipper chip* (ou puce pirate) permettant de surveiller les communications.

16 septembre 1994 : Les motifs stratégiques d'Echelon sont exposés dans un mémorandum confidentiel de la Maison-Blanche : « *la fin de la Guerre froide a dramatiquement changé les priorités et les menaces vis-à-vis de notre sécurité nationale. Outre les questions politiques et militaires traditionnelles, les thèmes économiques suscitent une préoccupation et un intérêt croissant* ».

1995 : L'envoyé de Bill Clinton au Japon, Mickey Kantor, bénéficie de l'aide de la NSA lors de discussions très serrées avec Tokyo sur les quotas d'importation de voitures.

15 juin 1995 : Un document, aujourd'hui déclassifié, donne des indications sur « l'activation d'unités Echelon » de l'armée de l'air sur plusieurs bases dans le monde.

Juillet 1995 : Les satellites Keyhole auraient vu les massacres de Srebrenica.

3 décembre 1995 : Le *Baltimore Sun* révèle que « à partir d'un satellite de communications commerciales, la NSA s'empara de tous les fax et appels téléphoniques entre le consortium européen Airbus, la compagnie aérienne nationale de l'Arabie Saoudite et le gouvernement saoudien. L'agence découvrit que les agents d'Airbus offraient des pots-de-vin à un officiel saoudien. Elle transmit l'information aux officiels Américains qui appuyaient l'enchère de Boeing Co. et McDonnell Douglas Corp., lesquels triomphèrent l'année dernière (1994) dans la compétition à six milliards de dollars ».

1996 : Une chaîne néo-zélandaise est parvenue à obtenir des images de l'intérieur du centre des opérations de la station de Waihopai. Les images furent obtenues clandestinement en filmant de nuit à travers des fenêtres partiellement obstruées par des rideaux. Le reporter parvint tout de même à faire des gros plans des manuels des techniciens du centre de contrôle. Il s'agissait de manuels techniques d'Intel-

sat, prouvant que la station espionnait des satellites civils. Le film montrait également que la station était pratiquement vide, gérée presque exclusivement par des ordinateurs.

1996 : Le néo-zélandais Nicky Hager met en évidence l'existence et le fonctionnement du plus grand réseau d'espionnage des communications jamais conçu. Il dévoile ce réseau baptisé « Echelon » dans un livre intitulé « *Secret power* ».

1996 : Signature d'un accord entre Lotus et le gouvernement américain pour l'exportation des systèmes de cryptage de 65 bits : en échange de la licence d'exportation, Lotus garantit aux autorités américaines l'accès à 24 de ces bits appelés « *champs de réduction de charge de travail* ».

Juin 1997 : Un exercice secret, appelé Eligible Receiver, voit 50 à 75 agents de la NSA attaquer et pénétrer les ordinateurs du DoD à partir de programmes téléchargés sur Internet (63% des attaques n'ont pas été détectées). Le commandement de la Zone Pacifique aurait pu être rendu inopérant.

Septembre 1997 : Lors du jugement de deux activistes britanniques arrêtées et jugées pour avoir essayé de pénétrer dans la base de Menwith Hill, R. Morris, chef de la planification d'urgence chez British Telecom, rend publics des documents prouvant le branchement de la station sur trois tronçons de fibre optique qui permettent chacun de véhiculer plus de 100 000 communications domestiques.

1997 : La NSA reçoit le « National Intelligence Meritorious Unit Citation » décerné par le DCI pour services rendus pendant la Guerre froide et durant 50 ans.

Novembre 1997 : les pouvoirs publics suédois ont appris que le système cryptographique du logiciel Lotus Notes d'IBM, utilisé notamment par les parlementaires et l'administration, mais aussi l'industrie, avait été affaibli pour faciliter le décryptage des courriers électroniques par la NSA, qui disposait d'une partie de la clé de cryptage. Lotus s'est défendu mollement de ces accusations, assurant seulement avoir reçu des garanties que le gouvernement américain n'en ferait pas « mauvais usage ».

Décembre 1997 : Le Parlement européen publie, sur l'initiative du député britannique Glynn Ford, le rapport *Évaluation des techniques de contrôle politique*[114] qui dénonce le système d'interception des transmissions hertziennes mis en place par les États-Unis dès 1948 pour recueillir le maximum d'informations sur l'Union soviétique et ses alliés.

1998 : La NSA aurait infiltré des agents au sein de la mission de désarmement de l'ONU en Irak. Leur mission : installer de petits systèmes d'interception pour capter les communications de Saddam Hussein et de l'état-major irakien.

1998 : Le NRO annonce un plan de restructuration des différentes classes SIGINT dans une architecture commune dénommée IOSA pour accroître les performances des satellites et le traitement du signal.

Février 1998 : Le général Michael Hayden est nommé à la tête de la NSA qu'il modernise, notamment par la création des premières cellules opérationnelles chargées d'intervenir dans le cyberespace.

11 mai 1998 : Le *Sunday Times* a relaté que par le passé les radômes de Menwith Hill (station NSA F83) dans le Nord du Yorkshire au Royaume-Uni, avaient eu pour tâche d'intercepter l'ensemble du trafic ILC — essentiellement des communications commerciales ordinaires. Le personnel est passé de 400 personnes dans les années quatre-vingt à plus de 1400 aujourd'hui auxquelles s'ajoutent 370 personnes venues du ministère de la Défense. Le *Sunday Times* fait part également d'allégations selon lesquelles les conversations entre la société allemande Volkswagen et General Motors ont été interceptées et que les Français se sont plaints que Thomson-CSF, l'entreprise électronique française, avait perdu un contrat d'un montant de 1,4 million de dollars destiné à la fourniture d'un système radar au Brésil parce que les Américains avaient intercepté des détails des négociations et les avaient transmis à la compagnie américaine Raytheon qui avait par la suite remporté le contrat. Selon une autre plainte, Airbus industrie aurait

[114] Disponible sur Internet.

perdu un contrat d'une valeur d'un milliard de dollars au profit de Boeing et McDonnel Douglas car des informations avaient été interceptées par l'espionnage américain.

20 août 1998 : Treize jours après un double attentat contre les ambassades américaines au Kenya et en Tanzanie, les États-Unis bombardent des camps d'extrémistes musulmans visant, sans l'atteindre, le milliardaire Oussama ben Laden. Les satellites du NRO guidèrent les missiles grâce aux signaux du téléphone satellitaire de ce dernier.

3 septembre 1998 : La NSA a mis en place il y a deux ans un astucieux programme de mise à la retraite anticipée d'une partie de ses personnels, qui lui permet à la fois d'élargir son influence dans l'industrie privée en y plaçant ses cadres qui souhaitent partir, et de recruter les jeunes talents dont elle a besoin. Intitulé « *Soft Landing* » (atterrissage en douceur), ce programme aurait déjà permis à la NSA d'économiser 25 millions $.

Septembre 1998 : Une étude commandée par le Parlement européen souligne les dangers que fait peser l'activité de ce réseau sur les pays de l'Union européenne et sur leurs entreprises. Steve Wright, membre d'OMEGA, une association britannique pour les droits des citoyens (Manchester) constate, dans un rapport adressé au Parlement européen, que tous les courriers électroniques, les conversations téléphoniques et les fax sont enregistrés par routine par la NSA qui fait suivre toutes ces données à Fort Meade.

24 février 1999 : Le *New York Times* publie un article décrivant en termes généraux le système Echelon comme une coopération entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis visant à écouter l'ensemble des échanges téléphoniques et électroniques du monde.

Février 1999 : La Maison-Blanche lance un programme de recherche afin que l'industrie informatique développe des ordinateurs ayant la possibilité de vitesse de traitement de 30 téraflops[115] en 2001 et de 100 téraflops en 2004. L'objectif est de répondre au défi que pose la cryptographie.

Printemps 1999 : Les Commissions du Renseignement du Congrès — créées dans les années 70 en partie à cause des activités illégales de la NSA sur le sol américain — se sont néanmoins émues d'accusations selon lesquelles des Américains auraient été placés sur écoute.

11 mars 1999 : Martin Brandy, Directeur du DSD Australien (Defense Signals Directorate), brise le silence et révèle que son service « *coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre-mer sous l'égide de l'alliance UKUSA* ». Cette déclaration fut diffusée le 11 avril 1999 dans le « *Programme du Dimanche* » sur Channel 9 TV.

Eté 1999 : Un expert en sécurité informatique, Andrew Fernandes, annonce qu'il a découvert deux « clés secrètes » dans un logiciel de Microsoft, dont l'une était dénommée... « NSA Key ». Microsoft assure que cette appellation signifie simplement que cette clé est conforme aux standards imposés par la NSA, mais se défend de « partager les informations » que donne cette clé avec des tiers, même avec la NSA.

20 novembre 1999 : Le professeur Christopher Simpson, de l'American University de New York a révélé quelques-uns des mots clés grâce auxquels le système Echelon effectue ses écoutes : AK-47, Cocaïne, Stinger (du nom du missile anti-aérien portable), TWA 800 (l'identification du vol du Boeing qui a explosé au-dessus de l'Atlantique), Militia, Davidian (le surnom de la secte Waco en 1993) ou « Vince Foster » (un ami de Bill Clinton travaillant à la Maison Blanche qui s'est donné la mort en 1993).

6 décembre 1999 : Le *New Yorker* révèle que l'*USS Jimmy Carter* (SSN-23), de type Seawolf, va être réaménagé en vue de missions de services secrets de type subaquatiques (écoutes de câbles) à partir de 2004.

[115] (tera FLoating point OPerations per Second) un trillion d'opérations en virgule flottante par seconde. On s'attend à ce que l'ordinateur géant du BlueGene/L d'IBM, conçu pour la science informatique au laboratoire national de Lawrence Livermore, réalise 360 teraflops une fois entièrement mis en application avec 65.536 processeurs. On dit que le cerveau humain traite 100 teraflops ; cependant cela semble être une exagération.

1er janvier 2000 : Le passage à l'an 2000 a provoqué une panne des systèmes terrestres de traitement de l'information des satellites-espions.

5-12 janvier 2000 : L'ordinateur central du système Echelon était hors service pendant toute la semaine : le coût de la remise en marche du système s'élèverait à la modique somme de 1,5 million de dollars.

24 janvier 2000 : La NSA admet que l'ensemble de son réseau informatique de traitement et d'analyse a connu une panne totale pendant trois jours : le système a littéralement été noyé sous l'information.

Février 2000 : Des documents « top-secret » déclassifiés de la NSA confirment l'existence du programme Echelon.

22-23 février 2000 : Examen par le Parlement européen du rapport sur le fonctionnement d'un réseau Echelon.

23 février 2000 : Exposé de Duncan Campbell devant les eurodéputés des activités de la NSA et du système Echelon.

Mars 2000 : La DGSE est mise en cause par la presse spécialisée pour collaborer avec la NSA qui lui aurait transmis une partie de son savoir-faire dans les années 70.

28 mars 2000 : Le Figaro relate les confidences d'un expert des services de renseignement américains : « Pour l'adversaire, il est chaque jour plus aisé de cacher son jeu dans le brouhaha. Et pour nous, il devient chaque jour plus difficile de déchiffrer les partitions qui nous intéressent. C'est un vrai problème pour la NSA ».

10 mars 2000 : Selon le journal *Le Monde*, Georges Tenet, directeur de la CIA, aurait déclaré devant le Congrès américain que les États-Unis n'utilisaient pas leurs services de renseignement pour promouvoir leurs activités économiques.

Mars 2000 : La presse allemande affirme que la station de Bad Aibling se consacre à l'espionnage d'entreprises allemandes et suisses.

24 mai 2000 : Le parquet de Paris a ouvert une enquête préliminaire sur le réseau Echelon, soupçonné d'avoir servi à l'espionnage industriel.

Juin 2000 : La diffusion de comptes rendus d'interceptions de la NSA classés « secrets » et relatifs aux conversations de Hilary Clinton et de Jimmy Carter suscite un vif émoi chez les membres de la commission pour les affaires de renseignements de la Chambre des Représentants.

Juin 2000 : L'Irlande s'intègre au Pacte UKUSA.

13 octobre 2000 : Ilka Schröder, députée allemande des Grünen au Parlement européen, a décidé de déposer une plainte contre X auprès du plus haut magistrat de la république fédérale, pour « *exploitation et tolérance du système d'espionnage* Echelon » dans son pays. « *Cette plainte vise tout particulièrement les États-Unis et la Grande-Bretagne, ainsi que le gouvernement allemand* ». Elle a également porté plainte auprès du procureur de Berlin, son lieu de résidence.

16 octobre 2000 : le général Michael Hayden, lors d'un congrès sur la guerre de l'information qui s'est tenu à Baltimore a réitéré sa volonté que la NSA représente la figure de proue du Pentagone pour toute la défense du Cyberespace.

21 janvier 2001 : Le ministre néerlandais de la Défense nationale présente une note circonstanciée intitulée « *L'écoute à grande échelle des systèmes de télécommunication* » dans laquelle il estime l'existence du réseau Echelon plausible.

22 janvier 2001 : Dans l'exposé qu'il fait devant la Commission temporaire sur Echelon, Duncan Campbell estime que les USA font appel à leurs services de renseignement pour aider les entreprises américaines à obtenir des marchés. Les informations seraient transmises via la CIA, avec l'aide de l'*Advocacy Center* et de l'*Office of Executive Support* au *Department of Commerce*.

23 janvier 2001 : Le *Jane's Defence Weekly* révèle l'existence d'une base Échelon à Taiwan qui se trouverait dans les montagnes de Yangmingshan, au Nord de Taipeh.

25 janvier 2001 : Un cadre de la NSA a affirmé au *Monde du Renseignement* que l'Agence disposait d'un des premiers ordinateurs quantiques fonctionnant dans un cadre opérationnel. Cela lui donne une confortable avance dans la durée de déchiffrement de la plupart des algorithmes utilisés. Il y aurait ainsi cinq ordinateurs quantiques de 40 bits dont les performances surpassent largement les supercalculateurs de type ASCI Red Tops et Cray T3E.

Début 2001 : La Suède découvre que les logiciels *Lotus* utilisés par les services gouvernementaux et par de nombreuses entreprises disposent de clés activant des *back doors*[116] *contrôlées par la NSA.*

Février 2001 : Un second câble de liaison Internet casse entre la Chine et les USA. Les internautes chinois risquent de ne plus pouvoir surfer pendant plusieurs jours en raison de « travaux » sur un câble sous-marin défectueux, un câble qui donne accès aux serveurs basés aux États-Unis. C'est la seconde fois qu'un câble sous-marin est « défectueux » dans cette région. Il y a quelques mois déjà un autre câble, donnant une liaison entre l'Europe et l'Australie avait souffert du côté de Taiwan. Un sous-marin poserait-il une dérivation ?

Février 2001 : « NSA Career Fair 2001 » : séance de recrutement organisée par la NSA, à l'intérieur du R&E Building de Fort Meade. 600 postes sont à pourvoir dans sept domaines : la recherche fondamentale en informatique, l'ingénierie informatique, la cryptanalyse (et notamment la cryptographie quantique), les mathématiques, l'analyse des signaux radio électriques, les langues étrangères et l'analyse du renseignement.

5 février 2001 : Le fabricant de logiciels *Vmware* vient de s'associer à la NSA pour créer un ordinateur inviolable : le projet, baptisé *Net Top*, vise à transformer chaque ordinateur en autant de PC virtuels tournant sur un ordinateur sous Linux. Ces murs virtuels, mais quasi inviolables permettraient de retrouver la configuration actuelle d'ordinateurs séparés physiquement sur différents réseaux correspondant à des classifications différentes.

Mars 2001 : Les États-Unis devraient déployer, à partir de 2005, un réseau de satellites-espions aux performances encore inégalées dans le monde. A ce titre, le groupe américain de défense Boeing vient de recevoir un contrat portant, à terme, sur un total de 25 milliards de dollars. À l'heure actuelle, le NRO exploite, en permanence, six satellites-espions : trois de la classe KeyHole pour l'observation optique et infrarouge par beau temps ou temps couvert, et trois autres de la classe Lacrosse pour la reconnaissance radar, par mauvais temps et de nuit. Ces satellites pèsent quinze tonnes en moyenne. Tel qu'il a été révélé par des indiscrétions de sources ayant requis l'anonymat, le projet consiste à passer, dès 2005, à l'exploitation de vingt-quatre satellites-espions en orbite haute, pesant le tiers des satellites actuellement en service et capables de collecter, selon les cas, entre huit et vingt fois plus d'images avec une précision de quinze centimètres. Le NRO a donc fait le choix d'une constellation de satellites-espions moins lourds que les précédents et maintenus ou renouvelés en orbite, de façon à disposer d'une couverture relativement permanente de la Terre.

Mars 2001 : La *Lettre de l'Expansion* révèle que la NSA s'est lancée dans ce qui semble bien être le plus important plan de mise à niveau de l'histoire dans le domaine des technologies de l'information. Le projet intitulé « *Groundbreaker* », évalué à 5 milliards de dollars, s'étalera sur dix ans. Trois équipes s'affrontent pour remporter le contrat. La première, conduite par Computer Science Corporation, comprend General Dynamics et Verizon Communications. La deuxième est menée par AT&T. Enfin, la troisième est composée notamment de Raytheon et WorfdComm. Verdict en juillet. Dès le 07/06/200, le *Washington Post* annonçait qu'afin de maintenir son avance technologique la NSA envisageait de privatiser une partie non classifiée (1200 à 1500 employés seraient transférés vers le secteur privé) de ses activités technologiques (économie d'1 milliard de $ sur les dix prochaines années).

[116] Back door, porte dérobée : routine logicielle ouvrant un port de communication à l'insu de l'utilisateur et permettant l'intrusion dans un système informatique. Ce point est développé dans la section traitant de la sécurité informatique.

Mars 2001 : *Der Spiegel* a publié un article qui explique pourquoi le ministère des Affaires étrangères et le ministère de la Défense allemand se sont débarrassés du système d'exploitation Windows. En effet, selon le journal, le système de Microsoft laisserait un « backdoor » qui permettrait à la National Security Agency (NSA) américaine de pénétrer et d'espionner les ordinateurs sur lesquels le système est installé. De plus, le chef de la diplomatie allemande a également décidé de suspendre tous les projets de vidéoconférence, après que les autorités ont découvert que les données transitaient par Denver, Colorado. L'administration allemande a donc fait appel à deux firmes locales, Deutsche Telekom et Siemens, pour trouver, dans les plus brefs délais, des solutions de remplacement.

8 mars 2001 : Des consultants intervenant dans des sociétés d'intelligence privée apportent des informations à la « *Commission temporaire sur le système* Echelon » du Parlement européen. Cette expertise sert principalement à démontrer l'agressivité du système en matière d'espionnage économique.

Mars 2001 : *Libération* révèle que la Commission européenne aurait permis à la NSA d'accéder à ses systèmes de cryptage des informations confidentielles. Ce serait le chef du bureau chargé du cryptage lui-même, le britannique Desmond Perkins qui aurait reconnu : « *J'ai toujours eu de très bons contacts avec la NSA à Washington* : *elle vérifie régulièrement nos systèmes (de cryptage) pour voir s'ils sont bien verrouillés et s'ils sont correctement utilisés* ». Ainsi, la NSA n'a même plus besoin de recourir à Échelon... puisqu'elle dispose de ses entrées à la Commission ! Le lendemain, démenti officiel : « *L'entreprise Siemens, qui a fabriqué notre système de cryptage, nous a expliqué qu'il avait été testé par la NSA. C'était un argument de vente. Cela s'est passé il y a dix ans...* ».

Avril 2001 : Une station d'Échelon vient d'être démilitarisée. Le site *Physics Todays* présente la nouvelle acquisition de « *Pisgah Astronomical Research Institute* » : une ancienne station de la NASA construite dans les années 60 puis transformée dans les années 80 pour permettre l'interception des signaux des satellites géostationnaires de l'hémisphère Nord. Rosman Station est située au Sud-ouest d'Asheville, dans la forêt de la Caroline du Nord (à l'Ouest de l'État). La station eut pour vocation d'espionner les relations entre Cuba et le Pacte de Varsovie et d'intercepter les messages échangés entre Moscou et les sites des missiles SS-20 en Allemagne de l'Est. Puis, ce fut l'Amérique Latine et le trafic de drogue.

11 Avril 2001 : La NSA vient de signer un accord de 1,2 million US$ avec NAI Labs pour développer le système sécurisé SeLinux. Le 2 janvier dernier, l'agence gouvernementale américaine NSA annonçait avoir mis au point un noyau pour Linux plus exigeant en matière de sécurité. Chose encore plus étrange, elle comptait – dans l'esprit de l'Open Source – mettre le code de Security-Enhanced Linux (SeLinux) à disposition du public. Cette véritable rupture avec la tradition de la NSA vient d'être renforcée cette semaine avec la signature d'un accord avec NAI Labs. Portant sur 1,2 million de dollars sur deux ans, il stipule que NAI Labs, compagnie privée de sécurité, continuera le développement du prototype SeLinux. NAI Labs est en fait une filiale de PGP Security, véritable Némésis privée de la NSA depuis plus de dix ans. Cet accord s'inscrit dans la continuité d'un précédent contrat passé entre les deux agences en juin dernier.

13 avril 2001 : Un sondage montrait récemment que la moitié des Américains étaient d'accord pour que le FBI ou d'autres agences gouvernementales espionnent leur courrier. L'ACLU a donc décidé d'utiliser les grands moyens pour que les citoyens américains comprennent à quel point leur vie privée est violée, en toute illégalité et en toute impunité, par ces systèmes qui peuvent intercepter à tout moment des courriers électroniques. Pour l'un des directeurs de l'association américaine, Barry Steinhardt, le but premier d'Echelon est « *la surveillance mondiale, pas seulement des autres services de renseignement, mais aussi des civils* ». L'ACLU met l'accent sur le fait que *Carnivore*, mis en place par le FBI, viole le quatrième amendement de la Constitution américaine. L'Union propose sur son site des astuces pour écrire ou rencontrer son élu local et pour envoyer directement des fax aux députés et sénateurs. Dans la presse, la campagne (qui paraîtra dans le *New York Times* et le *New Yorker*) présentera un téléphone portable

avec ce titre : « *Désormais équipé d'un système à trois interlocuteurs* : *vous, la personne que vous appelez, et le gouvernement* ».

24 avril 2001 : Dans son audition devant la Commission temporaire sur Echelon, Nicky Hager souligne que le système n'est pas tout puissant : « *Tout ne peut être intercepté en raison de ressources par définition limitées ; il faut se contenter de ce que promettent des informations importantes* ».

26 avril 2001 : Le quotidien *La Meuse* reproduit les inquiétudes du Comité R, chargé de contrôler les services de renseignement et de sécurité belges, qui vient de remettre un rapport au Parlement. Selon lui, l'absence de moyens et d'instructions interdit à la Sécurité de l'État de mener à bien sa mission de protection du patrimoine scientifique et économique belge. Le Comité R évoque également la mésaventure survenue à un centre universitaire de recherche victime d'une tentative d'intrusion dans son système informatique, doublée d'un cambriolage au cours duquel du matériel a été manipulé ou volé. Ces événements font suite à un important contrat portant sur la livraison de matériel de pointe (les autorités américaines avaient refusé qu'une firme US livre ce type de matériel pour motifs de non-prolifération). Les soupçons se portent sur les Allemands ou les Américains.

11 mai 2001 : après les difficultés d'Alain Krivine, député européen et membre de la commission Échelon, pour obtenir un Visa d'entrée aux États-Unis, la délégation européenne a quitté Washington jeudi 10 mai : la plupart des rencontres prévues avec les autorités américaines n'ont pas été honorées (entre autres celles avec la CIA, le Département d'État et la NSA). Cette politique de la porte close semble cohérente (!) si on considère le peu de pouvoir dont dispose en la matière un organisme comme le Parlement européen, pour ne pas parler de l'actuel comité (temporaire) sur le système d'interception Échelon. Les députés ont tout de même pu rencontrer des membres de la Chambre des représentants, un ancien patron des renseignements américains, et des responsables du département américain de la justice. À cela s'ajoutent des ONG de défense de la vie privée comme l'ACLU ou l'Epic.

11 mai 2001 : Lors de sa rencontre avec la délégation de la Commission temporaire sur Echelon à Washington DC, Jeff Richelson, auteur américain et ancien membre de la NSA, a déclaré qu'Echelon désignait un réseau d'ordinateurs au moyen duquel seraient filtrées des données échangées entre les services de renseignement.

18 mai 2001 : Un virus nommé Échelon aurait pour but de saturer les grandes oreilles américaines. Ce ver arrive par email sous le nom de « Echelon.*vbs* ». Ce virus contient un texte caché conçu pour attirer les robots fouineurs du réseau d'espionnage Échelon.

31 mai 2001 : Le quotidien britannique *The Register* publie une liste réactualisée des mots qui déclenchent Echelon.

2 juin 2001 : Une fuite de la Commission temporaire sur le système d'interception Échelon nous permet de vous présenter son projet de rapport, rédigé le 18 mai 2001[117].

6 juin 2001 : Le quotidien bavarois *Münchner Merkur* a eu accès à un dossier secret du Pentagone dans lequel est programmée la fermeture de la station de Bad Abling pour septembre 2002. Cette fermeture intervient dans le cadre d'une réduction des forces américaines en Europe où les bases terrestres seront remplacées par des satellites d'interception.

10 juin 2001 : Selon *La Tribune*, la NSA voit d'un mauvais œil l'évolution de la technologie. Depuis 1989 le Pentagone aurait réuni des chercheurs pour tenter de percer les connexions réalisées via la fibre optique. Finalement, la NSA aurait conçu une chambre sous-marine destinée à mettre sur écoute des câbles transatlantiques. Y aurait-il cause à effet des câbles sous-marins qui ont mystérieusement cassé en Australie et en Asie du Sud-est ?

16 juin 2001 : Les États-Unis vont fournir une aide « *sur le plan technologique, de l'information et de la détection des communications* » au gouvernement espagnol. Cela se traduira par un recours au réseau de

[117] *Projet de Rapport Européen sur Echelon.*

satellites-espions américains Echelon, capables, disent-ils, de localiser tout mouvement des membres de l'ETA et d'intercepter leurs communications.

18 juin 2001 : Le serveur public de la NSA est hors service : il n'est plus possible de télécharger le guide sécurité Windows 2000 en raison d'un afflux massif de connexions.

21 juin 2001 : Dans la journée du 31 mai dernier, un agent du Government Communications Headquarter (GCHQ) est décédé dans des conditions inhabituelles. Quittant son service peu avant 13 h pour rentrer chez lui en voiture, Donald Brian Davies (53 ans) a percuté une barrière de sécurité sur la route. Les premiers examens pratiqués à l'hôpital de Cheltenham ont indiqué qu'il avait perdu la maîtrise de son auto après un malaise. Puis, dans les heures qui ont suivi, le fonctionnaire a succombé sans que les véritables causes de son décès ne soient identifiées par les médecins. La police a ouvert une enquête. Et la semaine dernière la famille a annulé les funérailles pour cause d'autopsie.

27 juin 2001 : Dans un témoignage exclusif publié le 27 juin 2001 par le quotidien *Mainichi Shimbun*, le journaliste néo-zélandais Nicky Hager affirme que les moyens d'interception de la NSA ont été « ouvertement » utilisés en secret pour des missions d'espionnage industriel contre le Japon, et au bénéfice des États-Unis.

2 juillet 2001 : Echelon a espionné le Pape et a aussi écouté une grande partie de l'activité diplomatique du Vatican, en particulier durant les années 1995 à 1998. Le Saint-Siège s'en est aperçu et a pris des « *mesures telles qu'on peut dire aujourd'hui que le Vatican est le seul État à être entièrement crypté* ». Aucun fax, mail, téléphone, émettant depuis les « pièces qui comptent » dans le palais ne peuvent être interceptés, envoyés et enfin lus et déchiffrés par les services des États-Unis d'Amérique. (*Repubblica*).

3 juillet 2001 : Duncan Campbell, dans un article du *Gardian*, revient sur le « *Rapport* Echelon » en discussion au Parlement Européen et met en garde les Européens contre la volonté des Américains de saper les projets (allemands) d'une Europe du renseignement. En effet, les USA créent progressivement des alliances bilatérales avec l'Espagne (lutte contre l'État), la Norvège, le Danemark, la Suisse et l'Italie (lutte contre le terrorisme).

3 juillet 2001 : Une cinquantaine de militants de Greenpeace occuperait depuis cinq heures du matin trois points stratégiques de la base de Menwith Hill afin de protester contre le projet de bouclier antimissile. Un autre groupe manifeste devant l'entrée de la base au son la musique du film « *Misson Impossible* ».

3 juillet 2001 : Alors qu'un soldat américain du 353rd Special Operations Group de Kadena Air Base est accusé du viol d'une Japonaise de vingt ans, la presse nippone dénonce l'espionnage économico-politique que mènerait la Nouvelle-Zélande à l'encontre du Japon dans le cadre du pacte UKUSA.

4 juillet 2001 : La station chypriote d'Ayios Nikolaos (appartenant aux Britanniques) est victime depuis plusieurs jours de manifestations d'une centaine d'écologistes protestant contre l'installation de nouvelles antennes qui, selon eux, mettent en danger la vie des riverains et des oiseaux en raison des radiations électromagnétiques. Un député et un écologiste se sont enchaînés à un des pylônes de la base.

5 juillet 2001 : Au cours d'une session du Parlement européen, mardi 3 juillet, les membres ont entériné 60 amendements avant de valider la résolution informant qu'Echelon n'était pas un outil d'espionnage industriel menaçant. Quelques membres du comité ont protesté, indiquant notamment que cette réunion n'avait que bien peu fait pression sur les États-Unis pour brider ses capacités d'espionnage. Le rapport sera soumis au vote de l'ensemble des députés européens, lors de la prochaine session parlementaire à Strasbourg, au mois de septembre.

7 juillet 2001 : Le *Wall Street Journal* rapporte que la NSA a réussi l'exploit d'aller percer et capter des câbles à fibres optiques, qui transportent des millions de liaisons entre matériels informatiques et téléphones, au fond de l'océan, grâce à un sous-marin spécial. Mais, selon son directeur général, Michael Hayden, la difficulté est d'analyser des masses d'informations. « *Avec les nouvelles technologies, il y a trop de choses, trop compliquées à interpréter* », a-t-il confié au WSJ.

10 juillet 2001 : Dans son supplément économique, *Le Monde* publie une série d'articles relatifs à l'espionnage industriel mené par les États-Unis — *les grandes oreilles de l'Oncle Sam* — au nom de la lutte contre la cybercriminalité.

16 juillet 2001 : Après une action coup de poing de Greenpeace dans la base Échelon de l'US Air Force de Vandenburg en Californie, 15 militants et deux journalistes ont été poursuivis pour « violation de zone sécurisée » (ils risquent 6 ans de prison et 255 000 $ d'amendes). Ils auraient empêché un test de missile dans le cadre du programme « Star Wars ».

29 juillet au 10 août 2001 : Les plus hauts responsables du renseignement américain se sont réunis dans les locaux de l'Aspen Institute, sur le site du Wye River Plantation Conference Center, dans le Maryland. Le partage des informations entre services secrets et agences de police judiciaire s'est imposé comme un thème saillant. En outre, plusieurs intervenants ont souligné la nécessité d'élaborer de nouveaux produits, confondant sources ouvertes et données classifiées, qui assureraient une information en temps réel des décideurs politiques.

31 juillet 2001 : Le contrat relatif au projet Groundbreaker — plus de 2 milliards de dollars sur 10 ans — a été attribué à un consortium industriel dirigé par Computer Sciences Corporation (CSC), choisi pour son expérience en matière de reclassement des employés gouvernementaux.

09 août 2001 : Dans un article du magazine *New Scientist*, un astronome (Jonathan McDowell) dénonce comment l'enregistrement des satellites-espions américains sur les registres de l'ONU ne correspond pas aux orbites réellement empruntées par ces satellites.

21 août 2001 : L'agence américaine (CERT, Computer Emergency Response Team) et son homologue australienne (AusCERT) « vont s'allier pour accélérer le développement de méthodes, d'instruments, et de techniques en vue d'assurer la protection des réseaux interconnectés servant de support aux infrastructures d'information nationales et mondiales », ont-elles annoncé dans une déclaration commune. Cet accord intervient alors que les deux agences ont coopéré de manière informelle depuis longtemps, notamment lors du passage à l'an 2000, pour prévenir le bogue informatique.

23 août 2001 : Un article du *Washington Post* reprend les événements du 24 janvier 2000, date à laquelle le système d'écoute Echelon a été frappé de surdité. On y apprend que c'est l'ensemble des stations qui a été affectées, que la NSA est confrontée à un difficile problème de sureffectif, qu'Echelon semble dépassé par l'augmentation du flux d'informations numériques parcourant la planète et que l'interception systématique doit faire place à une recherche ciblée. Reste que la NSA peut saisir au vol un peu plus de 6 To à l'heure soit près d'un cinquième de la capacité moyenne des communications téléphoniques mondiales.

28 août 2001 : Un sergent major de l'Air Force qui était détaché au NRO par TRW (société spécialisée dans l'électronique de défense), Brian P. Regan (ancien membre également de la Defense Intelligence Agency), a été arrêté par le FBI alors qu'il tentait de quitter les États-Unis pour Zurich : il est convaincu d'espionnage au bénéfice d'une puissance étrangère, en l'occurrence la Libye ou l'Irak. Il était spécialisé dans la cryptanalyse, l'analyse d'images satellites et la gestion du réseau Intelink. Durant la Guerre du Golf, il avait été assigné à l'Irak Regional Intelligence Task Gorce du Joint Intelligence Center.

5 septembre 2001 : 367 votes pour, 159 votes contre, 34 abstentions, le Parlement Européen réuni à Strasbourg vient d'entériner sa reconnaissance du réseau d'écoute UKUSA connu sous le nom d'Echelon. Un vote qui n'aura strictement aucun effet tangible, mais qui admet officiellement les possibles interférences entre le monde des affaires et celui des services de renseignements.

6 septembre 2001 : *TTU* confirme que la NSA améliore sa présence en Europe (en Espagne et en Irlande) ce qui lui permettrait de développer une infrastructure SIGINT. De plus le FBI aurait également détaché une équipe à Dublin pour aider les autorités irlandaises à intercepter les communications GSM et utiliser le système Carnivore dans la capture des messages Internet circulant sur les téléphones portables.

12 septembre 2001 : Au lendemain des attentats, les analystes parlent d'un Pearl Harbor des services de renseignement US : manque de moyens ou inadéquations de ces derniers ? En tout état de cause, « *Si les services de renseignements étaient parvenus à se rassembler, nous aurions pu déjouer les attaques* » a estimé le sénateur Richard Shelby, vice-président de la commission des services de renseignements du Sénat. Un constat renouvelé par John Martin, ancien représentant du Département américain de la Justice. « *C'est un échec de la sécurité et de l'ensemble des services de renseignements américains* ».

13 septembre 2001 : Selon le *Frankfurter Allgemeine Zeitung*, la NSA, depuis déjà trois mois, collectait des informations sur des actions terroristes en préparation qui concernaient le détournement d'avions de ligne devant servir d'armes contre des cibles symboliques de la culture des États-Unis et d'Israël. L'accord ne se serait pas fait à temps sur les modalités à mettre en place pour combattre cette menace.

14 septembre 2001 : Alors que l'on se demande aux États-Unis si l'on ne va pas en revenir aux méthodes humaines de surveillance, des activistes prévoient pour le 21 octobre prochain une journée de lutte contre le système de surveillance mis en place par la NSA.

18 septembre 2001 : BAE a installé un laboratoire de R&D en guerre de l'information à Arlington, en Virginie, qui travaille avec la DARPA, la NSA et le Naval Research Laboratory. Un autre bureau spécialisé dans la gestion des programmes avait déjà ouvert en mai.

18 septembre 2001 : Selon la BBC, les satellites-espions américains se concentrent tous et de façon exclusive, sur les pays hôtes de Bin Laden. De plus des satellites commerciaux (Orbimage-4, doté d'une caméra destinée à analyser la composition des sols qui va être lancé le 21 septembre ; Quickbird, qui devrait être lancé le 18 octobre) vont également être affectés à cette tâche afin de pallier à l'absence des satellites militaires quand ces derniers ne seront pas au-dessus de l'Afghanistan. Rappelons enfin qu'en 1998, lors des frappes américaines contre des sites terroristes en Afghanistan, les écoutes de Menwith Hill avaient permis de localiser Bin Laden dans son camp de Zhawar Kili au sud est de la ville de Khost. Cette interception avait permis de discriminer le téléphone satellitaire du banquier saoudien. Probablement prévenu par des informateurs au sein des services pakistanais l'ISI, Bin Laden avait précipitamment quitté son camp, échappant de peu aux Tomahawks américains.

21 septembre 2001 : Les deux satellites OrbView 4 (appartenant à la société d'imagerie Orbimage) et Quick Toms (propriété de la NASA) sont tombés dans l'Océan Indien : une minute après le lancement, le deuxième étage de la fusée Taurus a pris feu. OrbView 4 était doté d'un instrument d'imagerie hyper spectral, baptisé « Warfighter », qui aurait notamment servi à localiser les terroristes cachés — dans le sous-sol ou dans des grottes — en Afghanistan.

27 septembre 2001 : Selon le *Réseau Voltaire*, le 11/09, le Secret Service, reçoit un appel des auteurs des frappes de New York et Washington. Pour créditer sa menace, la voix donne les codes secrets permettant d'authentifier les ordres présidentiels donnés depuis la Maison-Blanche ou Air Force One. Immédiatement, pour protéger Georges W. Bush, l'avion présidentiel à bord duquel il rentre à Washington est dérouté vers une destination inconnue, tandis que la Maison-Blanche et le Capitole sont évacués et les personnels politiques conduits dans abris antiatomiques. Aucun membre du Conseil national de sécurité ne pense plus à des « attaques terroristes », tous pensent qu'un coup d'État militaire est en cours. Le calme ne reviendra qu'à 20 h 30.

2 octobre 2001 : *Metamute*, site qui traite de la culture numérique, lance un concours littéraire autour d'Echelon, dans le cadre de la troisième édition de la « Jam Echelon day ». Il offre un total de 1 000 euros aux meilleures œuvres de fiction sur le thème. Echelon serait en effet capable d'ignorer une simple liste de mots clés, mais pourrait, par contre, s'intéresser à un récit complet. Attention : le mot « Echelon » ne doit jamais apparaître dans l'œuvre.(*Vnu Net*)

3 octobre 2001 : La NSA a commencé à moderniser les équipements cryptographiques du gouvernement. Cette mutation devrait s'échelonner sur une quinzaine d'années. Selon l'agence, il faudra changer 400 000 téléphones, radios, cartes à puce et autres appareils de télécommunication utilisés dans tous les

ministères. La principale raison invoquée est que de nombreux hackers ont réussi à décoder les algorithmes de cryptage qui permettent l'accès aux infrastructures vitales de l'agence. D'après les spécialistes cités par *USA Today*, la NSA a grossi artificiellement ses lacunes sécuritaires et chercherait tout simplement à obtenir une augmentation de ses budgets pour le quinquennat 2003-2008.

5 octobre 2001 : Selon *BBC News*, la fusée Titan IV qui a décollé la semaine dernière d'une base de l'US Airforce a mis en orbite un satellite-espion KH-12 pour Key Hole, (trou de serrure), (ou Krystal) capable de suivre des déplacements de véhicules, d'armes ou de petits groupes de personnes se déplaçant à pied. Cette opération est organisée par le NRO.

13 octobre 2001 : Près de 300 personnes ont manifesté devant la base de Menwith Hill, essentiellement pour protester contre le projet américain de Guerre des Étoiles et des interceptions qui n'ont pu empêcher l'attentat du WTC.

16 octobre 2001 : L'Agence Spatiale japonaise (NASDA) et la société australienne Xantic, filiale de Telstra, ont signé un accord pour la construction de deux stations de contrôle de satellite dans le Telstra International Telecommunications Centre de Perth. La première station assurera les communications avec deux satellites japonais à buts scientifiques et commerciaux. La seconde contribuera à la sécurité de quatre satellites de renseignement dans leur phase de lancement et de mise en orbite, puis elle sera démantelée.

17 octobre 2001 : Selon D. Campbell, dans *The Gardian*, le gouvernement américain achète toutes les images de l'Afghanistan produites par Space Imaging, la plus performante société civile d'imagerie satellitaire américaine. Pour 1 912 500 dollars, la National Imagery and Mapping Agency (NIMA) s'est réservé l'exclusivité des droits sur toutes ces images. Actuellement des photos satellitaires de l'Afghanistan sont disponibles sur le marché commercial. Elles sont produites par deux satellites, Eros d'ImageSat et Spot. Le gouvernement israélien est cependant prêt à interdire à ImageSat de vendre ses images dès que les États-Unis le demanderaient.

18 octobre 2001 : Selon *Intelligence Online*, le déménagement de la base allemande Bad Aibling est reporté, à l'issue de discussions entre les ministères de la Défense allemand et américain, en raison des attentats du 11 septembre.

18 octobre 2001 : La NSA sort la 3e partie de sa version de Linux : le prototype SELINUX LSM vient d'être mis en ligne, doté de plusieurs corrections d'erreurs et des améliorations de sécurité.

Fin octobre 2001 : Selon *Intelligence Online* les multiples échanges entre la NSA et un fournisseur tel que World Com UUnet rendraient crédible une intervention des services de sécurité US dans les serveurs de l'opérateur, en cas de crise grave. (cf. les cônes de silence).

1er novembre 2001 : Selon TTU, l'Indian Space Research Organisation (ISRO) a procédé au lancement du Technology Experiment Satellite officiellement destiné à tester les technologies nécessaires aux futurs satellites-espions ainsi qu'aux IRS-2. Sa caméra panchromatique serait capable d'une résolution inférieure à 2,5 mètres — certaines sources n'hésitant pas à placer la barre à un mètre. Le programme aurait du reste été lancé en juillet 1999, peu après les événements de Kargil et le premier test du missile de portée intermédiaire pakistanais Ghauri-2, en avril 1999.

4 novembre 2001 : Le *New York Times* révèle qu'une station secrète de la CIA se trouvant sous le WTC a été détruite par les attentats du 11 septembre, provoquant d'importantes difficultés dans la gestion du Renseignement US.

9 novembre 2001 : La CIA pourrait bien devenir le nouveau VC à la mode dans la Silicon Valley : l'agence de renseignements américaine, sur la sellette depuis les attentats terroristes du 11 septembre, n'hésite pas à financer les start-ups susceptibles de l'aider dans la lutte antiterroriste via son fonds In-Q-Tel.

10 novembre 2001 : Une commission créée à la demande du Président Bush à la suite 11 septembre propose de restructurer la Communauté du Renseignement Militaire Américain et d'en confier la tête

à la CIA qui dirigerait la NSA, le NRO et la National Imagery and Mapping Agency (chargée d'interpréter les photos satellites et de créer les cartes militaires). Ainsi tout le Renseignement US, militaire et civil, électronique et humain, serait rassemblé en une seule institution ! Les conclusions définitives seront rendues le mois prochain.

14 novembre 2001 : la NSA vient de fermer le Musée National de la Cryptographie « pour une période non déterminée ».

22 novembre 2001 : Selon TTU, la mise en place du projet Groundbreaker au sein de la NSA est en passe de provoquer des mouvements sociaux. Une menace de licenciement de 400 techniciens a déjà provoqué des débrayages. À cela s'ajoute le flou qui entoure l'avenir de la NSA : elle pourrait être dissoute et passer sous le contrôle de la CIA.

24 novembre 2001 : Le Sénat américain a voté le Patriot Act qui vise à renforcer les moyens d'écoutes, de surveillance et de contrôle des communications du territoire national par l'emploi du système Carnivore (rebaptisé DCS 1000), complément amélioré du système Echelon. C'est un pas de plus dans la tentative de maîtrise totale de l'information.

29 novembre 2001 : La firme Booz Allen & Hamilton a développé à la demande du FBI un nouveau virus de type *keylogger*, Magic Lantern, qui, agrégé au système Carnivore, réalise des intrusions et des écoutes électroniques. Il enregistre les frappes d'un clavier avant que, par exemple, les informations ne soient cryptées ou supprimées. Il comporte enfin une base de données réservée à l'enregistrement de mots clés à rechercher dans la machine cible. (*Intelligence Online*).

3 décembre 2001 : Microsoft apprécie peu la perspective de voir Windows NT, qui équipe les ordinateurs des parlementaires allemands au Bundestag, remplacé par un système d'exploitation à base de noyau Linux. C'est pourquoi l'éditeur a décidé de permettre à la présidence du Parlement, ainsi qu'à la Commission pour les technologies de l'information et de la communication, d'avoir accès au code source de Windows.

6 décembre 2001 : Le ministère américain du commerce (US Department of Commerce) vient d'approuver un standard de cryptage des données, l'Advanced Encryption Standard (AES), qui a pour vocation de protéger les données d'ordre personnel et financier utilisées par le gouvernement, ou dans le cadre d'échanges commerciaux. Il remplace les deux normes actuellement utilisées, le protocole Triple DES et le Data Encryption Standard (DES), adopté en 1977 par le National Institute of Standards and Technology (NIST), une antenne du ministère du Commerce américain. L'AES supporte des clés de codage à 128, 192 et 256 bits, alors que le DES ne supportait que les clés à 56 bits.

7 décembre 2001 : Lockheed Martin Corp. a annoncé que plus de la moitié de sa division télécommunications serait démantelée et largement liquidée. Lockheed Martin va également tenter de vendre ses parts dans plusieurs sociétés de communications, comme Intelsat (24 %), Inmarsat (14 %), New Skies Satellites N.V. (14%), Americom Asia-Pacific (50 %).

10 décembre 2001 : Quatre fabricants de logiciels antivirus (Symantec, McAfee, Trend Micro, Sophos) ont déclaré qu'ils n'ouvriraient pas la porte au virus/ver de surveillance électronique du FBI. Cette décision serait davantage liée aux activités de certains fabricants dans des marchés émergents (comme la Chine) qu'à des préoccupations d'ordre éthique pour les clients actuels (*Les Chroniques de Cybérie*).

12 décembre 2001 : Un porte-parole du FBI l'a reconnu : le développement de Magic Lantern est en cours. Ce logiciel, dont l'existence a été révélée pour la première fois par la chaîne Internet MSNBC en novembre, appartient à la catégorie des *keyloggers*. Installé sur un micro-ordinateur, le *keylogger* surveille et garde en mémoire les touches frappées au clavier par l'utilisateur. Lorsque quelqu'un crypte ses communications avec un logiciel trop difficile à casser, il est beaucoup plus simple de découvrir son mot de passe ou bien le contenu de ses messages en récupérant les données du keylogger.

13 décembre 2001 : Le FBI et les douanes américaines épaulés par l'Australie, le Royaume-Uni, la Finlande et la Norvège ont démantelé mardi 11 décembre un réseau mondial de pirates informatiques qui fournissait sur la toile des copies illégales de programmes.

14 décembre 2001 : Les services de renseignement américains, dont l'efficacité a été mise en doute par les attentats du 11 septembre, verront leur budget augmenter de 8% l'an prochain. L'augmentation des crédits à la CIA, à la NSA (National Security Agency) et aux autres services de renseignement, a été entérinée à l'unanimité par le Sénat jeudi soir. Le budget actuel est d'environ 30 milliards de dollars. L'augmentation servira notamment à accroître les moyens « humains » de la CIA et à recruter de nouveaux spécialistes de langues ou dialectes, deux domaines dont les carences ont été mises en lumière par les attentats de New York et Washington. (*Reuter*)

17 décembre 2001 : Après le lancement réussi le 10 décembre de « Maroc-Tubsat », le Maroc est, après l'Égypte et l'Arabie Saoudite, le troisième pays du monde arabo-musulman à disposer d'un satellite spatial, rapporte lundi la télévision marocaine *2M*. Entièrement conçu par des chercheurs marocains, « Maroc-Tubsat », dont les tests de fonctionnalité ont été réalisés en partenariat avec l'université de Berlin, a été lancé à bord de la fusée russe Zenit depuis la base de Baïkonour (Kazakhstan). Pesant environ 50 kilos, ce satellite assurera, selon l'agence officielle de presse marocaine *MAP*, « quatre missions : observation de la terre, messagerie, collecte de données et localisation ».

21 décembre 2001 : Les états arabes du Conseil de coopération du Golfe (CCG) envisagent d'acheter leur propre satellite-espion. Ce besoin a été mis en lumière lors de la guerre contre l'Afghanistan : les Émirats Arabes Unis, membres du Conseil, ont été incapables d'obtenir des images satellites de l'Afghanistan malgré leur contrat avec la société américaine Space Imaging Inc (le Pentagone avait obtenu l'exclusivité des photos de l'Afghanistan prises par le satellite Ikonos de Space Imaging).

Quartier général de la NSA à Fort Geore (Maryland)

Glossaire

Advocacy Center : structure de lobbying créée en 1993 par l'Administration Clinton et coiffée par l'International Trade Administration. Cet organisme appuie les efforts des entreprises américaines dans la conquête de marchés en faisant appel aux agences fédérales, dont celles traitant du Renseignement.

AIA : l'Air Intelligence Agency est l'agence de renseignement de l'Air Force. Elle est l'agence du Pentagone à la fois la plus impliquée dans la guerre de l'information — depuis l'intégration des missions de cyberdéfense et de guerre de l'information au sein de I'US Space Command — mais également la plus présente à l'international — son bras armé, le 67 th Information Operations Wing emploie à lui seul 5 200 personnes, réparties sur 57 sites dans le monde. Des personnalités du renseignement US se sont succédé à sa direction, dont Michael Hayden, patron de la NSA.

Antennes : le Réseau utilise 120 antennes : 40 seraient pointées vers des satellites commerciaux, 30 vers les satellites d'écoute (type Mercury, Keyhole, etc.) et 50 vers l'ex-URSS (la réorientation s'est faite progressivement vers les satellites commerciaux).

Analyse sémantique : les logiciels d'analyse sémantique permettent à un ordinateur de comprendre une conversation « codée ». En clair, ces logiciels sont capables de repérer le sujet d'une communication (téléphone, fax, email) sans que celui-ci soit directement évoqué.

Brusa : nom donné à l'accord entre la Grande-Bretagne et les USA instaurant le 17 mai 1943 une collaboration en matière de renseignement électronique.

Canusa : Sigint Agreement entre les USA et le Canada le 7 juin 1948 ou le 15 septembre 1950.

Carnivore : le logiciel Carnivore a été conçu par le FBI pour surveiller les communications Internet des suspects placés sous mandat d'écoute judiciaire, mais le système peut aussi collecter les emails de personnes ne faisant pas l'objet d'enquêtes judiciaires. Lancé en 1997 sous le nom d' « Omnivore » sous Sun Solaris, il fut modifié fin 1998 par le FBI (Network Surveillance Lab) pour tourner sous NT. Vinrent les versions 1.2 (septembre 1999), 1.2 (mai 2000) et 1.3.4. La version 2 fut pleinement opérationnelle... Percé au jour, il fut rebaptisé « DCS100 », DCS pour « Digital Collection System ».

Classification : les documents produits par la NSA reçoivent les codes de « Moray » (secret), « Spoke » (plus secret), « Umbra » (top secret), « Gamma » (pour l'interception des communications russes) ou « Druid » (pour les documents à destination de pays non membres du Pacte UKUSA). Un dernier code indique à qui le message doit être transmis via « Platform » (système central) , « Alpha » (GCJQ britannique), « Echo » (DSD australien), « India » (GCSB néo-zélandais), « Uniform » (CSE canadien) et « Oscar » (NSA).

CFIUS : le « Committe on Foreign Investment in the United States » se consacre depuis à examiner pour le compte de la Maison-Blanche tous les projets de cession à des étrangers d'entreprises américaines constitutives du patrimoine technologique et économique du pays. Placé sous l'autorité du secrétaire au Trésor, il rassemble les représentants de 11 agences fédérales, dont le FBI, la NSA, le NSC et l' « Office of Strategic Industries and Economic Security » du département du Commerce.

COMINT : collecte et traitement des communications extérieures (acheminées par des moyens électromagnétiques), ainsi que l'interception et le traitement des communications écrites non cryptées, de la presse et de la propagande, à moins qu'elle ne soit cryptée (Directive du DoD du 23/12/91). Le renseignement des communications (Comint) est défini par la NSA comme « l'information technique et le renseignement dérivé des communications étrangères ainsi que de leurs destinataires » (i.e. : interception des signaux de communication étrangers et extraction de renseignements de ces signaux par des personnes autres que celles auxquelles il étaient destinés). Comint est un composant majeur de Sigint

(renseignement sur les signaux), qui inclut également la collecte des signaux de non-communication, tels que les émissions des radars.

CIA : c'est l'agence la plus connue, en raison de ses interventions dans le passé à Cuba, en Europe de l'Est et en Amérique du Sud. Elle emploie aujourd'hui environ 16 000 personnes et dispose d'un budget approximatif de 20 milliards de francs (les chiffres exacts sont secrets). C'est elle qui a notamment en charge le travail d'espionnage sur le terrain (grâce à ses 5 000 agents de la Direction des Opérations). Longtemps infiltrée par plusieurs agents soviétiques (puis russes), marquée par de nombreux échecs, fortement décriée, elle a connu plus de six directeurs depuis la fin de la guerre froide. Celui-ci est pourtant toujours un proche collaborateur du président.

CSE : le « Communications Security Establishment » est l'agence SIGINT canadienne.

Cônes de silence : ce concept vise pendant un laps de temps, à perturber les communications électroniques de leaders politiques étrangers, médias ou ONG dont les positions pourraient menacer les actions planifiées par le Pentagone. Cela consiste à créer des cônes de silence dans le cyberespace, à des endroits très précis, par exemple aux points d'entrée des routeurs ou dans les centrales des fournisseurs d'accès. La surveillance par le FBl, notamment grâce à sa *CALEA, Implementation Section*, des carrefours électroniques que représentent les *Internet Exchange Points (IXP)*, rend cette théorie aisée à mettre en application.

DARPA : Defense Advanced Research Projects Agency des USA.

Dictionnaire : maillage d'ordinateurs à très forte puissance en réseau capables d'absorber, d'examiner et de filtrer en temps réel d'énormes quantités de messages numériques et analogiques, d'extrapoler les données de ceux qui contiennent chacun des mots clés programmés, de les décoder et de les envoyer automatiquement au QG des renseignements des cinq pays intéressés. Chacun d'eux possède un identifiant codé qui lui est propre.

DIA : la Defense Intelligence Agency, exclusivement militaire, regroupe 19 000 employés pour un budget d'environ 12 milliards de francs – soit six fois le budget de l'ensemble des services secrets français. Elle coordonne le travail des agences de renseignement de chaque arme (Navy, Air Force, Army) et dispose de sa propre force de recherche (2 000 agents à l'étranger).

DSC : le Defense Satellite Communications System est responsable des communications satellites de l'US Army. Il accomplit des missions de conseil et de définition sur l'ensemble des moyens de l'US Army Information Systems Engineering Command (USAIEC).

DSD : Defence Signals Directorate (Directorat des signaux de la Défense); l'agence SIGINT australienne.

DSS : le Defense Security Service est l'organe de sécurité du Pentagone. L'une de ses missions est la sécurité des systèmes d'information ainsi que le contrôle des accès aux serveurs et de la délivrance des logins. Ainsi, le contrôle de l'utilisation des réseaux classifiés du département de la Défense (Intelink), favorise sa collaboration croissante avec la NSA : en mai 2001, il a d'ailleurs intégré les locaux de Fort Meade qui a affecté une partie de ses moyens – à l'été 2001 — au soutien de la subdivision DSS-2, responsable des contrôles d'accès aux divers réseaux des SR américains.

ELINT : (renseignement électronique) c'est l'interception, le traitement et l'analyse des radiations électromagnétiques ne concernant pas les communications émises par des équipements militaires (comme un radar) pendant son fonctionnement.

EP-3 : avion-espion des forces navales américaines volant à faible vitesse afin d'effectuer des interceptions dans la bande des micro-ondes, des ondes ultracourtes et des ondes courtes. Les signaux sont exploités directement à bord.

Espionnage économique : selon Samuel Porteous du Service Canadien du Renseignement de Sécurité (SCRS) c'est « le fait, pour un gouvernement étranger et ses affidés d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour acquérir des renseignements économiques ».

Fluent : logiciel de traduction simultanée qui cherche, traque et traduit les documents écrits en langue peu conventionnelles (il est également utilisé par la CIA).

GCQH : le Government Communications Headquarter est le service d'interception des communications britannique. Il compte quelque 11 500 agents dont la moitié seulement travaille au quartier général de Cheltenham. Les autres sont affectés aux bases étrangères, du Sri-Lanka (Perkar) à l'Allemagne (Kiel), en passant par la Turquie et Chypre.

GIG : le Global Information Grid est un réseau maillé à l'échelle planétaire destiné à connecter l'ensemble des systèmes du Pentagone, dont les systèmes de combat.

Groundbreaker : programme de rénovation des technologies – gestion des ressources informatiques non opérationnelles — de la NSA à hauteur de 5 milliards de dollars sur dix ans.

HSC : le Homeland Security Council a été créé par le Président Bush à la suite des attentats du 11 septembre 2001. Ses missions, définies par l'Executive Order du 8 octobre 2001, sont la coordination dans les domaines du renseignement, de la prévention, de la préparation à la gestion des conséquences des attentas. Ces fonctions s'exercent également en temps de crise. Ses membres de droit sont le Président et le vice Président, les secrétaires à la Défense, à la Justice, aux Transports, à la Santé, les directeurs de la FMA, du FBI et de la CIA.

ILETS : l'International Law Enforcement Telecomunications Seminar rassemble les membres d'UKUSA et de nombreux pays européens, dont le rôle est d'exercer des pressions sur les fabricants de systèmes de communications, afin qu'ils conçoivent leurs matériels de façon à ne pas empêcher l'interception et le décodage effectués par les agences nationales de sécurité.

Intelink : né en 1994, sous l'impulsion de James Woolsey, directeur de la CIA, et de John Deutch, secrétaire d'État adjoint à la Défense, Intelink rassemble les treize agences de renseignements américaines. Ses objectifs : mettre en commun des informations jusque-là dispersées et augmenter la réactivité du renseignement américain. Ce réseau est aujourd'hui régulièrement utilisé par plus de cinquante mille personnes et compte près de quatre cents serveurs répartis sur trois cents sites hautement surveillés. La clé de ce succès est l'interopérabilité du réseau et l'utilisation de protocoles et de logiciels commerciaux (protocole TCP/IP et navigateurs classiques, forums de discussion, vidéoconférences, des dialogues en ligne, moteurs de recherche). Le dernier des réseaux en date est Intelink-Commonwealth qui regroupe les services de renseignements militaires américain (DIA), britannique (DIS), australien (DIO) et le J2 canadien.

Intelsat : l'Organisation Internationale des Télécommunications par Satellites a été créée en 1964. C'est une autorité dont la structure est similaire à celle des Nations Unies et dont l'activité consiste à assurer les communications internationales. 144 gouvernements en sont membres. Intelsat dispose d'une flotte de 20 satellites géostationnaires qui mettent en contact plus de 200 pays et dont les services sont loués à ses membres, lesquels disposent de leurs propres stations au sol.

Jam Echelon *Day* : il a pour objectif de perturber les moyens mis en place par la National Security Agency américaine pour intercepter les communications mondiales. Pour ce faire, il encourage tous les internautes à inclure des mots-clés réputés subversifs dans leurs messages électroniques.

Key Recovery Technology : utilisation de moyens de cryptage dont une partie de la clé est détenue par les agences de renseignement US.

Keyhole : nom de code des satellites d'observation du NRO (l'un des derniers était le KH 12 Imporved Crystals). Ils permettraient d'observer la terre de jour comme de nuit avec une précision de quelques centimètres.

Lacrosse : satellites fabriqués par le NRO qui, dotés d'un radar, « voient » à travers la nuit ou les nuages.

Magic Lantern : virus/ver, couplé au système Carnicore, développé par Booz Allen & Hamilton à la demande du FBI chargé d'effectuer des intrusions afin de réaliser des écoutes électroniques. Ce logiciel,

dont l'existence a été révélée pour la première fois par la chaîne Internet MSNBC en novembre 2001, appartient à la catégorie des « keyloggers ». Installé sur un micro-ordinateur, le keylogger surveille et garde en mémoire les touches frappées au clavier par l'utilisateur.

MASINT : (Measurment and Signature Intelligence) dans le domaine des interceptions (cf. Comint and Elint), cette technique consiste à écouter tous les moyens télémétriques de positionnement ou de ciblage. Il s'agit d'identifier et d'analyser tous les signaux radars, infrarouges, otiques ou acoustiques. Ces moyens sont destinés aux armées de l'air et notamment la *National Air Intelligence Center*, installée sur la base de Wright-Patterson.

Memex : ce système de filtrage élaboré par la firme britannique Memex Technology est en mesure de rechercher de grandes quantités de données au départ de concepts-clés consignés dans des *Dictionnaire*s ; un tri s'effectue ensuite avant expédition.

Mercury : nom de code des premiers satellites d'interception des communications transitant par le réseau Intelsat utilisés par la NSA (orbite géostationnaire). Ce sont des paraboles captant et réacheminant les signaux vers une station d'écoute qui se charge du décryptage.

N-gram analysis : système d'analyse des documents textuels, dans ce contexte, système pour comparer un vaste ensemble de documents à un plus petit qui définit un sujet d'intérêt. La méthode repose sur le comptage de la fréquence à laquelle des groupes de caractères d'une longueur *N* apparaissent dans chaque document.

NIAP : le National Information Assurance Partnership est un programme consacré à l'évaluation de la sécurité des systèmes informatiques. Le NIAP travaille notamment en collaboration avec le National Institute of Standards and Technologie (NIST) et la NSA.

NNI : la NSA est responsable de la National Nanotechnology Initiative qui vise à développer les recherches dans les nano sciences et leurs applications.

NSG : le Naval Security Group, de Fort Meade, en raison de son statut d'organe de sécurité rattaché à la direction des opérations de l'US Navy, a installé des détachements dans le monde entier durant la Guerre Froide. Progressivement, il a assuré la sécurité des communications de la Navy, puis les activités de chiffrement pour les unités projetées à l'étranger, et enfin les missions d'interceptions de la NSA réalisées depuis l'étranger. En avril 1994 ses activités ont plus spécifiquement été dirigées vers la guerre de l'information et les écoutes. La note de l'*Office of the Chief of Naval Operations* du 1er avril 1994, référencée OPNAVINST 5450.191 B assigne au NSG les responsabilités d'agent exécutif de la NSA dans le domaine de l'*information warfare*. Il entretient 25 détachements répartis sur l'ensemble des continents, chargés de mettre en œuvre les moyens de la NSA. Pour l'Europe, ils sont positionnés à Naples et à Agnano en Italie ; à Augsburg et à Todendorf en Allemagne ; à Menwith Hill, à Edzell, à Digby et à Londres en Grande-Bretagne ; et enfin à Rota en Espagne. L'importance des activités du NSG a été mise en évidence lors des premières révélations sur le réseau Echelon. Il s'agissait en particulier des écoutes des satellites de télécoms réalisées depuis la base de Sugar Grove aux États-Unis.

NRO : le National Reconnaissance Office a en charge, pour le compte de l'armée de l'air américaine, la planification de l'espionnage par satellites, en relation avec la NSA. Ce service, créé en 1961, mais officiellement reconnu par le Pentagone qu'en 1992, mobilise un budget de 6 à 8 milliards de dollars soit le quart des crédits alloués à la communauté du renseignement US. Il emploie 2000 personnes. Sa dernière réussite connue est le lancement d'une constellation de satellites relais qui permettent la transmission des images en temps réel. Le NRO est l'œil, quand la NSA est l'oreille de l'espionnage américain...

NSIRC : le National Security Incident Response Center est une structure du département de la Défense placée sous la tutelle du National Security Operations Center (NSOC), l'une des sous-directions de la NSA en cas de menace, la NSIRC émet un « Cyber-CRITIC » qui remonte à travers les diverses instances chargées de la protection des infrastructures critiques, notamment le National Infrastructure Protection Center (NPIC, sous la tutelle du FBI).

Oasis : logiciel mis au point par « The Office of Advanced Information Technology » (filiale de la CIA) qui permet de récupérer des informations en fonction de mots clés, mais aussi de convertir les signaux sonores de la télévision et de la radio en format texte, ou encore de définir et de reconnaître une voix.

ONYX : nom du projet de système d'interception des communications en cours de développement en Suisse.

OSI : l'Office for the Strategic Influence a été créé dans la plus grande discrétion au sein du Pentagone en octobre 2001. Le général Worden, un ancien de l'US Space Command, en charge du projet, prévoit une large gamme de missions : « Ça ira de la mission *noire* à la mission *blanche* à destination des médias étrangers ; de la désinformation à l'information. »

OSP : l'*Office of Special Plans*, a été créé le après 11 septembre 2001 par Paul Wolfowitz, le numéro deux du Département de la Défense. Ce Bureau a pour mission de trier les données recueillies par les différentes agences de renseignement (CIA, DIA, NSA), afin d'établir des synthèses et les remettre au gouvernement.

Oratory : logiciel qui permet de d'extraire automatiquement les messages oraux contenant un mot prédéfini (cette technique est loin d'être au point du fait même de la voix humaine).

Patriot Act : le Sénat américain a voté ce texte le 24 novembre 2001 afin de renforcer les moyens d'écoutes, de surveillance et de contrôle des communications du territoire national par l'emploi du système Carnivore (rebaptisé DCS 1000), complément amélioré du système Echelon. Il s'agit d'un pas de plus vers la maîtrise totale de l'information.

Plaform : depuis 1983, 52 systèmes informatiques de la communauté UKUSA sont reliés entre eux par un réseau informatique désigné Platform, basé au QG de la NSA à Fort Meade, Maryland. Le système actuel s'intitule Platform II.

SCOL : la « Sigint Combined Operations List » est le document visant à répartir les tâches des membres du pacte UKUSA. Personne n'en a jamais vu trace.

SCS : la CIA et la NSA ont créé le « Special Collection Service », unité secrète qui opère à partir de quartiers généraux situés près de Beltsville, dans le Maryland. Sous couverture diplomatique, les unités d'interceptions (Éléments Spéciaux de Collectage) qui en dépendent montent des services d'écoute dans les ambassades et consulats américains. Parfois ce sont les alliés du Commonwealth — moins suspectés d'espionnage — qui réalisent l'opération. L'objectif est de trouver des procédés qui permettent des intrusions authentiques — mais secrètes — dans les systèmes adverses, c'est-à-dire des mécanismes électroniques et informatiques « actifs », comme par exemple, la possibilité d'introduire des virus, de collecter des mots-clés qui faciliteront les repérages en toute impunité, et de s'infiltrer dans les ordinateurs ou dans les réseaux de communications. Seule la CIA, grâce à ses agents spécialisés dans les « covert actions », autrement dit les opérations clandestines sur le terrain, est en mesure d'intervenir. C'est la raison de cette alliance entre la CIA et la NSA, au travers d'équipes conjointes qui travaillent au profit du SCS.

Shamrock : cette opération consistait, dès 1945, en l'obtention systématique, auprès des bureaux des principales entreprises de télégraphie américaines, des messages circulant par câble — ou par téléphone — vers l'étranger.

SIGINT : on entend par « signal intelligence » des informations de caractère technique et ayant trait au service d'informations qui sont obtenues par des signaux notamment des télécommunications sans que le destinataire de l'information soit impliqué.

Silkworth : système au sol, développé à partir d'août 1978 par Lockheed à la station de Menwith Hill, de traitement des informations relayées par les satellites d'interception des signaux de l'U.S. Air Force, Chalet, Vortex et Mercury.

Smasher : ce nom de code désigne un nouveau système pour briser les codes en utilisant des capacités de stockage et des vitesses de traitement jamais égalées grâce à la technologie des ordinateurs holographiques. Le brevet est le nº 6.026.053, à l'Office des Brevets des USA.

Statmux : système américain permettant de trier les messages : chaque message individuel est isolé et les bandes de fréquences intéressantes (utilisées pour les communications importantes) sont envoyées au *Dictionnaire*.

TELINT : c'est l'interception, le traitement et l'analyse de télémétrie étrangère (renseignement télémétrique).

USS : (United State Signal Intelligence) c'est le système SIGINT des États-Unis qui comprend la NSA, les unités de support militaire collectivement appelées le Service de Sécurité Central, les départements de la CIA et d'autres organismes.

Venona : opération à succès de la NSA qui permit aux États-Unis et à la Grande-Bretagne de démasquer un certain nombre d'agents doubles travaillant pour Moscou, dont Kim Philby.

Vortex : nom de code de la constellation de satellites-espions mis en orbite par la NSA dans les années 70. Celui qui couvre l'Europe est en orbite à 36 000 km d'altitude au-dessus de la Corne de l'Afrique. Il est contrôlé par la base terrestre britannique de Menwith Hill.

X Group Special Acces System : les hackers de la NSA. Leurs missions sont diverses, mais convergent vers un seul et unique but : rapporter de l'information, aller la chercher là où elle se trouve, c'est à dire dans le cœur même des systèmes informatiques. Certains d'entre eux, appelés « the snifers », les renifleurs, ont pour seule et unique mission de trouver, d'archiver et d'exploiter les failles des principaux serveurs et systèmes informatiques. (Information sujette à caution, car contenant des fautes de traductions et étant en provenance du site de JPNEY, Intelink.org)

Historique de la National Security Agency

Introduction

Vous pensez être anonyme sur le net, avoir une vie vraiment privée parce que nous sommes 6 milliards sur terre ? Illusion du monde moderne et voici pourquoi.

Chaque pays possède comme il se doit sa propre agence de renseignement. Mais s'il y a bien un pays qui en possède une digne de ce nom, ce sont les États Unis.

Cette agence s'appelle la NSA (National Security Agency). Si les États-Unis sont aujourd'hui le pays le plus puissant du monde aussi bien en terme militaire qu'économique, c'est sûrement en bonne partie grâce à elle.

La NSA est née pendant la 2e guerre mondiale, en 1941, après l'attaque de Pearl Harbor par les Japonais.

Afin d'intercepter et de décoder les communications militaires des Nazis et des Japonais, elle a mis en place progressivement des moyens technologiques fabuleux. Aujourd'hui, la NSA peut intercepter toute forme de communication dans pratiquement n'importe quel pays du monde pour ensuite les utiliser à son avantage en termes économique, stratégique et politique.

1 — Qui sont la NSA et le NRO ?

Tout commença probablement en 1941 lors de l'attaque surprise des Japonais à Pearl Harbor. Les Américains n'avaient semble-t-il pas pu l'anticiper. Ils développèrent alors avec les Britanniques le gigantesque centre d'écoute de Bletchley Park en Grande-Bretagne. Ce centre d'écoute devait permettre deux choses : intercepter et décoder les communications militaires des Nazis et des Japonais.

Près de 10 000 personnes, dont des mathématiciens très renommés comme Alain Turing pour n'en nommer qu'un, travaillaient dans ce projet dénommé le Projet ULTRA.

Le pacte UKUSA

Le United States Sigint (Signal Intelligence) — USS — comprend la NSA, des unités de support militaire appelé le Central Security Service, et une partie de la CIA.

Après la collaboration de la Grande-Bretagne et des États-Unis durant la 2ème guerre mondiale, en 1947, ces deux pays signèrent un pacte secret pour continuer leur collaboration axée sur les écoutes.

Trois autres nations anglophones rejoignirent le pacte peu de temps après : le Canada, l'Australie et la Nouvelle-Zélande en tant que membres secondaires.

Ce pacte n'a été rendu public qu'en mars 1999, quand le gouvernement australien confirma que son agence d'écoute, le « Defense Signals Directorate », « coopérait avec d'autres agences étrangères sous le pacte UKUSA ».

Ce pacte permet de partager les ressources, les tâches et les résultats entre les gouvernements participants au système Echelon qui sera expliqué dans le détail dans les pages suivantes.

Le budget de la NSA

Selon les publications officielles du gouvernement Américain, le budget de la NSA s'élevait à 4 milliards d'US$ en 1996, ce qui représente environ 28 milliards de FRF au taux de change de 1 US $ = 6 FRF. Pour information, Georges Tenet directeur de la CIA, a révélé (cf. *Nouvel Observateur* - N°1779 - 10/12/1998) que le budget total des treize agences de renseignements US s'élèverait à environ 28 milliards de dollars pour l'année 1999.

Pour donner un ordre de grandeur, cela représente 2,1 % du PIB Français, soit pratiquement l'équivalent de la croissance en France.

2 — Le NRO (National Reconnaissance Office).

Historique et présentation

Le NRO (National Reconnaissance Office) est l'agence américaine concevant et fabriquant les satellites-espions. On sait très peu de choses sur cette agence. Par exemple jusqu'en 1992, on ne connaissait même pas son entête de papier à lettres. Son véritable budget est classé Secret Défense.

Le NRO est née en le 25 août 1960 suite à une controverse intense entre la Maison Blanche, la CIA et le Département de la Défense pour déterminer qui aurait la responsabilité de la reconnaissance par satellite du pays, voire de suivre un véhicule ou une personne.

Cette agence, sous l'impulsion du Président Eisenhower, fut créée dans le but d'assurer les intérêts de tous les demandeurs, aussi bien dans le renseignement civil que militaire.

Aujourd'hui, le NRO posséderait des capacités d'observation uniques au monde. Cette agence est d'ailleurs le fournisseur officiel de la NSA en terme d'imagerie satellite.

Les noms de codes relativement connus de ces satellites sont les *Keyhole*. L'un des derniers en date s'appellerait *KH 12 Imporved Crystal*. Il permettrait d'observer la terre de jour comme de nuit en utilisant la technologie radar avec une précision de quelques centimètres (il devient facile de reconnaître une marque de voiture, de compter le nombre de personnes sur un square).

En sus de ces satellites d'observation, il existerait également les satellites d'interception et d'écoute des communications. Ceux-là sont utilisés par la NSA. Leurs caractéristiques sont inconnues, mais il y en aurait un certain nombre en orbite géostationnaire (cela signifie que le satellite reste fixe par rapport à un point de la terre) pouvant intercepter les communications transitant initialement vers le réseau Intelsat (organisme civil de télécommunications possédant plusieurs satellites) qui a pour mission de relayer nos communications transcontinentales.

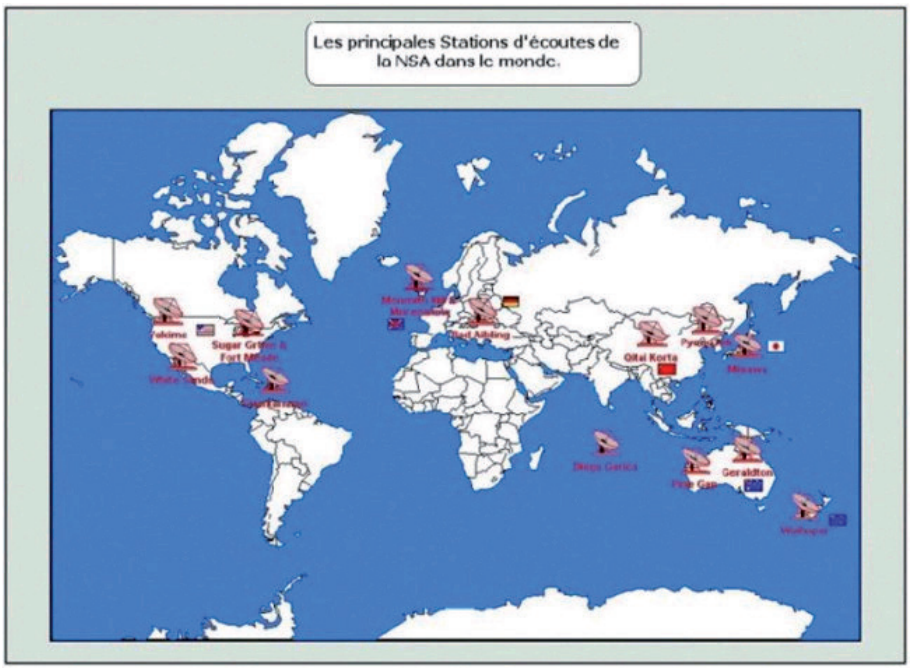
Ces satellites développés par le NRO ont pour nom de code *Mercury*. Ils sont placés juste à côté des satellites INTELSAT. Leur diamètre serait énorme (entre 80-100m ?). Ce sont des gigantesques paraboles dépliables qui captent le signal, tout comme l'INTELSAT, puis le réacheminent vers une station d'écoute qui se charge de décrypter les communications (vocal, fax, mail, télex) en utilisant les *Dictionnaires*.

Pour plus de détails techniques, lire le chapitre Réseau Échelon — section Moyens matériels & humains.

Budget et fonctionnement.

Il y a quelques années, le Congrès américain a découvert que le NRO avait dissimulé dans sa comptabilité environ 25 milliards de Francs. La manipulation comptable était légale, mais elle permettait surtout de pouvoir mener des opérations clandestines (notamment l'installation de systèmes d'écoutes) sans alerter les pays étrangers. Tout comme la CIA d'ailleurs. Comme précisé ci-avant, le budget du NRO reste classé secret défense. Néanmoins, on peut l'estimer à environ 8-9 milliards d'US$. Soit la une somme de 50-60 milliards de FRF. Les derniers chiffres officiels donnés datent par ailleurs de 1996.

Principe général de fonctionnement du réseau Echelon



Le schéma ci-dessus situe les principales stations d'écoutes de la NSA

Le réseau Echelon tel que nous le connaissons a été conçu et construit par la NSA dans les années 80. Il permet d'intercepter de manière non discriminatoire, des e-mails, des fax, des télex et des communications téléphoniques transportées sur pratiquement n'importe quel support (satellites, câbles sous-marins, etc.) et par n'importe quel réseau de télécommunication.

Ce système, à la différence des autres développés pendant la Guerre Froide, est avant tout à but non militaire : gouvernements, entreprises, individus sont devenus les cibles primaires du réseau Echelon.

Bien sûr, nous savons tous que dans chaque pays, les organismes d'espionnage et de contre-espionnage réalisent des écoutes sur leur propre territoire pour assurer la sécurité du pays. Mais ce qui est extraordinaire, c'est qu'Echelon fonctionne à l'échelle planétaire.

ECHELON n'a pas pour but premier d'intercepter des communications sous toutes ses formes d'un individu en particulier, mais plutôt d'intercepter des informations en masse pour réaliser ensuite le tri de ce qui est intéressant au moyen de super ordinateurs (les *Crays*) et des *Dictionnaires*.

Pour cela, comme nous le verrons par la suite, un réseau de stations d'écoute a été établi au niveau mondial pour permettre ces interceptions. Certaines stations écoutent des satellites, d'autres des communications terrestres, voire des communications radio.

Les antennes d'interception dans le monde

Le réseau Echelon permet de relier toutes ces stations pour fournir aux États Unis, la possibilité d'intercepter un très grand nombre de communications transitant sur la planète.

– Sugar Grove – en West Virginia. Six paraboles sont pointées vers l'Europe et l'atlantique.

Sugar Grove se trouve à environ 300 Km au Sud-Ouest de Washington. Il serait dirigé par l'US Naval Security Group ainsi que l'US Air Force Intelligence Agency.

Vue terrestre de la station Sugar Grove

Nom des stations	Pays	Fonctions & commentaires
Yakima	Etats Unis	Écoute (Intelsat Océan Pacifique)
Sugar Grove	États Unis	Écoute (Intelsat Océan Atlantique)
Fort Meade	États Unis (Maryland)	Écoute+analyse+archivage (siège de la NSA)
Morwenstow	Royaume Uni	Écoute (Europe)
Menwith Hill	Royaume-Uni	Écoute + photos satellites
Geraldton	Australie	Écoute (Région Sud Asie)
Waihopai	Nouvelle Zélande	Écoute (Région Sud Asie)
White Sands	Etats Unis (Nouveau Mexique)	Photos satellites
Guantanamo	Cuba	Écoute (relation cuba - ex URSS)
Bad Aibling	Allemagne	Écoute (bloc des pays de l'Est)
Qitai Korta	Chine	Écoute (Russie & Corée du Nord, Inde ?)
PyongTaek	Corée du Sud	Écoute (Corée du Nord & pays voisin, Chine...)
Misawa	Japon	Écoute
Pine Gap	Australie	Écourte + photos satellites
Diego Garcia	Océan indien	Écoute (pays de l'océan Indien)

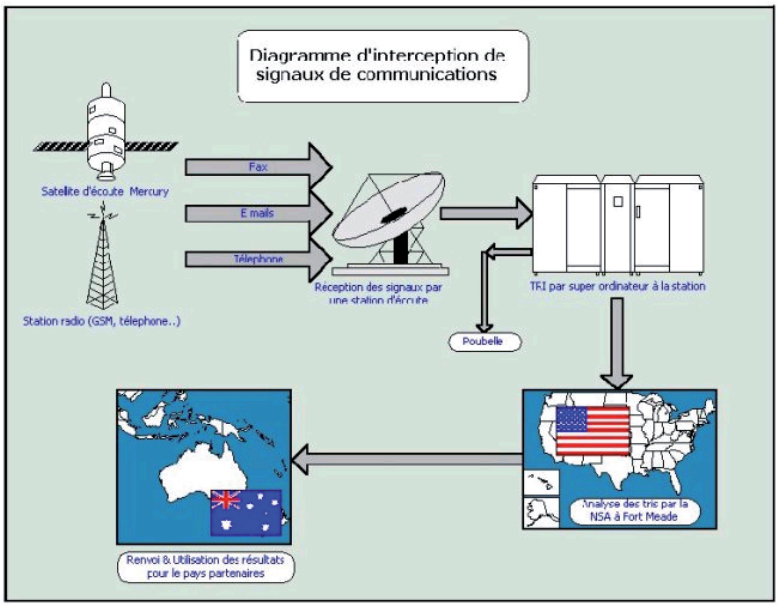
Tableau exhaustif des stations d'écoutes appartenant à la NSA :

Méthode d'interception

Chaque station du réseau ECHELON utilise des super ordinateurs par lesquels transitent tous les messages. Dans ces ordinateurs, des *Dictionnaires* contenant des mots clés préprogrammés. Ainsi, des mots relatifs à des sujets types, des villes, des noms, etc. permettent de réaliser des tris, afin de produire des dossiers cohérents.

Bien que des milliers de messages se déversent dans ces ordinateurs chaque minute, ces derniers sont lus et traités en temps réel. Le patron de la NSA, dans l'une des rares interviews affirmait que l'agence devait traiter toute les 3 heures, autant d'informations qu'il y en a dans la bibliothèque du Congrès Américain, la plus grande du monde.

Diagramme décrivant l'opération :



5 étapes sont nécessaires à l'interception :

— dans une station d'écoute d'un pays du pacte, tous les signaux, numériques ou analogiques (téléphone, GSM, ondes radio, signaux satellites...), sont captés par des stations d'écoutes ;

— ils sont ensuite amplifiés puis triés. Seuls les messages intéressants sont retenus ;

— ils sont ensuite passés à la moulinette des super ordinateurs très puissants contenant les *Dictionnaires*. Chaque station possède d'ailleurs son propre dictionnaire afin de mieux coller à l'environnement local. Par un système de mots clés contenus dans ceux-ci (exemples : NSA, bombe atomique, C4, terrorisme, etc.), toutes les transmissions en rapport avec ces mots et ces concepts sont conservées, cryptées, puis transmises aux États-Unis ou aux partenaires ;

— au siège de la NSA, à Fort Meade dans le Maryland (près de Washington), les messages sont décryptés, analysés puis classés ;

— les écoutes ainsi traitées sont ensuite renvoyées aux pays intéressés sous forme de rapports, de notes succinctes ou de compilations.

Exemples d'écoutes commerciales

En 1994, la NSA avait intercepté des appels téléphoniques entre Thomson-CSF et le Brésil pour le projet SIVAM, un système de surveillance de la Forêt Amazonienne de 1,3 milliard d'US$. Thomson était soupçonné d'avoir « acheté les membres stratégiques du gouvernement brésilien ». Conclusion, le contrat fut remporté par Raytheon Corporation qui annonça peu de temps après : « *le Département du Commerce américain a travaillé durement pour soutenir l'industrie US dans ce projet* ».

Au passage, la société Raytheon assure la maintenance et l'ingénierie de la station d'interception du réseau Echelon à Sugar Grove.

En 1995, par l'intermédiaire d'un satellite de communications commercial, la NSA a réussi à récupérer tous les fax et conversations téléphoniques entre le consortium Européen AIRBUS, la compagnie d'aviation Saoudi National Airlines et le gouvernement saoudien. L'agence avait trouvé que les commerciaux d'Airbus offraient des dessous de table aux officiels Saoudiens. L'information fut transmise à Boeing et Mc Donell Douglas Corp, qui firent une offre plus avantageuse pour finalement remporter ce contrat de 6 Milliards d'US$.

Moyens matériels et humains

Antennes, satellites, ordinateurs et réseaux

Les antennes

La récolte systématique de communications transitant par satellite commença pour la NSA en 1971.

Deux stations terrestres furent construites dans ce but :

— la première à Morenstow, Cornouailles, en Grande-Bretagne, avec deux paraboles de 30m de diamètre. La première parabole interceptait les communications provenant de l'Intelsat de l'Océan Atlantique, la deuxième celle de l'Intelsat de l'Océan Indien.

— la deuxième station fut construite à Yakima, près de Washington, pour intercepter les communications transitant par le satellite Intelsat de l'océan Pacifique.

La situation resta inchangée jusqu'à la fin des années 70. C'est alors qu'un troisième site, toujours aux États-Unis, fut installé à Sugar Grove, en « West Viriginia ». La responsabilité du site fut confiée à l'US Naval Security Group.

Par la suite, le réseau d'écoute Echelon se développa en parallèle du nombre croissant de télécommunications entre 1985 et 1995. Des stations furent implantées au Canada, en Australie ainsi qu'en Nouvelle-Zélande. Celles qui existaient déjà, furent agrandies et modernisées.

Comme montré plus haut, une quinzaine de stations d'écoute principales réparties dans le monde seraient en activité actuellement. Il existe sûrement d'autres stations, mais elles seraient plus discrètes, plus petites et plus spécifiques à la région voire au pays où elles sont installées.

Aujourd'hui, on estime, que le réseau ECHELON utilise 120 antennes réparties dans les pays du pacte UKUSA, à des fins d'écoutes et de renseignements.

Les catégories d'antennes (sachant que plusieurs types d'antennes peuvent se trouver sur une même station d'écoute):

— 40 sont pointées vers des satellites commerciaux ;

— 30 sont dirigées vers les satellites d'écoute (type *Mercury*, *Keyhole*...);

— 50 étaient pointées vers l'ex-Pacte de Varsovie, mais un certain nombre a sans doute été réorienté vers d'autres objectifs, tels que les satellites commerciaux.

Les satellites

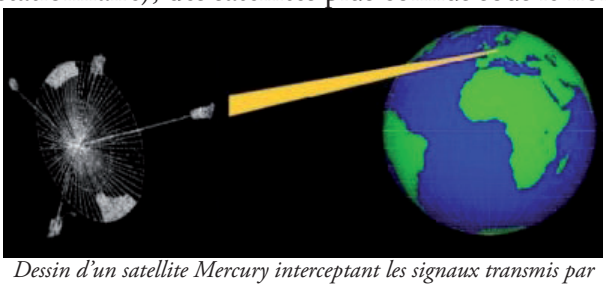
On distingue trois classes de satellites :

— *Satellite géostationnaire* : c'est un satellite de type *Mercury* placé juste à côté d'un satellite relayant des communications transcontinentales de type Intelsat. De par la taille de sa parabole (de 80 à 100m), les signaux initialement reçus par le satellite Intelsat le seront également par le *Mercury*. Ce dernier les retransmettra à la station d'écoute la plus proche afin d'en analyser les données.

— *Satellite d'observation* : c'est un satellite de type *Keyhole* utilisant une technologie radar, qui permet de voir de jour comme de nuit et sous les nuages avec une précision de l'ordre de quelques centimètres. Ces satellites évolueraient à des altitudes variant entre 200 et 1000 km. Le dernier modèle a pour nom de code *KH-12 Improved Crystal*.

Aucune spécification officielle n'existe sur ce produit. Selon les Services secrets français, une quinzaine seraient en orbite actuellement.

— *Satellite d'écoute basse altitude* : cette classe de satellites sert de système d'écoute d'appoint principalement pour les régions dans les latitudes proches du Pôle Nord. Les *Mercury* couvrant mal ces régions (à cause de leur orbite géostationnaire), des satellites plus connus sous le nom de *TRUMPET* évoluent à



Dessin d'un satellite Mercury interceptant les signaux transmis par des antennes terrestres à destination des satellites relais Intelsat.

des orbites polaires elliptiques, leur permettant de rester longtemps dans les régions du Nord. L'Agence peut alors écouter tous les transmetteurs dans ces zones et par la même occasion intercepter les signaux envoyés par l'ex-URSS à ses satellites de communications évoluant dans les mêmes orbites.

Petite précision tenant de l'anecdote. Motorola a lancé en 1997 le réseau de communication planétaire connu sous le nom d'IRIDIUM. Ce réseau constitué de 66 satellites évoluant en orbite basse et quadrillant la terre, devait permettre de pouvoir appeler et d'être joignable de n'importe point du globe.

Ce qui posa un problème pour la NSA dans un premier temps, attendu que les communications transitent du téléphone cellulaire directement par plusieurs satellites sans passer par des stations relais terrestres (en revanche INTELSAT utilise le principe des relais terrestre). Mais Motorola étant un gros fournisseur de l'Agence, on peut être sûr que le réseau est largement écouté par celle-ci d'une manière ou d'une autre.

Ordinateurs et réseaux

L'Agence est l'organisme au monde le plus grand consommateur de matériel informatique. Elle travaille par ailleurs en étroite collaboration avec quelques grands fabricants américains tels que Motorola, Intel, IBM, ainsi que le fabricant de super ordinateurs : CRAY/SGI.

Elle possède même sa propre unité de fabrication de composants à Fort Meade, pour éviter les fuites, et produire des processeurs à la demande.

Fournir un bilan informatique de la NSA afin d'estimer sa puissance de calcul est impossible, mais en se fondant sur les informations fournies par CRAY, le listing des 500 ordinateurs les plus puissants du monde, et surtout en essayant de dimensionner les besoins par rapport au volume d'écoute, il devient possible d'émettre quelques hypothèses.

En regardant sur le site de Cray (www.cray.com), on peut se faire une idée des performances des super ordinateurs, le haut de gamme étant le CRAY SV1. Aujourd'hui c'est le super ordinateur commercial le plus puissant du monde (en 2002)[118]. Il est configurable sur mesure en fonction des performances et des attentes du client comme le montre le tableau ci-dessous :

CRAY SV1-1A	CRAY SV1-1	CRAY SV1-4	CRAY SV1-8	CRAY SV1-32	CRAY SV1-32 (?)
Nombre de noeuds SMP	1	1	4	8	32
Performance de pointe	9.6 à 19 GFLOPS	9.6 à 38 GFLOPS	38 à 154 GFLOPS	77-308 GFLOPS	308-1229 GFLOPS
Mémoire	2-16 GB	4-32 GB	16-128 GB	32-256 GB	128-1024 GB
CPU à 4.88 GFLOPS	jusqu'à 3	jusqu'à 6	jusqu'à 24	jusqu'à 48	jusqu'à 192
CPU à 1.2 GFLOPS	4 et plus	8 et plus	32 et plus	64 et plus	256
Cadence CPU (Mhz)	300				
Type de Mémoire	DRAM				
Refroidissement	Air				Air et eau

Noeud SMP : Symmetric Multi Processing. Cela permet de réaliser plusieurs opérations en simultané. Chaque processeur effectue en quelque sorte une tâche particulière, dédiée.

GFLOPS : Giga FLoating Point Operations Per Second. Nombre d'opérations en virgule flottante par seconde. 1 GFLOPS équivaut à mille milliards d'opérations/sec.

Le *Cray SV1* utilise le principe de processeurs parallèles pour augmenter la vitesse de calcul..

Partant du principe qu'il existe une quinzaine de stations d'écoutes terrestres dans le monde, il faut donc par station au moins un super-calculateur, pour réaliser les premiers tris. Les données étant centralisées au siège de la NSA (là où s'effectue le tri final, le classement et les rapports), il faut sûrement rajouter au moins 4 autres super ordinateurs :

— un pour réceptionner les données puis les stocker,

— un autre pour transmettre les résultats aux autres stations amies et ambassades. Cela suppose par ailleurs des capacités de transmissions gigantesques (plusieurs dizaines de Gbits/sec) par fibre optique ainsi que par satellite.

[118] Documentation CRAY disponible sur Internet.

— un, voire deux, pour les opérations courantes au siège (Fort Meade) et le cassage de messages cryptés.

— un pour l'archivage. Celui-ci agira plus en tant que super serveur.

D'autres supers-calculateurs doivent exister, mais de puissance peut être plus réduite mais, surtout, dédiés à certaines tâches, notamment l'analyse vocale des écoutes téléphoniques. À ce propos, des puces spécialisées dans la reconnaissance vocale existent déjà sur le marché.

Nous arrivons donc à une vingtaine de supers-ordinateurs, des capacités de transmission optique/satellite de plusieurs dizaines voire centaine de Gbits/sec et des capacités de stockage pouvant sûrement atteindre des dizaines de milliers de Go. Il sera difficile d'en dire plus par manque d'informations pour l'instant.

Pour terminer sur le chapitre des ordinateurs et réseaux, la NSA serait dotée d'un réseau ultra sécurisé appelé *INTELINK* (Source : *Top Secret Intranet* Ed. Charles Goldfare Series - aut. Frederick Martin). Selon l'auteur, un ancien de l'agence, ce réseau, mis en place depuis 1994, serait relié aux bases de données secrètes de la NSA, de la CIA ainsi que des services spéciaux de l'armée américaine. La manière dont transitent les données n'est pas connue, mais on peut penser que cela s'effectue par satellite et par des lignes spécialisées isolées des réseaux publics.

Il serait consultable depuis n'importe où dans le monde par environ 50.000 officiers de renseignement soigneusement triés sur le volet. Cela inclut bien entendu les principaux décideurs politiques, les ambassades américaines et les espions disséminés un peu partout dans le monde.

Ce réseau donnerait alors accès aux dernières écoutes, photos satellites ou aux rapports d'agents sur le terrain. *INTELINK* comprendrait ainsi plusieurs centaines de milliers de pages.

Superordinateurs de la NSA (2002)

Type d'ordinateur	Puissance (en gigaFlops)
Cray T3E-1200E LC1900	2 280
Cray T3E-900 LC1324	1 191,6
Cray SVI-18/576 (-4Q02)	1 152
SGI 2800/250-2304	1 152
HP SuperDome/552-512	1 130,5
Cray T3E-1350 LC800	1 080
SGI 3800/400-1064	851,2
Cray T3E-1200E LC540	648
Cray T3E-1200E LC540	648
Cray T3E-1200E LC540	648
Cray T3E-1200 LC404	484,8
Cray T3E-1200 LC284	340,8
Cray X1-6/192 (+1Q03)	1 966,08
Total	13 572,98

Les différents types d'écoutes

Les types d'écoutes possibles se décomposent en 4 grands axes :

— Satellites

— Câbles sous-marins

— Internet

— Radio (Micro-ondes, HF...)

Satellites

Comme cela a déjà été expliqué précédemment, les satellites de la NSA se positionnent de manière à être proches des satellites de communications civils afin de « copier » les signaux pour les retransmettre vers une station terrestre d'écoute qui se chargera de décrypter et d'analyser les messages.

Câbles sous-marins

Aujourd'hui une grande partie des communications transcontinentales passent par des câbles posés au fond des océans. Ces câbles sont maintenant pour la plupart en fibre optique, suite au besoin de plus en plus croissant de vouloir communiquer. Les débits par câble sont de l'ordre d'une dizaine de Gbits/sec ce qui permet d'acheminer des dizaines de milliers de communications téléphoniques simultanément.

On peut penser qu'il est impossible d'intercepter des signaux lumineux d'une fibre optique en raison du fait que la lumière ne produit pas d'émissions électromagnétiques, et qu'intercepter le signal lumineux sur une fibre reviendrait à rompre la communication.

Selon certains spécialistes, il n'en est rien. Le signal lumineux dans une fibre se dégradant au fur et à mesure du chemin parcouru à cause du support[119] (qui bien qu'étant un matériau translucide présente une certaine opacité), a besoin d'être amplifié environ tous les 100 Km par ce que l'on appelle des répétiteurs. À ce point précis, le signal optique est converti en un signal électrique numérique pour être amplifié puis reconverti en signal optique. Il devient alors possible de poser une bretelle à cet endroit-là pour transmettre les données vers un satellite relais en basse altitude qui les redirigera vers une station d'écoute, voire de dédoubler le signal sur un câble parallèle pour le réacheminer vers la station d'écoute la plus proche.

La pose d'une « bretelle » à 5.000 m de fond est bien entendu coûteuse en terme d'infrastructure, mais néanmoins tout à fait envisageable.

L'autre solution que la NSA a pu adopter est la pose de matériel d'écoute au point de sortie du câble sur terre ferme. En effet au nom du patriotisme et du pacte UKUSA, La NSA peut très bien imposer ses conditions à certains opérateurs télécoms anglo-saxons.

Internet

On peut penser que c'est là le bât blesse pour la NSA. Internet étant un réseau mondial constitué de milliers de serveurs où des quantités de données gigantesques circulent chaque jour.

Il n'en est rien. Durant les années 80, la NSA et les pays partenaires du pacte UKUSA, pilotait déjà un réseau de communications international plus grand que le Web en utilisant la même technologie.

Selon le partenaire britannique, GCHQ (Governement Communications Headquarters) : « tous les systèmes étaient reliés ensemble dans le plus grand LAN d'Europe (LAN : Local Area Network – réseau local), qui étaient connectés également aux autres sites dans le monde formant le plus grand WAN du monde (WAN : Wide Area Network - réseau local mais au niveau mondial). Le protocole de communication utilisé est le protocole IP (comme celui du Web) ». Ce réseau global, développé sous le nom de : Projet EMBROIDERY, inclut le super serveur de communications de la NSA, PATHWAY. Il permet de fournir un réseau rapide, efficace, sécurisé pour le système Echelon ainsi que les autres systèmes.

Il est fort probable d'ailleurs, que ce réseau s'appelle maintenant : « Intelink ».

[119] Le principal atout des fibres optiques est une atténuation extrêmement faible. L'atténuation va varier suivant la longueur d'onde. La diffusion Rayleigh limite ainsi les performances dans le domaine des courtes longueurs l'onde (domaine du visible et du proche infrarouge). Un pic d'absorption, dû à la présence de radicaux -OH dans la silice, pourra également être observé autour de 1385 nm. Les progrès les plus récents dans les techniques de fabrication permettent de réduire ce pic.
Les fibres en silice connaissent un minimum d'atténuation vers 1550 nm. Cette longueur d'onde du proche infrarouge sera donc privilégiée pour les communications optiques. De nos jours, la maîtrise des procédés de fabrication ont permet d'atteindre couramment une atténuation aussi faible que 0,2 dB/km à 1 550 nm. Après 100 km de propagation, il restera donc encore 1 % de la puissance initialement injectée dans la fibre, ce qui peut être suffisant pour une détection. Si l'on désire transmettre l'information sur des milliers de kilomètres, il faudra avoir recours à une réamplification périodique du signal, le plus généralement par l'intermédiaire d'amplificateurs optiques qui allient simplicité et fiabilité.
Il est à noter que le signal subira des pertes supplémentaires à chaque connexion entre fibres, que ce soit par des traverses ou bien par soudure, cette dernière technique réduisant très fortement ces pertes.

Deuxième point, Internet est originaire des États-Unis suite à l'extension d'ARPANET, l'ébauche du premier réseau reliant les sites militaires américains dans les années 60 pour parer à une éventuelle attaque nucléaire de l'ex-URSS. Le développement du net s'est réalisé aux États-Unis, ainsi que la majorité des ressources qui vont avec (Routeurs, serveurs, backbones[120]...). En clair, cela signifie qu'aujourd'hui les ressources physiques se trouvant majoritairement aux USA, de nombreuses connexions provenant de l'étranger passeront là-bas.

Les messages transitent sur le Web sous forme de « packets[121] » appelés aussi « Datagrams ». Ces datagrams afin d'atteindre la bonne destination, contiennent l'adresse IP (ex : 123.123.123.123) de l'émetteur et du destinataire. Ces adresses étant uniques pour chaque serveur connecté sur le Web, il devient facile de réaliser un tri selon l'origine et la destination. Ce processus, s'effectue bien entendu en permanence par les routeurs et les échangeurs afin d'acheminer correctement les messages ; il facilite ainsi grandement la tâche de l'Agence ou de celles qui écoutent, pour le tri.

Les trajets empruntés par ces « packets », dépendent du point d'origine et de destination, du serveur par lesquels ils transitent, ainsi que de nombreux autres facteurs incluant l'heure de la journée. En effet, les routeurs aux États-Unis sont calmes quand ceux de l'Europe atteignent des pointes d'activité dues au décalage horaire. Il devient alors possible et probable que certains mails devant parcourir une petite distance (par exemple : un mail de la France vers l'Allemagne), doivent d'abord transiter par un échangeur américain ou britannique, ce qui rend l'écoute des mails d'autant plus accessibles par la NSA.

Des sites où sont hébergés les *news groups* tel qu'*Usenet* produisent environ 15 Go de données par jour. Ces données sont accessibles à n'importe qui souhaitant les consulter. La NSA peut donc récupérer tout à fait officiellement ces informations pour un tri futur. D'ailleurs, en Grande-Bretagne, l'agence de la Défense de la Recherche & de l'Évaluation maintient une base de données de 1 Tera Octet comprenant 90 jours de messages Usenet.

La plupart des sites Internet accessibles au public sont parcourus par des « bots » (programme parcourant la page cherchant des mots clés) provenant de moteurs de recherches tels que Altavista, Hotbot, Google…, afin de les indexer. La NSA utilise également les mêmes méthodes pour récupérer les informations intéressantes.

Par exemple, un site basé a New York, connu sous le nom de http://www.jya.com[122] propose de nombreuses informations touchant à la crypto, ou aux différentes méthodes d'écoute. Ce site étant réactualisé très régulièrement, la consultation des logs sur le site montre clairement qu'un « Bot » du Centre de Sécurité Informatique de la NSA, parcourt tous les matins le site afin de chercher de nouveaux fichiers et de les récupérer.

[120] On appelle *backbones* (épine dorsale en Anglais) les réseaux à très haut débit constituant le cœur du réseau Internet. Ces réseaux sont constitués majoritairement de câbles à fibres optiques installés sous les océans et sur les continents, plus quelques liaisons satellites pour desservir des zones plus isolées. Le terme backbone ou réseau fédérateur est aussi utilisé pour désigner le cœur de réseau d'une entreprise. La Commission Spécialisée de Terminologie et de Néologie de l'Informatique et des Composants Électroniques a adopté le terme « dorsale » comme équivalent français de « backbone ».

[121] Un *packet* est un bloc d'information porté par un réseau informatique. Les liaisons d'ordinateur qui ne se font pas par des *packets*, tels que des liens traditionnels de télécommunications de *Point-to-Point*, transmettent simplement des données comme une suite de bytes, de caractères seuls. Quand des données sont composées dans un *packet*, le réseau peut transmettre de plus longs messages plus efficacement et sûrement. Mécanisme de *packet* : un *packet* se compose de trois éléments : le premier élément est un en-tête, qui marque le commencement du paquet, et le deuxième élément est un secteur de données, qui contient l'information à porter dedans le *packet*. Le troisième élément du *packet* est un bas de page, qui marque la fin du *packet*.

[122] Il est à noter que nombre de liens de ce site n'existent plus en revoient sur une page d'erreur, particulièrement ceux concernant la NSA…

Il est admis que le trafic Internet au niveau international contenant des informations pouvant intéresser les agences d'écoutes (mails, transfert de fichiers, réseaux privés virtuels), ne représentent que quelques pour cent de la majorité du trafic sur les points d'échanges américains.

Selon un ancien employé de la NSA, cette dernière avait depuis 1995, installé des logiciels de type sniffers (renifleurs) pour analyser le trafic sur les neuf échangeurs américains (Internet Exchange Point - IXP). Deux de ces points, FIX east, Fix West appartiennent au gouvernement. Ils sont implantés très proches des autres échangeurs appartenant à des sociétés commerciales : MAE East & MAE West (MCI Worldcom). Les trois autres sites sont des échangeurs initialement développés par la National Science Foundation pour fournir au Web américain le backbone d'origine du Web.

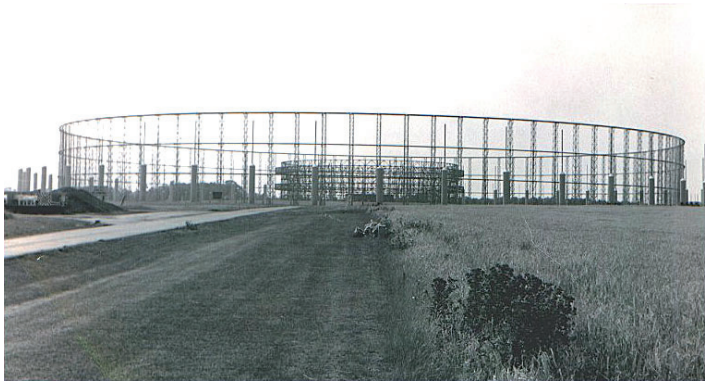
Nom	Lieu	Opérateur	Désignation
FIX East	College Park, Maryland	Gouvernement US	Federal Information Exchange
FIX West	Mountain View, California	Gouvernement US	Federal Information Exchange
MAE East	Washington, DC	MCI Worldcom	Metropolitan Area Ethernet
New York NAP	Pennsauken, New Jersey	Sprintlink	Network Access Point
SWAB	Washington, DC	PSInet / Bell Atlantic	SMDS Washington Area Bypass
Chicago NAP	Chicago, Illinois	Ameritech / Bellcorp	Network Access Point
San Francisco NAP	San Francisco, California	Pacific Bell	Network Access Point
MAE West	San Jose, California	MCI Worldcom	Metropolitan Area Ethernet
CIX	Santa Clara, California	CIX	Commercial Internet Exchange

Tableau des échangeurs américains surveillés par la NSA :

(A titre informatif, en France, il y a 3 échangeurs : 2 à Paris - GIX : Global Internet eXchange- et 1 à Grenoble)

Dernier point, il revient souvent que des grandes sociétés de télécommunications américaines, des éditeurs de logiciels (Microsoft, Lotus, Netscape...) collaborent avec la NSA pour développer des *backdoors* permettant de capturer des informations intéressantes sur les postes sur lesquels ces logiciels sont installés. Ils sont par ailleurs priés de modifier leurs produits destinés à l'exportation afin de faciliter la récupération d'informations.

Bien que la NSA n'ait jamais confirmé ni démenti ces rumeurs, en 1997 un jugement en Grande-Bretagne suite à une affaire de piratage démontra que l'agence surveillait le Web. Des témoins de l'US Air Force travaillant conjointement avec la NSA, admirent utiliser des *sniffeurs* de *packets* et des logiciels spécialisés pour « tracer » les tentatives de piratage d'ordinateurs militaires US. Le dossier s'écroula quand ces témoins refusèrent de fournir les preuves du système qu'ils avaient utilisé.



Station d'interception HF DODJOCC, Chicksands (USA)

Radio (Micro-ondes, HF, etc.)

Les Hautes Fréquences Radio

Une des caractéristiques des ondes radio HF est le fait qu'elles se répercutent contre l'ionosphère et à la surface de la Terre et se propagent donc rapidement d'un bout à l'autre du globe sans nécessiter des infrastructures de réception importantes. Elles ont donc été privilégiées jusqu'au milieu des années 60 pour toutes les communications diplomatiques et militaires.

Les micro-ondes radio

Cette technologie a été introduite dans les années 50, pour augmenter la capacité de transmissions entre cités pour le téléphone, le télégraphe et plus tard pour la télévision. Elles nécessitent à cause de la courbure de la terre des relais tous les 30 à 50 kilomètres sous la forme d'antennes de 1 à 3 m de diamètre au sommet de tours ou de building.

Le personnel humain

On sait seulement qu'environ 100.000 personnes travaillent directement ou indirectement pour la NSA. Par ailleurs, la NSA est probablement le plus grand recruteur de mathématiciens au monde.

Après la chute du mur de Berlin et de l'URSS, il semblerait que de nombreux savants russes se soient fait recruter par les États-Unis. L'État Russe étant incapable de payer ces savants, beaucoup d'entre eux se seraient exilés aux USA, en fournissant en contrepartie de la matière grise d'une valeur inestimable pour la NSA.

Aujourd'hui, la sécurité d'un pays repose en grande partie sur sa capacité à protéger ses données sensibles, par des moyens de cryptage. Les États-Unis l'ont bien compris, et travaillent pour cela sans relâche avec les mathématiciens de l'agence pour sécuriser ces informations, ces réseaux. Mais par la même occasion, l'agence joue le rôle de casseur de code, afin de mieux percer les secrets des pays

Conclusion

J'espère à travers cette présentation avoir pu vous montrer, ou plutôt vous donner un aperçu du fonctionnement de cette agence tentaculaire. La majorité des gens se disent probablement qu'ils ne sont pas vraiment concernés par ce genre de chose parce qu'ils n'ont rien à se reprocher de toute façon. Et surtout parce qu'une personne prise individuellement ne peut de toute façon rien y faire.

Eh bien moi je soutiens le contraire, nous sommes tous concernés. Les États-Unis qui se veulent être un pays ami de l'Europe joue le double jeu. Comme précisé en introduction, c'est le pays le plus puissant du monde aussi bien en terme stratégique qu'économique. Et le renseignement n'y est pas pour rien.

Le renseignement stratégique (militaire) à mon sens est bien entendu nécessaire et indispensable afin de préserver la sécurité d'un pays, mais sur le terrain économique c'est une autre histoire.

Il ne faut pas se leurrer, les 500 plus grandes entreprises françaises font sûrement partie des écoutes de la NSA, tout comme certains décideurs politiques du pays. D'ailleurs, ce n'est pas pour rien que l'ambassade des États-Unis à Paris se trouve si proche de l'Élysée. Les enjeux économiques suite à la globalisation des échanges sont tellement élevés qu'il devient difficile de résister à la tentation d'utiliser ce système à son propre avantage.

On dit que 90 % des informations sont disponibles au grand public si on sait chercher, 5 % le sont à un public restreint, les 5 % restantes étant secrètes. L'art du système Echelon c'est simplement de pouvoir récupérer 99 % des informations afin de les rendre cohérentes et de les utiliser à l'avantage des États-Unis.

Le 2e point, c'est la vie privée.

Prenons un exemple paranoïaque mais sûrement pas si surréaliste que ça. Cette page parle de la NSA. L'agence va finir par s'en rendre compte, et vérifiera sûrement qui se connecte sur cette page, et surtout saura qui en est l'auteur.

Peut être qu'une enquête rapide sera menée sur moi afin de mieux me cerner. Toute ma famille vivant à l'étranger, peut être que mes conversations téléphoniques seront enregistrées, mes mails interceptés.

Inquiétant non ? Alors il est temps de réfléchir afin de leur compliquer la tâche. C'est bien connu, on ne peut vaincre son ennemi qu'en apprenant à le connaître.

Perspectives

Aujourd'hui, la France n'a pas les moyens financiers pour créer ce genre de système. L'Europe pourrait le faire mais cela ne risque pas d'arriver tant qu'une véritable union ne sera pas mise en place.

Mais il y a des démarches encourageantes :

— Il a été décidé il y a peu de temps au niveau européen, de créer un système GPS concurrent à celui des Américains, qui le voient d'un mauvais œil d'ailleurs. Concrètement, qu'est ce que cela signifie ? Que nous aurons enfin accès à un système de positionnement précis de qualité militaire. En effet, pour avoir une précision de l'ordre du mètre, avec le GPS, il faut demander l'autorisation au Département de la Défense Américaine, sinon la précision accessible au public est de l'ordre d'une cinquantaine de mètres, ce qui est largement insuffisant pour l'armée. On imagine mal en effet l'armée Française effectuer ce genre de demande aux américains !

— La France, via le SCSSI[123] (organisme sous la tutelle du Premier Ministre) autorise le cryptage à 128 bits depuis la mi-mars 1999. C'est mieux que les 40 bits précédemment autorisés. Mais c'est loin des possibilités de cryptage pouvant aller jusqu'à 4096 bits. De toute manière, il ne faut pas se faire d'illusions : si l'État autorise ce genre de cryptage, c'est parce qu'il a les moyens matériels de casser la clé dans un laps de temps suffisamment rapide. Mais cela donne au moins le mérite de compliquer un peu plus les écoutes de nos « amis » de la NSA.

En tout cas, il apparaît clairement que la situation n'évoluera pas beaucoup dans les années à venir côté européen. Mais côté Américains, leur but est clair : rentrer de plein pieds dans le XXI^{e} siècle en maîtrisant les hautes technologies afin de mieux dominer aussi bien stratégiquement qu'économiquement la planète.

[123] SCSSI : Service Centrale de la Sécurité des Systèmes d'Informations. C'est un centre de formation des spécialistes de sécurité, qui a le rôle de conseiller en sécurité pour toutes les administrations françaises.

Le pacte UKUSA

Genèse

L'initiative visant à la création d'une alliance SIGINT fut prise par les Américains, en août 1940, lors d'une rencontre entre Américains et Britanniques, à Londres. En février 1941, les crypto-analystes américains envoyèrent en Grande-Bretagne une machine à décoder (PURPLE[124]). La coopération en matière de crypto-analyse débuta au printemps 1941.

La coopération entre services de renseignements fut renforcée par l'engagement commun des flottes dans l'Atlantique Nord, à l'été 1941.

En juin 1941, les Britanniques réussirent à casser ENIGMA, le code de la marine allemande. L'entrée en guerre de l'Amérique renforça encore la coopération SIGINT. En 1942, des cryptologues américains de la « naval SIGINT agency » commencèrent à travailler au Royaume-Uni.

La communication entre les « U-Boot Tracking-Rooms » de Londres, de Washington, puis, à partir de 1943, de Ottawa (Canada) devint à ce point étroite que, selon les participants, elles travaillaient comme une organisation unique.

L'accord BRUSA-SIGINT

Le printemps 1943 vit la signature de l'accord BRUSA-SIGINT ainsi qu'un échange de personnel. Le contenu de l'accord, qui concerne notamment le partage du travail, est résumé dans les trois premiers paragraphes : échange de toute information provenant de la découverte, de l'identification et de l'écoute de signaux, ainsi que des algorithmes des codes et clés de cryptage. Les Américains étaient compétents pour le Japon ; les Britanniques pour l'Allemagne et l'Italie.

Après la guerre, c'est surtout la Grande-Bretagne qui préconisa le maintien d'une alliance SIGINT. Les bases en furent convenues lors d'une tournée mondiale effectuée, au printemps 1945, par des agents de renseignement britanniques (parmi lesquels Sir Harry Hinsley). Un des objectifs était d'envoyer du personnel SIGINT d'Europe dans le Pacifique, dans le cadre de la guerre contre le Japon.

Dans ce contexte, il fut convenu avec l'Australie de mettre des ressources et du personnel (britannique) à la disposition des services australiens. Le voyage de retour, via la Nouvelle-Zélande et le Canada, conduisait aux États-Unis.

Le pacte UKUSA

En septembre 1945, Truman signa un mémorandum top secret qui constituait la clef de voûte d'une alliance SIGINT en temps de paix. Puis Britanniques et Américains ouvrirent des négociations en vue de la conclusion d'un accord. De plus, une délégation britannique prit contact avec les Canadiens et les Australiens, pour discuter d'une participation éventuelle.

En février et mars 1946, une conférence SIGINT anglo-américaine se tint dans le plus grand secret, pour discuter des détails. Les Britanniques étaient mandatés par les Canadiens et les Australiens. La conférence produisit un accord de quelque 25 pages, toujours classifié, qui arrêtait les détails d'un accord SIGINT entre les États-Unis et le Commonwealth britannique.

D'autres négociations eurent lieu au cours des deux années suivantes, de sorte que le texte final de l'accord dit UKUSA put être signé en juin 1948.

Pays contractants

L'alliance UKUSA a été établie par un accord secret de 1947, qui regroupait les structures anglaise et américaine, ainsi que leur personnel et leurs stations. À cet accord de base furent bientôt ajoutés les

[124] Machine utilisée par les Japonais pour coder leurs messages.

réseaux de trois pays du Commonwealth, le Canada, l'Australie et la Nouvelle Zélande. Les organisations ainsi rassemblées sont :

le GCHQ anglais, localisé à Cheltenham, en Grande-Bretagne,

le Defense Signal Directorate (DSD) australien,

le Communication Security Establishment (CSE) du Canada, à Ottawa, et l'organisme néo-zélandais,

le Government Communications Security Bureau (GCSB) à Wellington.

L'accord UKUSA répartit les équipements, les tâches et les résultats entre les gouvernements signataires.

Plus tard, d'autres pays dont la Norvège, le Danemark, l'Allemagne et la Turquie signèrent les accords SIGINT secrets avec les États-Unis et devinrent des participants « tiers » dans le réseau UKUSA.

Modalités

Par l'accord UKUSA, les cinq signataires prenaient la responsabilité de superviser la surveillance en différentes parties du globe. La zone britannique comprenait l'Afrique et l'Europe, jusqu'à la chaîne de l'Oural ; le Canada prenait en charge les latitudes nordiques et les régions polaires ; l'Australie couvrait l'Océanie. L'accord définit les procédures, les cibles, le matériel et les méthodes de chaque agence.

Les stations des alliés UKUSA forment un seul réseau intégré. Chacun répond à un identifiant unique indiquant sa nationalité d'origine et la technologie à l'œuvre pour chaque site. De plus, chaque pays emploie des officiels gradés comme agents de liaison dans les quartiers généraux des autres membres.

Les stations d'interception sont gérées officiellement par des militaires, qui assurent au moins pour partie ces interceptions. Ainsi, dans les stations gérées par les États-Unis, par exemple, c'est le *Naval Security Group* (ou NAVSECGRU) ou l'*Air Intelligence Agency* (ou AIA) ou encore le United States Army Intelligence and Security Command (ou INSCOM) qui assurent avec la NSA le fonctionnement des stations.

Dans les stations britanniques, il s'agit de la *Royal Air Force* en collaboration avec le service de renseignement britannique (GCHQ).

Ces dispositions garantissent un contrôle militaire strict des installations tout en permettant d'en camoufler les activités.

Fuites et dissensions

Jusqu'en 1995, aucun des gouvernements signataires ne reconnut publiquement la collaboration SIGINT internationale. Cette année-là, le gouvernement canadien affirma collaborer avec « *certains de ses plus proches et plus anciens alliés pour l'échange de renseignements extérieurs...* ». En mars 1999, le gouvernement australien brisa le rang pour affirmer spécifiquement et publiquement que le DSD « *coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre-mer sous l'égide de l'alliance UKUSA* ».

Plus globalement, les changements de gouvernement en Australie et en Nouvelle-Zélande à la fin des années 90 ont amené une modification des attitudes de ces deux pays à l'égard du pacte UKUSA. Il n'est pas sans signification de rappeler que, parmi les premiers à évoquer le réseau Échelon figurent des journalistes ou des hommes politiques de ces deux pays. Ce sont les confidences ou les auditions d'anciens membres des services de renseignement qui ont permis à ces journalistes de mieux comprendre comment fonctionnait le réseau et quelles étaient les cibles des écoutes.

Certes, les tensions entre partenaires sont concevables en raison, non seulement des différences dans les capacités, voire de la disproportion de leurs capacités, mais du fait du rôle de la NSA qui centralise l'ensemble des données collectées et les redistribue, donc les filtrent.

Le cas du Royaume-Uni reste cependant à part dans la mesure où seul ce pays dispose des capacités qui lui permettent d'analyser les documents et d'instaurer avec les États-Unis des relations « moins inégales » qu'avec les autres membres du pacte.

Les cibles

Dans les années 90, prétextant de nouvelles priorités comme le terrorisme, le trafic de drogue et la prolifération des armes, le pacte UKUSA prit le parti d'étendre la surveillance aux principales artères de communication du monde.

Ainsi, on affirme qu'Échelon, depuis à tous le moins la fin de la guerre froide, ne poursuit plus l'objectif qui était le sien au départ, à savoir la défense contre l'Est, et est désormais un instrument d'espionnage économique.

Dans le rapport commandé par le STOA, Campbell étaie cette thèse par de nombreux exemples ; ainsi, Airbus et Thomson CFS auraient subi des préjudices à cause de l'espionnage économique.

L'espionnage économique

L'orientation des services de renseignement des États-Unis vers un soutien direct à la politique commerciale de leur pays n'est pas nouvelle.

L'administration américaine sous la présidence de Bill Clinton a clairement exprimé le choix d'une intervention croissante de l'exécutif et des services gouvernementaux en faveur du secteur industriel. La création du National Council of Economy répond au même objectif de défense des intérêts économiques des États-Unis par tous les moyens.

Depuis quelques années, le gouvernement américain a reconnu une capacité d'interception des télécommunications à partir d'un système militaire d'écoutes qui s'est diversifié. L'élément nouveau est qu'à la suite du premier rapport au Parlement européen de son service d'études (STOA) en 1998, certains responsables officiels américains ont fait de multiples déclarations pour justifier le réseau Échelon en avançant deux raisons majeures : le développement de pratiques commerciales déloyales de la part des Européens et notamment des Français (argument économique de moralité) et l'existence de capacités similaires d'interception dans d'autres pays européens, en particulier en Allemagne et en France.

Les présentations de M. Michael V. Hayden, directeur de la NSA, ou de M. George J. Tenet, directeur de la CIA, devant les membres du Congrès, et en particulier leurs auditions à plusieurs reprises devant les deux commissions spéciales en charge du renseignement à la Chambre des représentants et au Sénat, s'appuient souvent sur l'énoncé de grands principes moralisateurs :

— d'une part, les deux responsables des agences fédérales ont toujours soutenu que les activités des services de renseignement étaient compatibles avec les « lois des États-Unis et les droits fondamentaux des citoyens américains ». Ils ont ainsi affirmé qu'aucune conversation privée de citoyens américains ne faisait l'objet d'écoutes. Ils ont rappelé que l'activité des services de renseignement était strictement encadrée par des mécanismes législatifs et réglementaires, dont l'Executive order nº 12-333, que ces activités devaient être approuvées par l'Attorney General, que les agents des services de renseignement étaient tenus de dénoncer les violations qu'ils pouvaient constater, et que les Inspecteurs généraux des services de renseignement (CIA, DIA, FBI ou NSA) faisaient rapport au Président des États-Unis des activités qu'ils estimaient illégales ;

— d'autre part, trois objectifs semblent avoir été fixés aux services de renseignement américains : surveiller les entreprises qui rompent les embargos décidés par l'ONU ou les États-Unis, suivre les technologies duales pour éviter leur utilisation dans la production d'armes de destruction massive, moraliser le commerce international et éviter ainsi que les entreprises américaines ne soient pénalisées par les comportements délictueux de leurs concurrents.

Les affirmations des responsables des agences fédérales doivent être relativisées au regard des considérations suivantes : plusieurs exceptions permettent aux agences fédérales américaines d'écouter les conversations privées, notamment le soupçon qu'une personne travaille pour un « pouvoir étranger », l'existence d'un mandat d'une cour de justice ou le fait que les communications se déroulent en dehors du territoire américain (overseas). En outre, les autorités fédérales auraient la possibilité de conserver des conversations au-delà du délai légal de 24 heures en dehors du territoire américain, donc de les exploiter même lorsqu'elles ont été réalisées par des citoyens américains ; des structures de coordination existent pour favoriser les échanges entre le secteur privé et les administrations américaines. Ces échanges ont bénéficié depuis quelques années d'un transfert mutuel de personnels. La CIA a embauché de plus en plus de jeunes disposant déjà d'une première expérience professionnelle dans le secteur privé. La NSA et la CIA ont encouragé la reconversion d'une partie de leur personnel vers le secteur privé. Les responsables des services informatiques et de sécurité des entreprises sont souvent d'anciens employés des agences fédérales ; les méthodes mises en œuvre pour contrôler certaines activités sont similaires à celles visant l'espionnage économique.

Comme le reconnaissent plusieurs membres du Congrès, il est quasiment impossible de séparer ces activités. Le directeur de la CIA affirme que l'agence intervient lorsqu'une entreprise américaine pourrait être « lésée » dans ses intérêts par un concurrent ne se conformant pas à des pratiques loyales. Les informations sont transmises aux ministères intéressés (Treasury Department, Commerce Department, Justice Department,...) qui peuvent alors décider d'avertir ou non l'entreprise concernée.

Les propos tenus par les actuels dirigeants des agences fédérales en charge du renseignement rejoignent ceux de M. R. James Woolsey, ancien directeur de la CIA. Dans deux articles, aux tons d'ailleurs assez divergents, mais empreints d'ironie et provocateurs, il a reconnu que des écoutes avaient été effectuées aux dépends d'entreprises européennes.

Il les a justifiées au nom de la lutte contre la corruption et de la croisade contre le versement de « pots-de-vin » par les groupes européens à des gouvernements tiers.

Lors de son audition, M. R. James Woolsey s'est tout d'abord défendu d'avoir affirmé que les États-Unis faisaient actuellement de l'espionnage économique aux dépens de sociétés étrangères. Il a affirmé que le titre du *Wall Street Journal* employant le présent (« *Why we spy our Allies ?* ») était dû aux journalistes et non à lui-même. Il a par contre admis que, lorsqu'il était directeur de la CIA, certaines écoutes concernaient des entreprises soupçonnées de verser des pots-de-vin.

Il a rappelé que 95 % des informations provenaient des ressources ouvertes et seulement 5 % des sources secrètes sur des sujets déterminés.

Aux États-Unis, la communauté du renseignement a toujours fait du renseignement économique pour trois raisons : suivi des biens à double usage, respect des sanctions économiques, utilisation de méthodes frauduleuses de la part d'entreprises ou de gouvernements étrangers.

Il n'a jamais été question de recueillir des secrets technologiques au profit d'entreprises américaines.

M. R. James Woolsey a également indiqué que lorsqu'il était directeur de la CIA, des sénateurs l'avaient interrogé pour savoir s'il était prêt à engager l'agence vers l'espionnage industriel. Certains journalistes ont interprété sa réponse comme un soutien aux entreprises américaines. Mais plusieurs analystes ont conclu que jamais le gouvernement américain n'autoriserait la participation d'une agence fédérale à de telles activités. De plus, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises. Il est ainsi quelquefois impossible de savoir si on s'adresse à une société étrangère ou américaine. Aussi laquelle faudrait-il aider ?

Si la presse américaine avait pu relever des cas où les agences fédérales ont favorisé les entreprises américaines, elle aurait été ravie de dénoncer leur hypocrisie. La transparence du système serait telle qu'il est impossible que des détournements n'aient pas été connus. De plus, l'espionnage ne correspond pas à l'objectif primordial de sécurité et risquerait de détourner les capacités d'enjeux plus importants.

Le détournement à des fins économiques place d'ailleurs les autres pays dans des situations difficiles, notamment le Royaume-Uni. Les intérêts des États-Unis et du Royaume-Uni peuvent diverger, par exemple en matière de marchés d'équipements militaires ou d'aéronautique civile. Or le Royaume-Uni participe à des interceptions dont les résultats peuvent être quelquefois utilisés contre les intérêts mêmes de ses entreprises nationales ou de sa politique extérieure. Le cas du marché perdu par le consortium Airbus est révélateur puisque le groupe British Aerospace détient 20 % de ce consortium.

De même, la présence du Royaume-Uni dans le système est encore plus préoccupante pour toutes les affaires relevant de l'Union européenne s'il s'avère que l'Union est « piégée » lors des négociations internationales ou dans les sommets concourant à la réforme des institutions communautaires ou encore au développement de la politique européenne de sécurité et de défense.

Des ONG surveillées

Les organisations non gouvernementales, comme la Croix-Rouge, font partie des nouvelles cibles potentielles de la surveillance électronique américaine de la NSA, d'après le quotidien danois *Ekstra Bladet*. Cela confirme une enquête du *Sunday Times* (février 2000) affirmant que des ONG comme Amnesty International et Greenpeace ainsi que des personnalités comme Mère Teresa et Lady Diana ont déjà été dans le collimateur d'Echelon !

Une série de documents des services secrets de l'armée de l'air américaine évoque les nouvelles menaces susceptibles de faire l'objet d'attentions particulières. Des diapos, présentées lors d'un briefing en 1999, montrent une liste de terroristes internationaux puis apparaissent le nom d'ONG comme la Croix-Rouge, à côté de la mention « ami ou ennemi ? » Ces documents émaneraient du « 544th Intelligence Group », division de l'US Air Force Intelligence Agency Division qui fait partie des maillons du réseau Echelon, selon les preuves déjà obtenues par des spécialistes américains.

« Les ONG opérant à l'étranger sont souvent surveillées pour les liens » qu'elles entretiennent avec des régimes controversés », écrivait le Sunday Times le 27 février, dans un article cosigné par le spécialiste Duncan Campbell. Il révélait d'autres noms ayant déjà fait les frais d'interceptions clandestines d'Echelon : Amnesty International, Greenpeace et Christian Aid, une ONG très connue dans le Commonwealth.

Les bases britanniques d'Echelon ont participé à ces opérations. La princesse Diana était aussi en ligne de mire tout comme Mère Térésa pour leur engagement dans la campagne contre les mines antipersonnel (les États-Unis refusent toujours de signer le traité d'interdiction).

Les communications du Vatican, dont la diplomatie parallèle est toujours très active, ont aussi été écoutées pour le compte du gouvernement britannique. Mark Thatcher, fils de l'ancienne Dame de fer, a lui été surveillé pour son action dans des ventes d'armes en Arabie Saoudite dans les années 80, toujours d'après le *Sunday Times*.

Margaret Thatcher aurait par ailleurs utilisé l'aide du Canada, l'un des cinq alliés officiels d'Echelon, pour espionner deux membres de son propre gouvernement.

Des actions internationales

Le cas du Kurdistan est intéressant. D'un côté, la CIA soutient à coups de millions de dollars les Kurdes opposés à Saddam Hussein ; de l'autre, elle renseigne les Turcs sur les allées et venues de leur ennemi juré, Abdullah Öcalan, leader du Parti des Travailleurs du Kurdistan, dont tous les déplacements sont surveillés par la gigantesque centrale d'écoute, la NSA.

C'est ainsi que les services d'Ankara ont pu arrêter au Kenya le chef kurde honni ; en échange de ces précieuses informations, le pouvoir turc a accepté d'intensifier sa collaboration avec les agences de renseignement américaines...

Les affaires

Les éléments relatés ci-dessus sont globalement de deux types. D'un côté des actions militaro diplomatiques, répondant à la mission américaine de défense du monde libre. De l'autre des actions économico financières justifiées par le mauvais comportement des concurrents américains. Les « révélations » tiennent ainsi plus de l'opération de marketing que du scoop !

Ainsi, les épisodes les plus intéressants sont en fait ceux pour lesquels nous avons le moins de détails, car ils relèvent quant à eux réellement de l'espionnage pur et simple.

Notons que, selon les Américains, la communauté du renseignement a toujours fait du renseignement économique pour trois raisons : suivi des biens à double usage, respect des sanctions économiques et utilisation de méthodes frauduleuses de la part d'entreprises ou de gouvernements étrangers. Il n'a jamais été question de recueillir des secrets technologiques au profit d'entreprises américaines.

Pour résumé, à Washington, on répète qu'il n'est pas question d'espionner pour Chrysler ou Exxon, que cela nuirait à la libre concurrence. Mais on ajoute que les services secrets peuvent aider les compagnies américaines dans un cas : pour dénoncer les pots-de-vin qui permettent à des firmes étrangères d'obtenir des gros contrats aux dépens de firmes américaines.

1950-60 : Opération Shamrock

Durant les années 50, les compagnies de télégraphe américaines, la Western Union en particulier, remettaient tous les soirs à un officier de l'agence une copie de l'ensemble du trafic qui entrait aux États-Unis ou en sortait.

Cette activité a resta complètement inconnue pendant 30 ans, jusqu'à ce que des enquêtes soient diligentées autour de l'affaire du Watergate.

Le 8 août 1975, le directeur de la NSA, le Lieutenant Général Lew Allen admet au « Pike Committes » que « la NSA intercepte systématiquement toutes les communications internationales, qu'elles soient aériennes ou par le câble »

Légalement, les législateurs américains considèrent de telles opérations comme étant anticonstitutionnelles. En 1976, le département de la Justice se livre à une étude sur les possibles « criminal offences » de la NSA.

Mais, selon un proche de la NSA, « le patriotisme et l'intérêt bien compris font céder n'importe quelle entreprise sollicitée par la NSA », explique un ancien de la maison. C'est pourquoi je suis sûr que le nouveau réseau mondial de téléphonie mobile, Iridium, [NDLR ayant fait faillite depuis] qui permet de téléphoner de n'importe où, est déjà sous la coupe de la NSA. Pourquoi ? Parce que les deux promoteurs principaux de l'entreprise sont de très importants fournisseurs de l'agence, qui, je vous le rappelle, dispose d'un budget d'au moins 50 milliards de francs...

1986 : Berlin-Ouest

En 1986, deux soldats américains étaient tués dans l'explosion d'une discothèque à Berlin-Ouest. L'attentat n'a pas été revendiqué.

Pourtant, l'État commanditaire, la Libye, a été immédiatement identifié par les États-Unis : la NSA avait intercepté et décrypté les communications entre les ambassades de Tripoli à Berlin-Est et Rome.

En effet, quelques minutes après l'explosion, un membre des services secrets de Kadhafi disait : « L'opération a bien eu lieu. Elle n'a pas laissé de traces. »

Quelques jours après, Reagan autorisait le bombardement de la capitale libyenne.

1990 : Koweït

En juillet 1990, les satellites Keyhole ont vu le déploiement des troupes irakiennes à la frontière du Koweït. Le 27, six jours avant l'invasion, les capteurs infrarouges ont même repéré les camions militaires transportant de l'eau, du gasoil et des munitions.

1991 : Ex-URSS

Le lundi 19 août 1991, à Moscou, ulcérés par la décomposition de l'empire soviétique, les chefs du KGB et de l'Armée rouge prennent le pouvoir au Kremlin. Ils prétendent que Mikhaïl Gorbatchev est soudainement tombé « malade », qu'il est « incapable » de diriger le pays et qu'il se repose dans sa datcha en Crimée. George Bush fait une première déclaration ambiguë, dans laquelle il ne condamne pas les putschistes. Le directeur de la CIA vient de lui montrer les photos du satellite-espion qui suit tous les faits et gestes de Gorbatchev : ce dernier est en réalité prisonnier dans sa maison, il lui est impossible de rentrer à Moscou. Le nouveau pouvoir va peut-être réussir à s'installer. Bush veut ménager l'avenir.

Quelques heures plus tard, le ton change radicalement : Bush dénonce violemment le pronunciamiento et refuse de reconnaître les usurpateurs du Kremlin.

Entre les deux déclarations, la NSA lui a fait parvenir un nouveau rapport : elle a intercepté et décodé toutes les discussions téléphoniques entre les chefs rebelles. Ils y apparaissent divisés, peu sûrs d'eux. Plus grave : les commandants régionaux de l'armée soviétique ne les suivent pas, la plupart refusent même de répondre à leurs appels téléphoniques.

Avant tout le monde, Bush sait donc que le coup d'État ne réussira probablement pas.

1992-98 : Lopez

La NSA découvre la trahison d'un dirigeant de General Motors, Lopez, qui a vendu à Volkswagen d'importants secrets commerciaux. Comment ? Un ancien de l'agence explique : « La NSA suit avec beaucoup d'attention tous les mouvements de fonds dans les banques suisses. Un jour, elle a découvert que ce Lopez cherchait à placer une fortune. Rien de plus simple, alors, que de remonter au généreux donateur, Volkswagen. »

La NSA a ainsi intercepté, par le biais de la station de Bad Aibling une vidéo conférence entre le directeur de VW, F. Piëch et Lopez. Les éléments de celle-ci sont transmis à General Motors et à Opel. Les charges sont suffisantes pour que le ministère public ouvre une enquête.

L'enquête révèle que Lopez et trois de ces collaborateurs transmirent des documents et des données des secteurs de la recherche, de la planification, de la fabrication et des achats (concrètement, il s'agit de documents relatifs à une usine en Espagne, d'informations relatives au coût des différents modèles, d'études de projets, de stratégies d'achat et d'économies).

En 1998, l'action en justice est suspendue. Intervient alors un règlement à l'amiable entre les deux groupes. Lopez démissionne de ses fonctions de directeur de VW en 1996 ; il verse 100 millions de $ à GM/Opel (prétendus frais d'avocats) et achète durant 7 ans des pièces de rechange pour un total de 1 milliard de dollars.

1

993 : Négociations du GATT

En 1993, les participants français aux négociations du GATT sont tous espionnés et mis sur écoute.

Jean Guisnel, journaliste au Point et auteur de *Guerres dans le cyberespace*, indique d'ailleurs que la NSA a percé les conversations du gouvernement français à propos du Gatt (General Agreement on Tariffs and Trade).

Les négociateurs, parmi lesquels Alain Juppé, alors ministre des Affaires étrangères, conversaient régulièrement avec leur cabinet parisien depuis des avions militaires Falcon sans que leurs communications soient cryptées…

Ce type d'espionnage est d'ailleurs institutionnalisé : au département du Commerce, existe un l'Office of Executive Support qui fait le lien entre les négociateurs et les agences de renseignement — plusieurs membres de la CIA et de la NSA en font partie.

1993 : Srebrenica

En juillet 1995, les Keyhole[125] ont vu les massacres de Srebrenica, mais la Maison-Blanche n'a pas bougé.

1994-95 : Airbus

Dans le cadre d'un contrat d'achat d'avions de 6 milliards de $ entre Airbus et la compagnie d'Arabie Saoudite, la NSA a intercepté les fax et les communications téléphoniques — transitant par satellites de communications — entre les deux partenaires. Les informations ainsi collectées sont transmises à Boeing et Mc Donell-Douglas. Ce dernier obtient le marché.

Au passage, aurait été mis au jour une manœuvre de corruption d'Airbus (pots de vin à des membres de la commission chargée d'attribuer le marché) qui empêcha le consortium européen de dénoncer ce procédé et/ou qui justifia l'action des Américains au regard du comportement déloyal des Européens.

1994-96 : Enercon

L'ingénieur A. Wobben, de la société Enercon GmbH, met au point une éolienne de haute technologie pour la production d'électricité. La NSA prend connaissance de ses travaux et les transmet à une entreprise américaine, Kenetech, qui s'empresse de déposer les brevets relatifs à cette découverte.

Finalement, Enercon obtiendra justice, mais le mal est fait : ses ambitions de pénétration du marché américain sont à jamais anéanties. Le préjudice s'élève à plusieurs millions de DM.

1994 : Thomson-CSF

En 1994, la NSA a intercepté des appels téléphoniques entre Thomson-CSF et le Brésil pour le projet SIVAM, un système de surveillance de la Forêt Amazonienne de 1,3 milliard d'US$.

Thomson était — bien entendu — soupçonné d'avoir « acheté les membres stratégiques du gouvernement brésilien ». Conclusion, le contrat fut remporté par Raytheon Corporation qui annonça peu de temps après : « *le Département du Commerce Américain a travaillé durement pour soutenir l'industrie US dans ce projet* ». Au passage, la société Raytheon assure la maintenance et l'ingénierie de la station de Sugar Grove.

Pourtant, en novembre 1995, quelque temps après cet épisode, la presse brésilienne publiait des transcriptions d'écoutes téléphoniques, probablement réalisées par la NSA, mettant en cause les tentatives de corruption d'un officiel brésilien par... Raytheon.

Ainsi, la NSA aurait informé la Maison-Blanche du montant des dessous-de-table versés par l'entreprise française à des responsables brésiliens, et Bill Clinton serait personnellement intervenu – selon quelles modalités ? — auprès de Brasília pour retourner la situation.

Signalons tout de même qu'au cours de la seule année 1998, Thomson-CSF et Raytheon se sont alliés pour remporter trois contrats : équipements radio pour la Royal Air Force, sonars pour l'US Navy et radars pour l'armée helvétique. D'ailleurs, un « rapprochement » avec Raytheon est évoqué par le P.D.G. de Thomson-CSF, Denis Ranque, dans un entretien publié dans *Le Monde* du 3 février 2000 ; fin juin, la revue confidentielle *Defense News* s'est montrée plus précise : citant des sources proches de Raytheon, elle évoque la création d'un joint-venture dans les radars hautement stratégiques.

[125] Satellites

De plus, depuis le début de l'année 2000, un certain Lord Roger Norman Freeman, 57 ans, fait partie du conseil d'administration de Thomson-CSF. Et ce, suite au rachat d'une société de défense d'Irlande du Nord qu'il dirigeait, Short Missile Systems. Or la notice biographique de Lord Roger précise qu'il était « ministre Defence procurement du gouvernement britannique entre 1994 et 1995 ». Le fait que ce haut fonctionnaire de Sa Majesté occupait ce poste au moment de l'affaire Sivam reste bien entendu pure coïncidence.

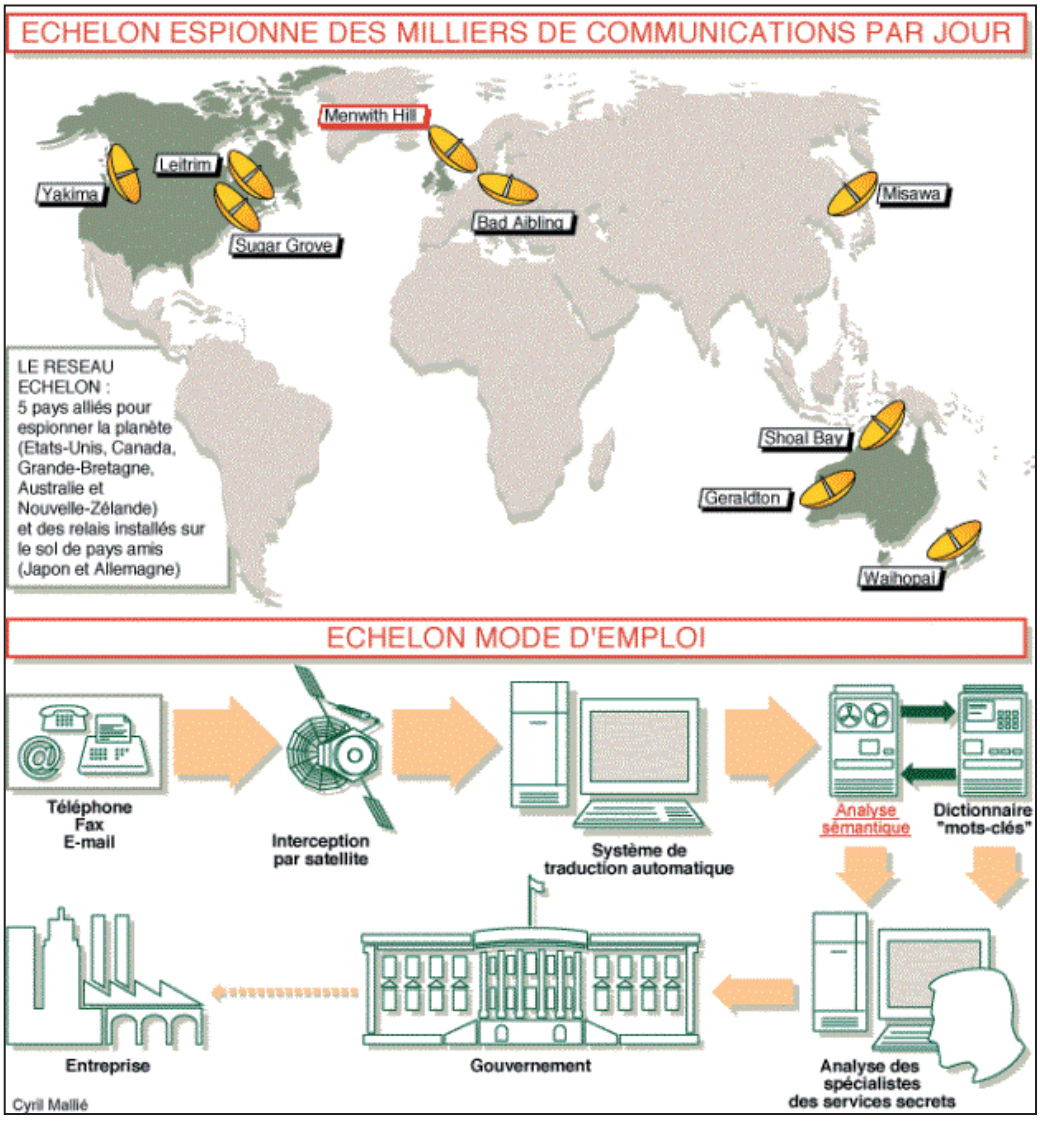
1995 : Voitures de luxe japonaises

Le *Washington Post* a révélé qu'en 1995 l'envoyé de Bill Clinton au Japon, Mickey Kantor, avait bénéficié de l'aide de la NSA lors de discussions très serrées avec Tokyo sur les quotas d'importation de voitures.

L'information portait sur les normes d'émissions des voitures japonaises. La barrière des normes est, rappelons-le, un grand classique des négociations économiques internationales.

Mars 2003 : Résolution de l'ONU contre l'Irak

Selon l'hebdomadaire dominical britannique *The Observer* qui a obtenu un mémorandum en date 31 janvier 2003, la NSA se livre à des interceptions à l'encontre des délégations du Conseil de Sécurité de l'ONU dans le cadre des efforts des États-Unis pour rallier les indécis — Angola, Cameroun, Chili, Mexique, Guinée et Pakistan — avant le vote sur une deuxième résolution concernant l'Irak.



Les technologies

Les Dictionnaires

Ces ordinateurs contiennent les listes de cibles et d'informations liées aux cibles, ce qui permet de sélectionner automatiquement les messages dignes d'intérêt.

Les ordinateurs *Dictionnaire* locaux dans chaque site stockent des bases de données exhaustives sur des cibles spécifiques, avec les noms, les sujets d'intérêt, les adresses, les numéros de téléphone et d'autres critères de sélection.

Les messages entrants sont jugés à l'aune de ces critères ; si un rapport est établi, les renseignements bruts sont automatiquement expédiés dans la suite du processus.

Ces ordinateurs sont assignés à des tâches obéissant à plusieurs milliers d'exigences différentes qu'on appelle « nombres » (codes à quatre chiffres).

Le triage et la sélection effectués par ces ordinateurs peuvent être comparés à l'usage des moteurs de recherche, qui sélectionnent les pages Web par mots ou expressions clefs, et établissent des liens. La fonction d'expédition des *Dictionnaires* peut être comparée au courrier électronique. Quand cela est nécessaire, pour le compte rendu, l'analyse, la condensation ou l'expédition, le système fournira des listes des communications recoupant chacun des critères.

L'ordinateur convertit d'abord les divers types de messages (téléphone, fax et email) en langage numérique standard, puis il active la recherche des mots clés insérés par les *Dictionary Managers* des cinq pays. Tous les messages contenant ces mots sont alors passés automatiquement dans un autre ordinateur qui les code et les expédie via satellite au QG de la NSA, à Fort Meade (Maryland), où ils sont analysés par des techniciens américains.

« Tous les trois ou quatre jours, les responsables de ces "*Dictionnaire*s" dans ces cinq pays changent la liste des mots clés, en insèrent de nouveaux, en retirent d'autres en fonction des thèmes politiques, diplomatiques et économiques qui intéressent à un moment donné les États-Unis et leurs alliés, explique Hager. Une fois les nouveaux mots insérés dans le système, quelques minutes suffisent pour que les *Dictionnaire*s, fassent apparaître les messages qui les contiennent ».

Cela signifie qu'au lendemain de la tragédie de Cavalese [le 3 février 1998, dans les Dolomites, un avion militaire américain coupe le câble d'un funiculaire, causant la mort de vingt personnes ; l'affaire provoquera une polémique sur les bases américaines en Italie], ayant eu connaissance des fortes réactions italiennes et craignant une escalade de la crise, la NSA a très probablement inséré dans le système les mots « Cavalese » et « Cermis » [lieu de l'accident]. « L'Italie et les autres pays européens sont la cible constante d'Echelon, et une demande américaine d'insérer de nouveaux mots clés concernant des questions italiennes aura été accueillie par les techniciens britanniques à Morwenstow sans surprise, comme une opération de routine », précise Hager.

Dans un rapport du 29 mars 1999, *Der Spiegel* indiquait que les termes clés proviennent avant tout du domaine économique américain.

Les antennes

Éléments généraux

Les stations d'interception sont gérées officiellement par des militaires qui prennent en charge l'aspect technique de l'interception. Dans le cas de la NSA, c'est le Naval Security Group (NAVSECGRU) ou l'Air Intelligence Agency (AIA) qui assure le fonctionnement des stations.

Dans les stations britanniques, c'est la RAF qui gère les stations pour le compte du GCHQ. Ces dispositifs garantissent un contrôle militaire strict de l'installation, tout en permettant d'en camoufler les activités.

La forme des antennes donne des indications quant au but poursuivi par l'installation. Ainsi, des rangées d'antennes verticales formant un cercle de grand diamètre (antennes Wullenweber) sont utilisées pour déterminer l'orientation des signaux hertziens.

Une succession circulaire d'antennes rhomboïdales (antennes dites en râteau) sont utilisées dans ce même but. Des antennes de réception multidirectionnelles ou antennes directionnelles, comparables à des antennes de télévision classiques gigantesques servent à intercepter des signaux hertziens non dirigés. Pour la réception des signaux satellitaires, seules sont utilisées les antennes paraboliques. Lorsque celles-ci sont à découvert, il est possible de calculer, en connaissant leur situation, leur angle d'inclinaison (élévation) et leur orientation (azimut) le satellite dont les émissions sont interceptées. Il serait possible de le faire, par exemple, à Morwenstow, à Yakima ou à Sugar Grove.

Antenne Wullenweber à Masawa, Japon.

Ces antennes sont ainsi le plus souvent dissimulées sous des enveloppes sphériques blanches appelées radômes. Ceux-ci servent non seulement à protéger les antennes, mais également à cacher leur orientation.

Les antennes de réception des satellites peuvent être utilisées pour :

1 — recevoir des communications militaires ;

2 — les informations des satellites espions (photos, radars) ;

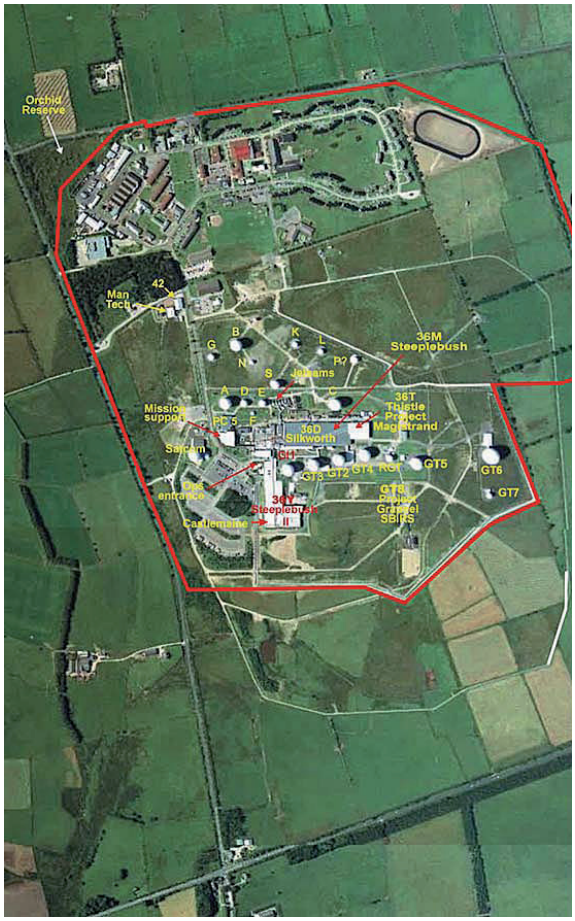
3 — intercepter les communications militaires SIGINT et civiles.

Radômes de la station Menwith-Hill

Il n'est pas possible de déduire les missions des antennes à partir de leur aspect extérieur.

Les stations au sol destinées aux satellites SIGINT ne nécessitent que de petites antennes, ce qui s'explique par les caractéristiques du signal renvoyé à la station (faisceau et fréquence importants). Cela concerne aussi les antennes captant les signaux des satellites d'espionnage

Si une installation présente au moins deux antennes par satellites de plus de 18m, il est certain que l'interception des communications civiles y est pratiquée.



Vue satellite de Menwith-Hill

Modalités chronologiques

Étant donné que les satellites INTELSAT furent les premiers satellites de communication et que, de plus, ils couvraient la terre entière, il est logique que la mise en place et l'agrandissement des stations suivent le développement des générations d'INTELSAT.

C'est en 1965 que le Premier satellite INTELSAT (Early Bird) fut mis en orbite géostationnaire. Il avait une capacité de transmission encore faible et ne couvrait que l'hémisphère Nord. Avec les générations INTELSAT II et III, mise en service respectivement en 1967 et en 1968, on obtint pour la première fois une couverture globale. Pour capter la totalité des communications, il fallait donc trois satellites.

Au début des années 1970, Yakima fut créée dans le nord-est des États-Unis ; en 1972/73, Morwenstow fut créée dans le sud de l'Angleterre. Yakima disposait d'une grande antenne (l'une orientée vers l'Atlantique, l'autre vers l'Océan Indien). La localisation des deux stations permettait de capter la totalité des communications.

Les satellites INTELSAT de la deuxième génération (IV et IVA) furent développés dans les années 70 et mis en orbite géostationnaire (1971 et 1975). Dès lors, deux stations munies de trois antennes satellitaires ne permettaient plus de capter la totalité des communications.

Ainsi, à la fin des années 70, Sugar Grove fut construite dans l'est des États-Unis (elle existait déjà pour écouter les communications russes) ; elle entra en service en 1980.

Vue satellite des antennes de Sugar Grove

À la même époque, une station fut mise en place à Hong-Kong. Dès lors, dans les années 80, les quatre stations — Yakima, Morwenstow, Sugar Grove et Hong-Kong — permettaient l'écoute globale des communications INTELSAT.

Station de Morwenstow

Station de Menwith-Hill

Les satellites

À titre d'exemple, Menwith Hill (ci-dessus) compte environ 22 terminaux pour satellites et est également station réceptrice des satellites de reconnaissance électronique (Magnum, Orion, Vortex, etc.).

Les satellites permettent de réduire et de concentrer les stations au sol.

En mer

Il est également prouvé que la NSA mène des écoutes à partir de navires comme le prouve la destruction « accidentelle » de l'USS Liberty (voir note *supra*) par les Israéliens lors de la guerre des Six Jours ainsi que l'arraisonnement du navire-espion USS Pueblo par la Corée du Nord.

Sous l'eau

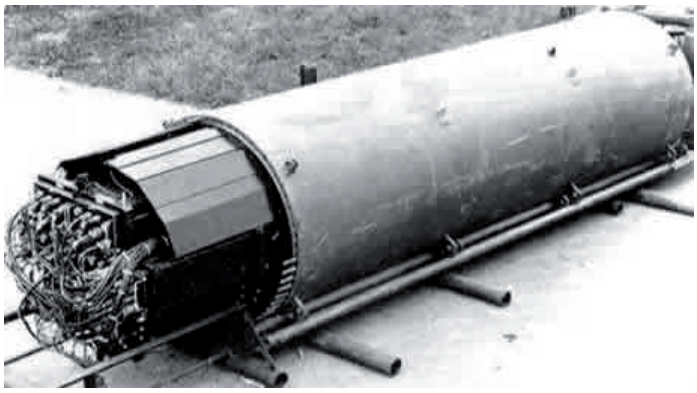
Les câbles étant généralement en fibre optique, l'interception se situe au niveau des répétiteurs qui transforment l'impulsion optique en impulsion électrique afin de redynamiser le signal puis la retransforment en signaux optiques.

C'est lorsque les données se trouvent sous la forme de l'impulsion électrique que se mène l'interception qui est alors similaire à celle d'un téléphone classique.

Les câbles sous-marins jouent maintenant un rôle dominant dans toutes les télécommunications internationales, puisque — contrairement à la largeur de bande disponible et limitée sur les systèmes spatiaux — les médias optiques offrent une capacité apparemment illimitée.[126]

Les câbles sous-marins semblent intrinsèquement plus sécurisés en raison de la nature de l'environnement océanographique.

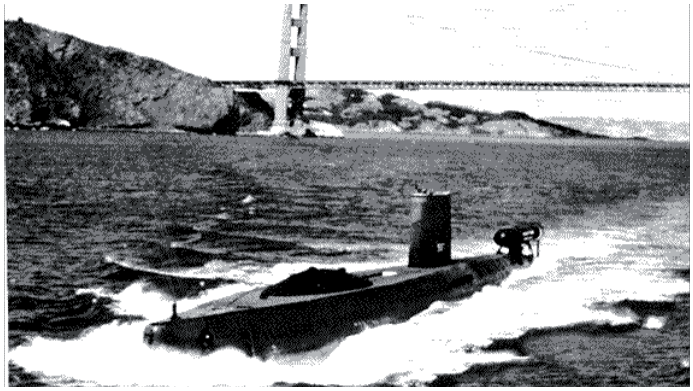
En octobre 1971, il a été démontré que cette sécurité n'existe pas. Un sous-marin Halibut, a visité la mer d'Okhotsk en URSS orientale et a enregistré les communications qui passaient sur un câble militaire vers la péninsule de Khamchatka. L'Halibut était équipé d'une chambre de plongée profonde, totalement visible sur la poupe du sous-marin. La chambre a été décrite par la marine des USA comme « un véhicule de sauvetage sous-marin ». La vérité était que le « véhicule de sauvetage » a été soudé fermement au sous-marin. Une fois immergé, des plongeurs ont quitté le sous-marin et ont enroulé et raccordé les selfs autour du câble. Par la suite, l'Halibut US est retournée en 1972 et a augmenté la capacité du *PoD* d'enregistrement de signaux du câble. La technique n'a impliqué aucun dommage physique et était peu susceptible d'être discernable facilement.



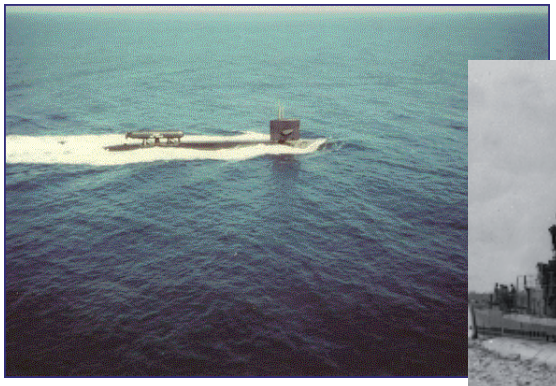
Manchon, ou PoD posé sur câble sous-marin

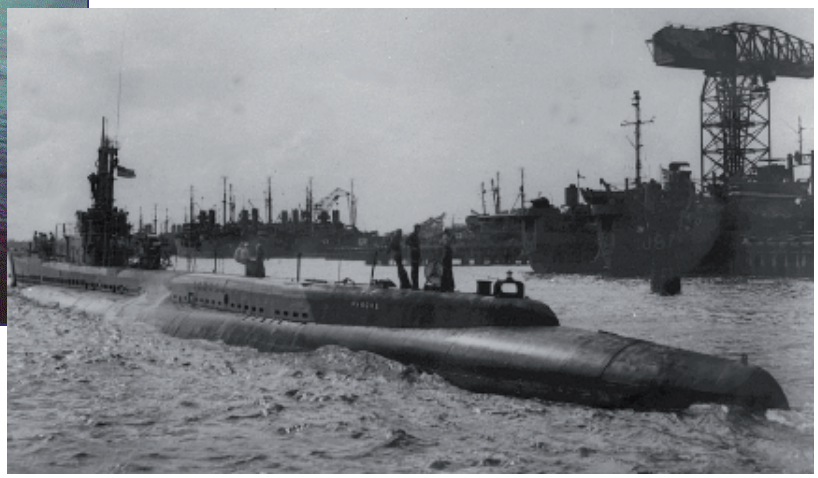
L'opération de raccordement du câble d'Okhotsk a continué pendant dix ans, impliquant des voyages courants pour trois sous-marins différents spécialement équipés pour collecter les anciens PoDs et en placer des neufs, parfois, plus d'un PoD à la fois. De nouvelles cibles ont été rajoutées en 1979. C'est cet été, qu'un submersible nouvellement converti appelé USS Parche a voyagé de San Francisco sous le Pôle Nord à la mer de Barents, et a étendu un nouveau câble de raccordement près de Mourmansk. Son équipage a reçu une citation présidentielle pour cette réalisation.

[126] Les câbles à fibre optique sont conçus pour transmettre les signaux numériques : les 0 et les 1 du code binaire sont codés sous la forme de très brèves impulsions lumineuses, émises par des diodes laser microscopiques. Ils sont constitués d'une, deux ou trois paires de fibres placées dans un bloc optique recouvert d'une armature d'acier, d'une enveloppe de cuivre pour l'alimentation électrique, d'une gaine d'isolation en polyéthylène. Le tout protégé par une à trois armures d'acier, au voisinage des côtes, pour les protéger des ancres ou des chaluts. Le premier câble transatlantique à fibres optiques, le TAT 8, a été posé en 1988, et permet, grâce à une unité de branchement en mer, de relier simultanément la France, l'Angleterre et les USA. Ce câble offre, grâce à des concentrateurs, une capacité de 40 000 voies téléphoniques simultanées. Comme les câbles coaxiaux, les câbles optiques sont équipés de répéteurs (à partir des années 1990, ils sont espacés de plus de 100 Km). Depuis 1995, des régénérateurs « tout optique » compensent l'atténuation du signal dans la fibre, ce qui permet d'augmenter considérablement le nombre des circuits (le TAT 12 posé en 1995 a une capacité de plus de 500 000 voies téléphoniques simultanées).



Sous-marin Halibut





Sous-marin USS Parche. Remarquer le « véhicule de sauvetage »…

Le raccordement du câble d'Okhotsk a été terminé en 1982, après que sa localisation ait été compromise par un ancien employé de NSA qui a vendu des informations sur ce raccordement, nom codé IVY BELLS, pour l'Union Soviétique. Un de ces PoDs IVY BELLS, est maintenant présenté dans le musée de Moscou de l'ex-KGB.

Le raccordement du câble en mer de Barents a continué à fonctionner, tant qu'il n'a pas été détecté, jusqu'à ce que raccordement soit arrêté en 1992.

Durant 1985, les opérations de raccordement sur les câbles ont été étendues en Méditerranéen, pour intercepter les liaisons câblées entre l'Europe et l'Afrique occidentale. Après la fin de la guerre froide, l'USS Parche a été remonté avec une section étendue pour faciliter le matériel de raccordement et les PoDs. Les câbles de raccordement ont pu être étendus par le contrôle à distance en utilisant des drones.

USS Parche continue à être en opération aujourd'hui, mais les cibles précises de ses missions demeurent inconnues. L'Administration Clinton garde évidemment le secret sur ses accomplissements, chaque année de 1994 à 1997, l'équipage du submersible a été fortement recommandé.

Les cibles probables peuvent inclure le Moyen-Orient, la Méditerranée et l'Asie orientale, et l'Amérique du Sud.

Les États-Unis sont la seule puissance navale connue pour avoir déployé une technologie sous-marine à cette fin.

Des enregistreurs inductifs miniaturisés ont été également utilisés pour intercepter les câbles souterrains. Cependant, les signaux radiofréquences ne fuient pas des câbles fibres optiques et ne peuvent pas être captés en utilisant les boucles inductives. La NSA et d'autres agences Comint ont dépensé beaucoup

d'argent en recherche pour se raccorder sur les fibres optiques, visiblement avec peu de succès. Mais les câbles à fibres optiques, même au fond de l'océan, ne sont pas invulnérables. Le principal moyen d'accès est de s'attaquer aux « répéteurs » optoélectroniques qui amplifient les niveaux des signaux sur les longues distances. Il s'ensuit qu'aucun système de câble submersible utilisant des répéteurs optoélectroniques submergés ne peut être considéré à l'abri des activités du renseignement des communications et des interceptions.

Signalons enfin qu'afin de limiter les coûts, il semble logique que des interceptions soient effectuées également à l'extrémité des câbles sous-marins, se trouvant sur les territoires des membres du Pacte UKUSA.

Ainsi, en Europe, l'accès à la communication par câble à l'entrée et à la sortie du territoire n'est possible qu'au Royaume-Uni.

Le partage de l'information

La distribution de l'information au sein du système Echelon s'effectue via un réseau baptisé Platform II. Celui-ci rassemble des moyens de communication protégés qui relient entre elles les bases militaires.

Au début des années 80, la première génération des moyens de communication dévolus à Echelon (Platform) avait permis de relier 52 ordinateurs à travers le monde et d'agréger leur travail. C'est vers cette époque que le réseau aurait élargi son champ d'observation, ne se limitant plus aux seules interceptions.

Ainsi, durant l'Administration Reagan, les services de renseignement anglo-saxons ont rajouté les comptes-rendus des ouvertures de courriers et des visites clandestines des domiciles.

Alliés

L'Allemagne

L'ancien Secrétaire d'État, Eduard Lintner (CSU), en poste au ministère de l'Intérieur de Bonn, a répondu le 30 avril 1998 à une question écrite, posée par le député socialiste Graf, portant sur les activités de la NSA, que le gouvernement fédéral allemand ne savait rien de plus que ce qu'avait dit la presse à ce sujet !

Pourtant, ce pays fait lui aussi partie des nombreux partenaires de la NSA, et accueille à Bad Aibling, depuis 1971, une station d'écoute et d'interception des télécommunications du programme Echelon.

De plus, le BSI (Bundesamt für Sicherhei in der Informationstechnik), chargé de la sécurité des systèmes d'information, travaille en partenariat avec la NSA sur la sécurité du Web, à partir du futur cadre juridique fourni par la Convention du Conseil de l'Europe.

L'héritage de la Guerre Froide

Les milieux informés considèrent qu'il y avait, en RFA, plus de 350 antennes des services spéciaux américains qui avaient des correspondants dans toutes les casernes et dépôts d'armes, les aéroports et les agglomérations. Ils manipulaient des équipements dirigés vers le Pacte de Varsovie.

Mais, les services de la NSA captaient également les faisceaux directionnels de la Poste de RFA qui retransmettaient environ le tiers environ des communications téléphoniques. En effet, elle intervenait directement sur le réseau téléphonique : des journalistes du *Spiegel* ont découvert à Francfort-sur-le-Main (plaque tournante des communications téléphoniques en RFA) l'une de ces stations branchées directement sur le réseau téléphonique.

Régulièrement l'Office Fédéral de Protection de la Constitution et l'Office Fédéral de la Police recevaient communication d'informations sur les « menées terroristes » et les « courants extrémistes » grâce aux informations obtenues par l'interception des communications téléphoniques.

La NSA disposait de neuf stations d'écoute en RFA (le long de la frontière avec la RDA) et à Berlin Ouest. Ceux qui ont pu observer ces stations, par exemple à Bad Aibling en Haute-Bavière, disaient qu'il s'agissait de gigantesques coupoles d'aluminium ou d'un réseau d'antennes de 300 mètres de longueur et d'une hauteur de 100 mètres pour les équipements de la plaine de Lech près de Gablingen, ou, encore, d'une série de pylônes d'acier comme sur la colline du Teufelsberq à Berlin Ouest. A chaque type de structure correspond un type précis de mission.

Bad Aibling

Cette base, occupée par l'US Army depuis 1947, fut annexée par les États-Unis en 1952 avant d'être gérée par la NSA en 1971. Son identifiant est NSA F81.

Bad Aibling vue satellite (Google)

Son effectif s'élève à 750 agents ou militaires américains. Y sont stationnés l'INSCOM (66th IG, 718 IG), qui assure le commandement ; le NAVSECGRU ainsi que divers groupes de l'AIA (402nd IG, 26th IOG). Ses équipements sont essentiellement constitués de 14 antennes paraboliques (d'un diamètre maximum de 18 mètres). Sa mission officielle est de servir de relais de communications radio (type HF et satellites) pour le dépar-

tement américain à la Défense (DoD) et de la Recherche : « *rapid radio relay and secure commo, support to DoD and Unified Commands, medium and longhand commo HF & Satellite, communication phyisics research, test and evaluate commo equipment* »

En fait, il s'agit d'une station terrestre pour satellites SIGINT et pour l'interception des signaux de satellites de télécommunications (notamment russes). Cette station sert principalement à écouter l'Europe centrale et la Méditerranée.

Une antenne découverte de Bad Aibling

En mars 2000, la presse allemande affirme que cette station se consacre à l'espionnage d'entreprises allemandes. Elle aurait cessé sous la pression des autorités fédérales et viserait maintenant la Suisse.

Cette station aurait permis à General Motors d'espionner l'un de ses cadres, Jose Ignacio Lopez, parti chez Volkswagen en 1992 avec des documents secrets dans ses bagages. Lopez fut contraint de démissionner de ses fonctions chez VW, avant de verser 100 millions de $ à GM/Opel (prétendus frais d'avocats) et d'acheter pendant sept ans des pièces de rechange pour un total de 1 milliard de dollars à GM/Opel. Enfin, il a été reconnu coupable par contumace en mai 2000 par un jury fédéral des États-Unis. La NSA avait intercepté une vidéoconférence entre Lopez et le directeur de VW, F. Piëch, qu'elle avait transmise à GM.

La sortie du réseau Échelon ?

La base américaine de Bad Aibling, la seconde installation la plus importante en Europe après Menwith Hill, devrait fermer ses portes le 30 septembre 2002. En effet, le Pentagone a décidé de fermer cette base américaine dans le cadre d'une réorganisation de ses forces en Europe.

La décision de la fermer a été motivée par les avancées technologiques de l'armée américaine. Elle aurait en effet décidé de remplacer ses bases terrestres par des satellites d'espionnage. Cette option a au moins l'avantage d'être moins voyante.

Avec les attentats du 11 septembre 2001 et à la suite d'une décision conjointe germano-américaine, la fermeture est reportée sin die (comme le prouve les images ci-dessus datant de 2006, la base est toujours opérationnelle. NDLR). Un nouveau départ des Américains ?

Il n'y a aucun lien, affirme-t-on à Washington, avec les tensions américano-européennes sur le dossier irakien et la décision de l'administration Bush de réduire ou de réorganiser sa présence militaire à l'étranger, et notamment en Allemagne où 71.000 soldats américains sont déployés.

Même si aucun projet définitif n'a été entériné, la démobilisation d'un certain nombre de soldats américains présents sur son territoire pourrait être envisagée, affirme-t-on au Pentagone. L'administration Bush aurait en fait l'intention de rendre ses troupes plus flexibles, en les faisant tourner régulièrement et en réduisant de façon importante les structures permanentes installées sur le sol allemand. Mais, assurent ces responsables, ces changements n'auront pas de rapport avec les tensions entre Berlin et Washington sur le dossier irakien. Ils refléteront à l'inverse la volonté américaine de réorganiser son armée dans l'objectif de faire face plus efficacement aux menaces du XXI^{e} siècle, comme le terrorisme.

« Onze ans après la fin de la Guerre froide, il y a une école de pensée qui est de revoir le nombre et le type de forces que nous avons déployées dans différents pays, alors que les événements changent de nature », expliquait le 11/02/2003 le porte-parole de la Maison Blanche, Ari Fleischer. Il a ajouté que les États-Unis garderaient cependant comme objectif de maintenir une présence militaire « pour assurer (la sécurité) de nos amis et alliés ».

Le porte-parole du Pentagone Tim Blair a pour sa part indiqué qu'« aucun plan sur le papier » n'avait pour l'instant été élaboré pour des redéploiements en Europe.

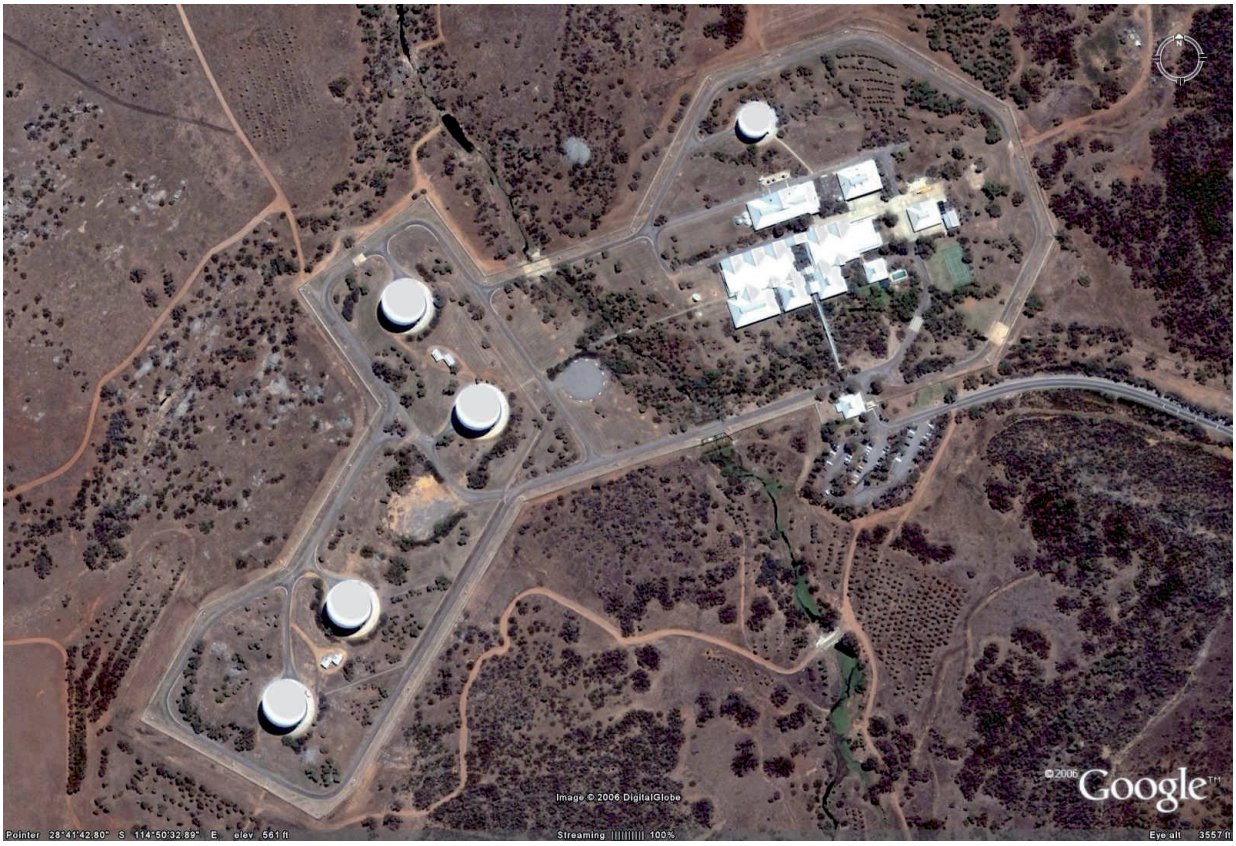
Le 07/02/2003, le secrétaire d'État à la Défense Donald Rumsfeld avait expliqué n'avoir « aucune idée » de la façon dont les troupes américaines en Allemagne allaient évoluer. « Certains (soldats) vont rester, d'autres vont peut-être être déployés dans d'autres pays et d'autres pourraient rentrer aux États-Unis », avait-il simplement dit. « Vous savez, à la fin de la Guerre froide, nos forces avaient pour objectif de nous défendre de l'Union soviétique. Aujourd'hui, les menaces sont quelque peu différentes », ajoutait le chef du Pentagone.

L'Australie

L'Australie est un des pays fondateurs du Pacte UKUSA de 1947. L'agence SIGINT nationale qui gère les interceptions est le DSD, « *Defense Signals Directorate* ».

A l'issue de la réunion des chefs occidentaux de SIGINT du pacte UKUSA, en 1984 à Wellington, fut décidé l'expansion d'Echelon. Ainsi, en 1987, l'Australie, comme la Nouvelle-Zélande, annonça la construction de nouvelles bases de « communications de Défense ». En fait, il s'agissait de bases d'interceptions.

La station de Geraldton



La station existe depuis le début les années 1990. Elle est dirigée par les services secrets australiens (le DSD). Des Britanniques, anciennement stationnés à Hong Kong font également partie du personnel.

Le site australien de Geraldton comprend quatre antennes satellitaires paraboliques d'interception d'un même diamètre (environ 20 m). Elles sont orientées vers des satellites en orbite au-dessus de l'Océan

Indien et vers les satellites en orbite au-dessus du Pacifique. Un ordinateur « *Dictionnaire* » serait également présent à Kojarena, dans l'ancienne base d'interception de Stanley Fort.

Les cibles les plus importantes de cette station sont les messages diplomatiques et commerciaux du Japon, les communications entrant et sortant de la Corée du Nord, ainsi que les informations en matière d'armement nucléaire de l'Inde et du Pakistan.

Plus des trois quarts des messages interceptés sont envoyés automatiquement à des stations éloignées, sans être examinés par le site ou l'Australie.

La station de Shoal Bay

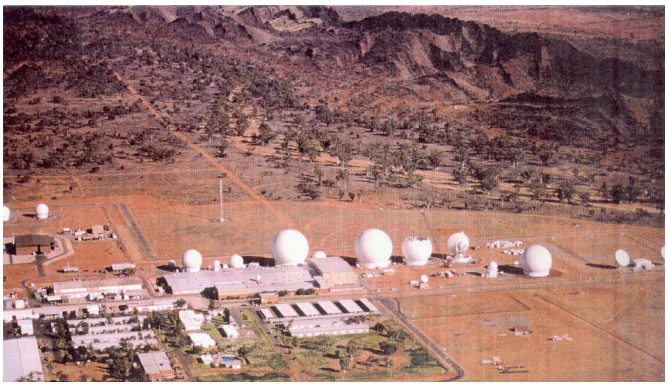
Située dans les Territoires du Nord, cette station a pour cible principale l'Indonésie et ses satellites PALAPA. Des sources australiennes affirment que ce site ne fait pas partie du Réseau Echelon dans la mesure où l'Australie refuse de fournir les fruits bruts de ses interceptions aux États-Unis. De plus, la station n'est desservie que par le service australien de renseignement.

La station compterait dix antennes satellitaires dont les dimensions ne sont pas connues. Les cinq plus grandes ont un diamètre de 8 mètres maximum, la sixième est plus petite.

La station de Pine Gap

En 1968, la CIA établit une station de réception à Pine Gap, près d'Alice Springs, pour recevoir des données des satellites « RHYOLITE », mis en orbite géostationnaire élevée. Ce satellite fut développé entre 1965 et 1985 ; il représente la seconde génération de satellites SIGINT. Par la suite, ils furent rebaptisés AQUACADE.

Elle est dirigée par les services secrets australiens ; à peu près la moitié des quelque 900 personnes qui y sont stationnées sont des Américains de la CIA et du NAVSECGRU.



La station compte 18 antennes satellitaires, dont une d'un diamètre d'environ 30 mètres et une autre de 20 mètres. Depuis ses origines, elle est destinée aux satellites SIGINT : elle commande plusieurs satellites d'espionnage, dont elle capte, traite et analyse les signaux. Toutefois, la présence des grandes antennes satellitaires laisse à penser que la station écoute aussi des satellites de communication, car les satellites SIGINT ne nécessitent pas des antennes satellitaires d'une si grande taille.

Jusqu'en 1980, les Australiens étaient exclus du département d'analyse des signaux. Depuis, ils ont libre accès à toutes les parties de la station, à l'exception de la salle de cryptographie des Américains.

Pour l'anecdote, la salle des ordinateurs y est si vaste que les opérateurs communiquent entre eux par radio.

Révélations

Le 11 mars 1999, Martin Brandy, Directeur du DSD, brise le silence et révèle que son service « coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre-mer sous l'égide de l'alliance UKUSA ». Cette déclaration fut diffusée le 11 avril 1999 dans le « Programme du Dimanche » sur *Channel 9 TV*.

Le Canada

Le Canada est un des pays fondateurs du Pacte UKUSA de 1947. L' agence SIGINT nationale qui gère les interceptions est le « Communication Security Establishment » (CSE), basé à Ottawa.

À l'issue de la réunion des chefs occidentaux de SIGINT du pacte UKUSA, en 1984 à Wellington, fut décidé l'expansion d'Echelon. C'est à partir de cette date que le Canada commença ses opérations d'interception dans l'espace, quand le premier des quatre radômes fut érigé dans sa principale station d'écoute de Leitrim.

La station de Leitrim, Ontario

Letrim en 1941

Letrim en 1999

Située au sud d'Ottawa, dans l'Ontario, Leitrim possède quatre terminaux satellites, érigés depuis 1984. Son nom de code est CAF 97.

Elle fait par ailleurs partie d'un programme d'échanges entre unités militaires canadiennes et américaines. Selon la Navy, quelque trente personnes y sont stationnées.

En 1985, on y installa la première de quatre antennes satellitaires, dont les deux plus grandes ont un diamètre d'environ douze mètres seulement. Officiellement, la mission de la station est le « cryptologic rating » et l'écoute de communications diplomatiques.

Les Forces armées canadiennes ont publié des informations à propos du rôle du personnel de la base de Leitrim, station appartenant à l'agence SIGINT du Canada, le CSE. Aussi sait-on que l'organigramme de l'équipe comprend sept analystes de satellites de communications, des superviseurs et des instructeurs.

Dans un résumé destiné au public, un analyste des satellites de communications anciennement basé à Leitrim raconte que son travail nécessitait des compétences dans : « le fonctionnement de nombreux systèmes informatiques COMSAT et les sous-systèmes correspondants... l'utilisation de systèmes d'analyse assistés par ordinateur... et tout une gamme d'équipements électroniques sophistiqués pour intercepter et étudier les communications étrangères et les transmissions électroniques. »

La base Alerte, à 817 km du Pôle Nord géographique, sur l'île d'Ellesmere, dans le Nunavut.

Perché sur le sommet de l'hémisphère nord, dans le silence du désert arctique, un petit poste militaire canadien espionne en secret les communications d'une bonne moitié du globe, avec pour mission de traquer les terroristes. Avec les antennes, dont est truffée la petite base, on peut couvrir tout le spectre de fréquences.

Les sept techniciens qui travaillent aux « opérations » ont pour tâche d'entretenir les machines. Les informations sont transmises et analysées directement au Leitrim, principale base d'écoute au Canada, située en banlieue d'Ottawa, plus de 4.000 Km au sud.

Les activités d'écoute dans l'Arctique ont commencé dans les années 1950, quand les militaires canadiens et américains se sont intéressés à ce qui n'était qu'un laboratoire scientifique. Pendant la guerre froide, Alert était l'un des postes aux premières lignes de la défense de l'Amérique du Nord : la station était munie de radars pour détecter rapidement toute attaque potentielle de l'Union soviétique.

Si le Canada décide de participer au projet de bouclier antimissile cher au président américain George W. Bush, Alert pourrait reprendre du galon.

Les liens entre le CSE et Echelon

Les rapports des comptes du CSE indiquent qu'en 1995-96, l'agence prévoyait des paiements de sept millions de dollars à Echelon et six millions de dollars à Cray (fabricant quasi exclusif des ordinateurs de décryptage superpuissants de la NSA).

De même, dans son rapport de 1997-98, le Commissaire du CSE dévoile l'interdiction de collecte et de conservation ou de dispersion d'informations relatives à des personnes physiques ou morales d'un autre pays de l'UKUSA : « Le CSE s'engage explicitement à traiter les communications des ressortissants des pays de la partie seconde de l'UKUSA d'une manière conforme aux dispositions prises par l'agence de leur pays, dans la mesure où ces dispositions ne contreviennent pas aux lois du Canada. Il s'agit d'un engagement réciproque qui vise à assurer que les États ne prennent pas pour cible les communications des uns et des autres ou ne circonviennent pas à leur propre législation en prenant pour cible des communications sur l'ordre des uns et des autres. En d'autres termes, qu'ils ne fassent pas indirectement ce qu'il serait illégal pour eux de faire directement ».

La première indiscrétion

Jusqu'en 1995, aucun des gouvernements signataires du Pacte UKUSA ne reconnut publiquement sa collaboration SIGINT.

Cette année-là, pourtant, le gouvernement canadien déclara : « Le Canada collabore avec certains de ses plus proches et plus anciens alliés pour l'échange de renseignements extérieurs (...). Ces pays et les agences responsables dans chacun d'entre eux sont les États-Unis (National Security Agency), le Royaume-Uni (Government Communication Headquarters), l'Australie (Defence Signals Directorate) et la Nouvelle-Zélande (Government Communications Security Branch) ».

Le Danemark

Le ministre de la défense danois a lui aussi avoué (fin 1999) la participation de son pays au projet Echelon, allant jusqu'à identifier le lieu d'implantation des installations sur une île danoise (Skibsbylejren station).

Le ministre, visiblement soucieux de ne pas heurter ses alliés, a affirmé qu'Echelon était en conformité avec les lois danoises. Questionné sur les garanties légales offertes aux citoyens du Danemark quant à l'utilisation du système à leur encontre par un pays tiers, le ministre a répondu : « malheureusement, aucune ».

Skibsbylejren station (Danemark)

Il affirme lui aussi que le projet ne s'appelle pas Echelon.

Le Danemark est semble-t-il, comme d'autres pays, considéré comme un « partenaire secondaire » pouvant bénéficier de certaines informations mais n'ayant pas les mêmes droits que les partenaires principaux tels que le Royaume-Uni ou l'Australie.

Le Royaume-Uni

En dépit des déclarations britanniques de fidélité à la cause européenne, le fait est que ce rapport de collaboration très étroite dans la collecte de *Signal Intelligence* a de très fortes implications politiques, diplomatiques et économiques, et pèse effectivement plus lourd que quelque alliance européenne que ce soit, comme en atteste un document secret, *1994 Strategy Summary*, préparé par sir John Ayde, chef du « *Government Communications Headquarters* », le service britannique qui réceptionne et diffuse le SIGINT : « *Le rapport sur l'UKUSA est pour nous de la plus haute importance,* y lit-on. *Nous devons fournir à nos partenaires une contribution d'une qualité et d'une quantité telles qu'ils puissent en tirer satisfaction. Cela peut vouloir dire qu'il est parfois nécessaire de mettre également les ressources du Royaume-Uni au service des demandes américaines.* »

Pour Londres, les bénéfices de cette extraordinaire alliance d'espionnage sont sans aucun doute énormes. Non seulement le Royaume-Uni peut avoir accès à un système global et omnivore qu'il n'aurait jamais pu créer, gérer et maintenir à jour seul, mais, grâce au pacte UKUSA, il est protégé contre l'espionnage diplomatique, industriel et économique américain dont ses partenaires européens sont la cible : « *Tant que l'accord UKUSA restera en vigueur, aucun des quatre autres pays membres ne pourra penser avoir une politique extérieure véritablement indépendante* », conclut Hager. Il ne faut donc pas s'étonner si, quand Washington attend son soutien (comme dans la crise irakienne), Tony Blair, bien qu'assurant la présidence de l'UE, ne cherche à aucun moment à construire un consensus européen, mais s'aligne immédiatement sur les positions américaines.

Fin 1988, après avoir réfléchi à l'éventualité de créer son propre réseau autonome de satellites-espions, le gouvernement de Margaret Thatcher (qui utilisa ce réseau pour piéger ses ministres) avait pris une décision difficilement réversible en signant un « mémorandum d'entente » ultra secret par lequel le Royaume-Uni s'engageait à intensifier son activité au sein d'UKUSA.

Pour ne pas être trop subordonnée à Washington, Londres s'engageait alors à verser une contribution de 500 millions de livres en échange du droit de réorienter sur une cible concernant ses propres intérêts l'un des trois satellites-espions de la NSA, à raison de quatre mois par an au maximum, les exigences de la NSA ne conservant la priorité qu'en cas de crise.

Le GCHQ

Au niveau organique, le GCHQ dépend du Foreign & Commonwealth Secretary (comme le MI6). Ses missions sont définies par le Ministerial Committee on Intelligence Service (CSI) que préside le Premier ministre. Enfin, les renseignements obtenus remontent vers le Joint Intelligence Comitte (le cabinet du Premier ministre) afin d'y être exploités par la Assesments Staff and Joint Intelligence Secretariat.

Au regard de ses « confrères » du Secret Intelligence Service — MI6 — et du Security Service — MI5 —, il est sans contexte sur un pied d'égalité. D'ailleurs, sa position est comparable à celle de la NSA.

Il dispose aux États-Unis d'un bureau de liaison installé sur la base de la NSA, la Columbia Annex, située au 7200 Riverwood Drive, dans le parc de Rivers Corporate, au sud de Columbia dans le Maryland. La NSA entretient quant à elle une structure identique sur le site Menwith Hill.

On estime ses effectifs à 4 500 agents ce qui en fait le service d'interception le plus important d'Europe.

Par ailleurs, une de ses entités, le Communications Electronics Security Group (CESG) est en charge des demandes de certification des industriels pour leurs logiciels et leurs matériels électroniques ou informatiques. Comme pour les États-Unis, il existe un risque indéniable qu'un tel « amalgame » entraîne ou conduise à l'ajout de backdoors dans les codes sources des logiciels inspectés.

Menwith Hill

Elle a pour mission officielle : « to provide rapid radio relay and to conduct communications research ». (*fournir un relai par radio rapide et conduire la recherche de communications…*)

La plus importante base d'espionnage électronique du monde est la station NSA Field Station F83 de Menwith Hill, dans le Yorkshire

Connue au sein de la NSA sous le nom de code de USD 1000, c'est l'un des quatre centres principaux de gestion et de traitement des données fournies par les satellites Sigint, qui écoutent depuis l'espace.

Sa deuxième fonction, Moonpenny, est d'intercepter les données transmises par les satellites étrangers, qu'ils soient militaires ou civils.

Description

La base de Menwith Hill n'est pas mentionnée sur les cartes de la région. À partir de Leeds, il faut prendre la direction de Harrogate. Arrivé dans cette ville thermale aux allures victoriennes, il ne reste plus que quelques kilomètres à parcourir à travers les paysages verdoyants et vallonnés des landes du Yorkshire du nord. C'est là, au milieu des prés délimités par des murs de pierres sèches que s'est établie la plus grande base d'espionnage du monde. Le site est entouré par une simple clôture grillagée qui semble destinée à arrêter les troupeaux de moutons des alentours plutôt qu'à véritablement protéger le site.

Situation de la base de Menwith Hill (Google Earth)

Sa superficie est de 2,270 kilomètres carrés (560 acres), cette station pourvoit à ses propres besoins d'énergie électrique et est une petite ville en elle-même : elle contient des maisons, des magasins, une église et un centre sportif ! (Voir détails sur Figure 6, plus haut)

La station a été créée en 1956 et, en 1974, elle comptait déjà huit antennes satellitaires. Depuis, on y trouve quelques 30 antennes satellitaires dont plusieurs d'un diamètre supérieur 20 mètres. Au moins une des grandes antennes, mais certainement pas l'ensemble de celles-ci, est une antenne de réception de communications militaires.

En 1980, cette station employait 400 personnes. En 1996, ce nombre a triplé pour devenir 1400 personnes. Ces personnes sont des ingénieurs, des physiciens, des mathématiciens, des linguistes et des ingénieurs informaticiens, plus 370 employés du ministère de la Défense. Au total, la station F83 emploie autant que le MI5 britannique...

Y coopèrent Anglais et Américains. Pour ces derniers sont stationnés le NAVSECGRU, la AIA (avec le 451st IOS) ainsi que l'INSCOM, qui a le commandement de la station. Le site appartient ministère britannique de la Défense et est loué au gouvernement américain.

Vue satellite de Menwith Hill

Elle compte quelque 22 terminaux pour satellites et est également station réceptrice des satellites de reconnaissance électronique. Tel les satellites Magnum, Trumpet (150m de diamètre), Orion (130m) et Vortex (105m). Lors de la catastrophe de Tchernobyl, le satellite Vortex put intercepter toutes les communications locales de la police et de l'armée jusqu'au niveau le plus bas. Ces satellites ont permis de réduire le nombre de stations au sol. Il est à noter que lorsque le nom d'un satellite est rendu public, son nom de code est immédiatement changé (Chalet > Vortex > Mercury)[127].

[127] Chronologie de lancements des satellites « CHALET *alias* Vortex »
10 juin 1978 — CHALET 1 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 3C. La masse : 820 kilogrammes (1.800 livres). Périgée : 29.929 kilomètres (18.596 milles). Apogée : 42.039 kilomètres (26.121 milles). Inclination : 12.00 degrés. Période : 1.446.30 mn. Le premier lancement du plus lourd, des satellites avancés du CHALET ELINT. (le projet a été renommé VORTEX quand le nom de code CHALET est apparu dans le *New York Times*). Longitude mal connue
1er octobre 1979 — CHALET 2 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 3C. La masse : 820 kilogrammes (1.800 livres). Périgée : 30.443 kilomètres (18.916 milles). Apogée : 41.497 kilomètres (25.784 milles). Inclination : 7.50 degrés. Période : 1.445.50 mn.
31 octobre 1981 — CHALET 3 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 3C. La masse : 820 kilogrammes (1.800 livres). Périgée : 134 kilomètres (83 milles). Apogée : 382 kilomètres (237 milles). Inclination : 29.30 degrés. Période : 90.40 mn.
31 janvier 1984 — CHALET 4 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 34D. La masse : 1.043 kilogrammes (2.299 livres). Périgée : 146 kilomètres (90 milles). Apogée : 1.023 kilomètres (635 milles). Inclination : 29.40 degrés. Période : 96.40 mn.
2 septembre 1988 — Etats-Unis 31 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 34D. ÉCHEC : Les lignes cassées d'alimentation de pressurisation de Transtage ont empêché la mise en orbite d'avoir lieu correctement. La masse : 1.045 kilogrammes (2.303 livres). Périgée : 151 kilomètres (93 milles). Apogée : 14.103 kilomètres (8.763 milles). Inclination : 29.30 degrés. Période : 99.80 mn.

La station a reçu une récompense pour le support aux opérations navales des USA dans le Golfe Persique de 1987 à 1988. En 1991, une autre récompense lui a été remise pour son support aux opérations de guerre en Irak (Desert Storm et Desert Shield).

Missions

Au départ, cette station avait pour tâche l'écoute de communications commerciales, principalement, puis dans les années 1980, la station a connu un nouveau bloc d'opération nommé Steeplebush, afin d'étendre ses programmes de surveillance satellite. Le nom de code de cette mission est MOONPENNY.

Au début des années 1990, un autre bloc Steeplebush II a été mis sur pied et actuellement, un troisième bloc, le Steeplebush III est en cours de construction.

C'est maintenant le site principal des USA pour la collecte COMINT contre un allié majeur des États-Unis, Israël. Ainsi, son personnel inclut des linguistes entraînés à l'arabe, l'hébreu, le persan et le farsi.

Menwith Hill a été récemment étendue pour intégrer des liens terrestres pour un nouveau réseau de satellites SIGINT lancés en 1994 et 1995 (RUTLEY). Le nom de la nouvelle classe des satellites demeure inconnu.

Morwenstow

Cette base, en Cornouaille, a été ouverte au début des années 70 avec l'introduction des satellites Intelsat 4 ; elle utilise d'ailleurs la station télécom satellite de Goonhille située à 110 kilomètres... dont elle intercepte les communications.

La station est desservie par le service de renseignement britannique (GCHQ). Elle compte environ 21 antennes satellitaires, dont trois d'un diamètre de 30 mètres.

10 mai 1989 — Etats-Unis 37 — emplacement de lancement : Cap Canaveral. Véhicule de lancement : Titan 34D. La masse : 1.045 kilogrammes (2.303 livres). Périgée : 455 kilomètres (282 milles). Apogée : 40.073 kilomètres (24.900 milles). Inclination : 27.50 degrés. Période : 720.00 mn.

Dès 1971, a commencé la collecte systématique des communications (ILC COMSAT). Sa mission était d'intercepter les communications Intelsat par le biais de deux antennes de 30 mètres : l'une était orientée vers l'Océan Atlantique et l'autre vers l'Océan Indien.

Cette CSOS (« Composite Signals Organisation Station «) a diversifié les interceptions et décodages de téléphones, fax et Internet (d'administrations mais aussi d'entreprises privées), et cible également les satellites régionaux.

En janvier 1998, un document de la BBC (repris par TTU) révélait que les services secrets de Sa Majesté espionnaient les Européens. Un ancien fonctionnaire anonyme de la section K (Europe) du Government communications headquarters (GCHQ), l'agence d'interception des communications a raconté comment son agence espionnait les vieux continents.

Chicksand

En 1964 y fut installé un système de réception AN/FLR-9 (antennes circulaires de 400 mètres de diamètre pouvant simultanément intercepter et déterminer l'azimut des signaux radio hautes fréquences sur autant de directions qu'il y a de fréquences).

La fonction principale de ce site était l'interception des communications soviétiques et des forces aériennes du Pacte de Varsovie. Elle était aussi appelée à collecter l'ILC et le NDC (transmissions diplomatiques non américaines). À cela s'ajoute la collecte du trafic FRD (communications diplomatiques françaises).

Bien que la plupart du personnel de cette station ait été des membres de l'Armée de l'Air des USA, l'interception diplomatique et ILC ont été manipulées par les employés civils de la NSA dans une unité appelée DoDJOCC.

Chypre

Depuis l'indépendance de Chypre en 1960, la Grande-Bretagne a conservé deux bases souveraines dans le sud et l'est de l'île où sont stationnés près de 4.200 soldats et qui recouvrent une superficie de 254 km^2. La base du sud-ouest comprend la garnison d'Episkopi et Akrotiri, la plus importante base aérienne britannique à l'extérieur de la Grande-Bretagne.

Celle de l'est comprend la garnison de Dhekelia et la station d'écoutes d'Ayios Nikolaos, qui selon des analystes, se révèle très utile dans la lutte contre les réseaux terroristes au Moyen-Orient.

La station de *Paramaly* est entrée en activité en 2000. On y trouve une unité SIGINT de l'armée anglaise, ayant pour nom de code UKM 253, y est stationnée.

La station d'Ayios Nikolaos compte 14 antennes satellitaires.

Station Ayios Nikolaos (Chypre) Source : Google Earth

Ses missions sont réparties entre deux unités : « Signals Regiment Radio » & « Signals Units » de la RAF. Sa spécificité tient à sa proximité

avec les États arabes et au fait qu'elle est située à l'intérieur de plusieurs zones de couverture des satellites de communications civiles.

L'ancienne station de Hong-Kong

Créée à la fin des années 70, en même temps que la deuxième génération d'Intelsat, la station équipée de grandes antennes satellitaires. Son démantèlement a commencé en 1994 et les antennes ont été transférées en Australie.

On ne sait pas quelle station a repris les missions d'Hong Kong : Geraldton, Pine Gap ou Misawa au Japon. Ces missions pourraient avoir été réparties sur différentes stations.

L'ordinateur Dictionnaire de Westminster

En 1991, la télévision anglaise diffusa une émission sur les opérations de l'ordinateur *Dictionnaire* de Westminster, à Londres. L'émission affirma qu'il « intercepte secrètement un par un chaque télex qui arrive à Londres, qui en part, ou qui traverse la ville : des milliers de messages diplomatiques, commerciaux et personnels quotidiens. Ceux-ci alimentent un programme connu sous le nom de « *Dictionnaire* », lequel choisit des mots clefs dans la masse de signaux interceptés et sélectionne des centaines d'individus et de corporations ».

L'émission faisait également remarquer que c'était une équipe de sécurité employée par British Telecom qui faisait fonctionner les « *Dictionnaire*s », bien qu'ils soient contrôlés et utilisés par le GCHQ.

Pour note, d'autres « *Dictionnaire*s » seraient présents à Kojarena, en Australie, dans l'ancienne base d'interception de Stanley Fort, à Hong-Kong (il ne doit plus y être !) et au GCHQ de Cheltenham, en Angleterre.

Le Japon

Au Japon, et conformément au « Traité de Sécurité » signé le 2 septembre 1945, les États-Unis entretiennent une base à Misawa, au nord du pays.

Station de Misawa (source : Google Earth)

La station de Misawa

Cette station, au nord de l'île principale de Honshu, existe depuis 1948. Elle est dotée depuis cette même date d'une antenne HFDF.

Y sont stationnés des Japonais et des Américains. Pour ces derniers, on y trouve le NAVSECGRU, l'INSCOM ainsi que certains groupes de la AIA (544th IG et 301st IS).

Son nom de code est USA 39. Officiellement, il s'agit d'un « Cryptology Operation Center ». En fait, cette station permettrait d'écouter les satellites russes Molnya ainsi que d'autres satellites de communication russes.

Les écoutes se font également par voies aéroportées, grâce aux célèbres avions-espions américains, les EP-3 . L'un de ces appareils est déjà célèbre : le 31 mars 2000, suite à une avarie, il est tombé entre les mains des Chinois et son équipage a été emprisonné sur l'île méridionale de Hainan[128].

De plus, le Japon, en sus des avions de l'US Air Force, possède 5 appareils de ce genre, qui ont été « modifiés » aussitôt après la « saisie » de l'EP-3 américain par les Chinois. Après chaque mission, les renseignements sont décodés et analysés au 1er sous-sol top secret du QG de l'Agence japonaise de la défense (JDA) située dans le quartier de Ichigaya, à Tokyo.

Enfin, le parlement de Tokyo a adopté en mars 2001 un budget de 8,6 millions de francs pour créer des programmes d'interception et de surveillance. Il s'agit du dossier « Kari-no-mail », logiciel « sniffer » dédié à l'écoute des communications internet. Un appel d'offres a été lancé en avril 2001 pour un coût estimé à 500 000 francs l'unité. Une première version doit être finalisée d'ici septembre 2001, pour être installée chez les FAI au printemps 2002.

Une étroite coopération américano-japonaise

Takamizawa Nobushige est devenu, en quelques années, l'une des personnalités les plus marquantes de l'Agence de Défense japonaise (JDA). Il dirige actuellement la Division renseignement du Bureau de Politique de défense de la JDA. Mais surtout, il est au cœur de la redéfinition de l'alliance Japon-USA.

Déjà en 1996, sous le gouvernement Hashimoto, il avait été le rapporteur principal de la « Commission Higuchi », chargée de définir la nouvelle part que le Japon devait prendre à sa politique de défense, qui avait débouché sur le Projet de Programme de Défense Nationale (National Defense Programme Outline), rédigé par le même Takamizawa.

Nommé directeur du Bureau des Opérations, il avait ensuite évalué l'impact des forces nippones dans d'éventuels conflits régionaux (avec la Corée du Nord ou la Chine). Son passage à la National Defense University du Pentagone que préside le vice-amiral Paul Gaffney, a été décisif dans la définition de la nouvelle politique japonaise. Les décideurs du Pentagone comme ceux de la JDA estiment que la NDU, par son système de stagiaires, est l'un des conduits principaux des échanges stratégiques entre les deux pays.

---

[128] La saga de l'avion espion américain EP-3E, toujours aux mains des autorités chinoises sur la base navale de l'île de Hainan, est révélatrice des nouveaux enjeux militaro-économiques qui se dessinent au niveau planétaire.
Certes, cet avion, faisant partie d'une flottille de 11 exemplaires semblables, est capable d'intercepter, enregistrer, décrypter tout message émis de terre ou de l'air par radio, radar, ordinateur, e-mail, et de signaler les modifications intervenues avec une interception précédente. Mais, en fin de compte, il n'est que la pointe de l'iceberg d'un programme colossal d'investissements où business et apparat militaire sont de plus en plus indissociables.
Les États-Unis d'abord !
Le Futur Imagery Architecture (FIA) est le programme financé par le National Reconnaissance Office (NRO), agence qui analyse les images reçues par satellite. Elle dispose d'un budget annuel de fonctionnement à hauteur, c'est le cas de le dire, de 5 milliards de dollars environ, supérieur à celui de la CIA ! Ce programme prévoit le lancement, d'ici à 2005, de 20 satellites de nouvelle génération, c'est-à-dire plus légers (15 tonnes), plus maniables et plus performants. Ils seront équipés de radars et télescopes qui pourront photographier n'importe quel objet à terre et ses mouvements éventuels, même la nuit, même à travers les nuages. Pour un coût établi à plus de 21 milliards de dollars. Les grandes entreprises américaines ne se sont pas fait prier pour profiter de cette manne : Boeing, Kodak, Harris, Raytheon sont sur les rangs... En Californie 5.000 nouveaux techniciens, programmeurs et ingénieurs, vont être embauchés. De quoi donner un bol d'air aux statistiques locales du chômage.

À la suite du 11 septembre 2001, Kanemoto Toshinori (ancien président d'Interpol) est chargé de la coordination du renseignement dans l'archipel ce qui le met en contact direct avec les directions des services de renseignent américains.

Allié ou victime ?

Au tableau de chasse des grandes oreilles, on compte Shin Kanemaru, ex-parrain de la politique japonaise. Au milieu des années 90, les écoutes des communications à micro-ondes ont permis aux Américains d'apprendre qu'il cachait chez lui des barres d'or et assez de liquidités pour aider ses amis politiques… et acheter les autres.

Le 20 juin 2001, une délégation de plusieurs ONG a déposé au Parlement une motion qui s'articule autour de deux questions principales :

— le Japon est-il intégré au système Échelon en vertu du « Traité de Sécurité » ?

— le Japon est-il victime du système comme le déclarent régulièrement des fonctionnaires du MOF et du METI ?

Sur ce dernier point, des doutes existent sur l'origine des connaissances américaines lors des négociations commerciales sur l'automobile ou sur l'OMC ainsi que sur celle des révélations sur les fonds secrets du ministère japonais des affaires étrangères.

Ce climat de suspicion est renforcé par la une d'un grand quotidien japonais, le *Mainichi Shimbun*, qui a raconté dans son édition du 26 juin comment la Nouvelle-Zélande était la tête de pont d'Échelon en Asie pour surveiller les diplomates japonais.

Puis, dans un témoignage exclusif publié le 27 juin 2001 par ce même quotidien, le journaliste néo-zélandais Nicky Hager affirme que les moyens d'interception de la NSA ont été « ouvertement » utilisés en secret pour des missions d'espionnage industriel contre le Japon, et au bénéfice des États-Unis.

Selon lui, le GCSB néo-zélandais (Government Communications Security Bureau, l'équivalent de la NSA) espionnait le Japon depuis sa base de Wellington jusqu'en 1989, en analysant les données lui venant des stations d'écoute « Sigint » américaines.

Après 1990, le bureau a créé une base à Waihopai, non loin de la ville de Blenheim, recourant à un réseau sophistiqué de recueil de données afin d'espionner les transmissions des ambassades et consulats japonais. Après traitement et traduction, des rapports parvenaient régulièrement à la NSA.

Parmi les documents secrets évoqués par le Mainichi, figurent des rapports et des télégrammes diplomatiques des missions et ambassades japonaises en Océanie, ainsi que des informations secrètes sur le commerce, la pêche, les négociations commerciales, le soutien aux pays en voie de développement et les questions d'immigration.

Dans les années 80, Echelon a notamment intercepté certaines communications concernant des négociations gouvernementales japonaises au sujet du prix du charbon. Une indiscrétion qui avait permis aux Néo-Zélandais de conclure un accord favorable à leurs exportations vers le Japon.

Coopération UKUSA

L' Agence Spatiale Japonaise (NASDA) et la société australienne Xantic, filiale de Telstra, ont signé un accord, le 16 octobre 2001, pour la construction de deux stations de contrôle de satellite dans le Telstra International Telecommunications Center of Perth.

La première station assurera les communications avec deux satellites japonais à buts scientifiques et commerciaux. La seconde contribuera à la sécurité de quatre satellites de renseignement dans leur phase de lancement et de mise en orbite, puis elle sera démantelée.

Une volonté d'autonomie...

Le Japon a procédé au tir, le 28 mars 2003, d'une fusée H-2A, porteuse des deux satellites-espions entièrement développés par des firmes locales et équipés de senseurs optiques capables d'identifier des objets mesurant moins d'un mètre.

Le Japon, qui se considérait comme protégé par le parapluie américain pendant les années de guerre froide, a brutalement pris conscience de la nécessité de capacités de défense plus autonomes lors du tir en 1998 par la Corée du Nord d'un missile de moyenne portée Taepodong[129] qui avait survolé l'archipel avant de tomber dans le Pacifique.

La Corée du nord, qui a qualifié ces lancements de satellites de « provocation », a tiré deux missiles sol-mer en février et mars et est soupçonnée d'avoir déployé une centaine de missiles de type Rodong-1 d'une portée de 1.300 Km et capables d'atteindre l'ensemble du Japon.

La Nouvelle-Zélande

La Nouvelle-Zélande, membre fondateur du pacte UKUSA, est la tête de pont d'Échelon en Asie.

Nicky Hager explique ainsi que les États-Unis voulaient surveiller la manière dont la seconde économie mondiale pouvait influencer les États du Pacifique Sud.

Selon lui, le GCSB néo-zélandais (Government Communications Security Bureau) espionnait le Japon depuis sa base de Wellington jusqu'en 1989, en analysant les données lui venant des stations d'écoutes « SIGINT » américaines.

---

[129] La Corée du Nord est un pays communiste dirigé d'une main de fer par Kim Jong II et les militaires. Le régime politique s'apparente très fort à celui érigé par Staline dans l'ancienne URSS dans la première moitié du XX[e] siècle. Comme toutes les dictatures, les militaires disposent d'un budget important, ce qui permet de développer un arsenal conséquent pour un pays de cette taille.

La Corée du Nord a livré des missiles à certains pays :

– l'Iran, en échange de pétrole dont la Corée manque. À partir des missiles Coréens, l'Iran a développé les Shabah ;

– le Pakistan, qui souhaite tenir tête face à l'Inde a acheté la technologie des missiles coréens pour mettre au point les Ghauri, Shaheen entre autres ;

– la Syrie, qui a acheté des Scud Coréen ;

– la Libye, aurait acheté des missiles Nodong coréens ;

– le Yemen aurait réceptionné quelques missiles ;

– le Vietnam pourrait également avoir acheté quelques missiles.

La Corée du Nord, l'un des plus importants exportateurs d'armes, livre la technologie, quand ce n'est pas des missiles entiers, à des pays ne pouvant y avoir accès pour diverses raisons. Souvent, il s'agit de pays islamistes ou sous un régime de dictature.

Le missile Taepodong a été aperçu par les Américains en 1994, à Taepodong, une ville au nord-ouest de la Corée du Nord. Il existerait en 2 versions : Taepodong 1 et 2. Son premier étage est un missile Nodong surmonté d'un second étage directement dérivé d'un missile Scud. Le tout, surmonté d'un troisième étage et d'une coiffe dans laquelle le satellite est logé.

Le missile Taepodong 1 est le plus connu, car le 31 août 1998, il a été tiré pour la première fois dans le cadre d'une tentative de satellisation. Aucune annonce n'a été faite sur la trajectoire de la fusée. C'est ainsi que le Japon a été survolé par cette fusée sans avoir été mis au courant. En cas d'anomalie, le lanceur aurait pu s'écraser sur une ville nipponne. Selon les sources officielles, Taepodong 1 aurait été chargé de lancer le satellite Kwangmyongsong 1, qui signifie Petite étoile étincelante. La satellisation aurait même été réussie, ce qui ferait de la Corée du Nord la 10[e] puissance spatiale après la Russie (1957), les États-Unis (1958), la France (1965), l'Angleterre (1971), La Chine et le Japon (1970), l'Europe (1979), l'Inde (1980) et Israël en 1989. Mais aucune trace du satellite n'a pu être trouvée, ce qui signifierait que le lancement aurait échoué. Selon le Pentagone, la Corée du Nord aurait bien envisagé de lancer un satellite, mais l'étage supérieur serait tombé en panne avant la mise sur orbite. Des sources affirment que Taepodong pourrait être un missile intercontinental d'une portée de 2 500 km mais aurait une précision faible.

Depuis, les États-Unis ont obtenu de la Corée du Nord un accord provisoire offrant l'assurance que le pays ne procéderait plus à des tests de missiles à longue portée.

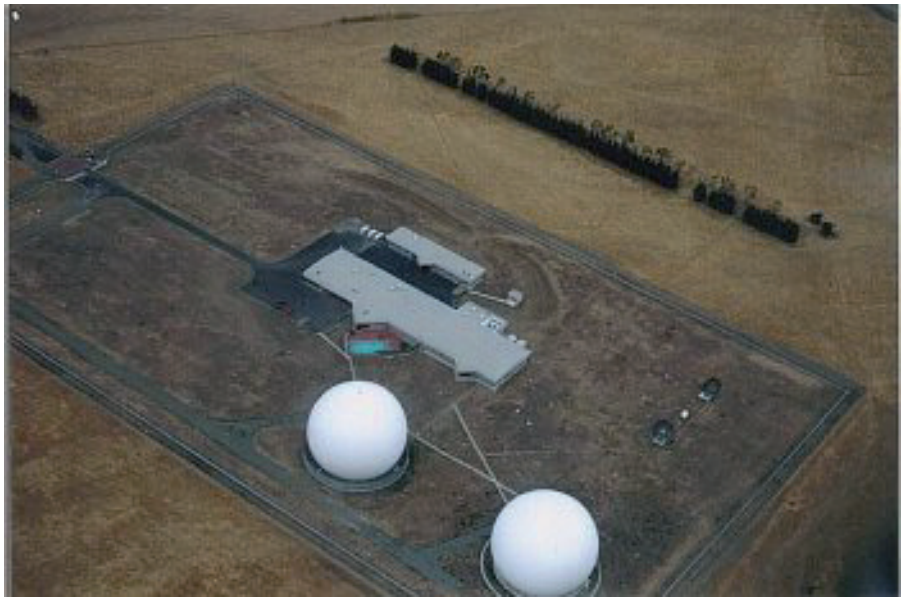
Suite à ce lancement « non prévu », le Japon a créé son propre programme militaire afin de surveiller les faits et gestes de la Corée voisine. En mars 2003, la Jaxa procédait à la mise sur orbite des premiers satellites espions japonais, les IGS.

Après 1990, le bureau a créé une base à Waihopai, non loin de la ville de Blenheim, recourant à un réseau sophistiqué de recueil de données afin d'espionner les transmissions des ambassades et consulats japonais. Après traitement et traduction, des rapports parvenaient régulièrement à la NSA.

Dans les années 80, Echelon a notamment intercepté certaines communications concernant des négociations gouvernementales japonaises au sujet du prix du charbon. Une indiscrétion qui avait permis aux Néo-Zélandais de conclure un accord favorable à leurs exportations vers le Japon.

Le siège du GCSB à Wellington

Le personnel des renseignements de Nouvelle-Zélande était en liaison avec la station Yakima de la NSA depuis 1981, quand la NSA demanda au GCSB de contribuer à un projet visant les communications de l'ambassade japonaise.



Jusqu'à l'ouverture de la station Waihopai en 1989, la Nouvelle-Zélande y recevait les communications japonaises interceptées à Yakima pour décryptage, traduction, et transcription dans le format des rapports de renseignements (la NSA fournissant le programme de décodage).

La station de Waihopai

Elle existe depuis 1989. Elle fut mise en marche fin 1991, juste avant la chute du mur de Berlin. Elle est désignée sous le nom « SIGAD NZC 333 » et porte également le nom de code de « FLINTLOCK ».

Deux dômes contiennent des antennes paraboliques. On y trouve une grande antenne d'un diamètre de 18 mètres, orientée sur des Intelsat 701 en orbite au-dessus du Pacifique, et une plus petite.

D'après les indications officielles du GCSB, la mission de la station consiste à intercepter les communications par satellite, à décrypter et à traiter les signaux. Étant donné que la station ne dispose que de deux antennes pour satellites, le service secret néo-zélandais ne peut intercepter qu'une petite partie des communications dans l'espace pacifique. La station n'est intéressante qu'en liaison avec une autre station dans la même zone. Hager cite généralement Geraldton en Australie comme station sœur de Waihopai.

Waihopai surveille la région Pacifique en interceptant les signaux au sol des satellites de communications commerciales Intelsat. Le Japon constitue sa cible principale. Le personnel de la base estime que 20 % des informations recueillies vont directement aux États-Unis sans être examinées en Nouvelle-Zélande.

Précisions et anecdotes

À partir des années 1995-1996, la base de Waihopai a renforcé son dispositif et ses cibles. L'une d'entre elles concerne les intérêts français puisqu'il s'agit des essais nucléaires de Muruora dans le Pacifique Sud et le transport de matières nucléaires (dont du plutonium) entre le Japon et la France. Un transport à haut risque, car le plutonium pouvait servir, en cas de détournement, à fabriquer un véritable arsenal nucléaire.

Dans ce cas, il est d'ailleurs possible que ce soit l'association Greenpeace qui ait relayé l'information malgré elle. L'organisation écologiste avait en effet pris l'habitude de pister ce type de cargaison.

Or elle a déjà été citée comme appartenant aux ONG qui, avec la Croix rouge, ont pu faire l'objet d'une surveillance de leurs communications.

En 1996, après la publication de *Secret Power*, Nicky Hager et le reporter John Campbell filmèrent, par de hautes fenêtres mal obstruées, l'extérieur et l'intérieur du centre des opérations. La station, complètement vide, fonctionnait de façon totalement automatique. Des lumières clignotaient sur de grands casiers de matériels informatiques pendant que des messages étaient analysés et envoyés. Une rangée d'ordinateurs disposés en fer à cheval avaient le code « envoi » par intermittence sur leurs écrans. Enfin, sur le bureau d'un superviseur, on voit que les manuels utilisés sont ceux pour le satellite Intelsat assurant les communications du Pacifique Sud.

D'autres stations

Lors d'une visite en Australie, en 1988, Bob Tizard, Ministre de la Défense de Nouvelle-Zélande, révéla que la construction de la base de Blenheim, dans l'Ile du Sud n'était pas destinée aux communications militaires, mais à l'interception des satellites de communications civiles lancés par des pays du Tiers-Monde, tels que l'Inde et l'Indonésie.

Base de Kojarena

Par la même occasion, il révéla la véritable destination de la station de Kojarena, Geraldton, près de Perth, dans l'ouest de l'Australie.

Les autres équipements

Ils disposent également de P-3 Orion. En effet, *Air & Cosmos* révèle dans son nº 1787 (16 mars 2001) que leur modernisation ne serait « plus prioritaire ». Le Premier ministre constate qu'en dix ans ils n'ont jamais détecté un sous-marin « pour la raison qu'il n'y en a pas dans le Pacifique Sud ! ».

En fait, le rôle principal des P-3 néo-zélandais n'est pas la chasse aux submersibles adverses, mais la veille électronique dans le cadre du dispositif Echelon, comme s'en sont rendus compte à leurs dépens les agents de la DGSE lors de l'affaire du Rainbow Warrior…

Un épisode peu connu :

Pendant le coup d'État de 1999 dans l'îles Fidjii dirigé par l'homme d'affaires George Speight et un ancien militaire du Special Air Services (SAS) britannique, Ilisoni Ligairi, les gouvernements australiens et Néo-zélandais de Canberra et de Wellington ont pu suivre presque en direct les événements qui se déroulaient dans l'île.

Vodaphone, seul fournisseur de services de téléphonie sans fil de l'île a permis la confection de la liste complète de tous les participants, petits et grands, du putsch. Les autorités possédaient la liste de tous ceux et celles contactés par les putschistes et de ceux et celles ayant contactés les putschistes.

Les agences responsables de ces écoutes ont été surtout le Government Communications Security Bureau (GCSB) de Nouvelle-Zélande à Waihopai et le Defence Signals Directorates (DSD) à la base militaire de Geraldton.

Divers

Le 18 décembre 2000, la Nouvelle-Zélande a décidé, comme l'Angleterre, de surveiller toutes les communications électroniques. Cette future loi s'inspire du « Regulation of Investigatory Powers Act » anglais.

Cela se traduit par la mise en place de mouchards chez les FAI pour permettre de suivre ce qui se passe sur leurs serveurs. De plus, un internaute suspecté sera obligé de délivrer ses mots de passe et clés de cryptage.

La Suisse

L'affaire Crypto AG

Des années 40 à nos jours, la NSA a cherché par tous les moyens à saper l'efficacité des systèmes de cryptographie fabriqués et utilisés en Europe. L'une de ses cibles les plus importantes fut Crypto AG, société suisse devenue un des principaux fournisseurs de système de codage et de cryptages après le Seconde Guerre Mondiale.

La NSA s'arrangea pour trafiquer les systèmes de cryptage vendus par Crypto AG afin de pouvoir lire le flux de messages diplomatiques et militaires codés de plus de 130 pays.

L'intervention de la NSA se fit par l'intermédiaire du propriétaire fondateur de la compagnie, Boris Hagelin, et consista en visites périodiques de « consultants » américains travaillant pour la NSA.

Nora L. Mackabee, une employée à plein temps de la NSA, était du nombre. Un journal américain se procura des copies de documents confidentiels de Crypto AG, lesquels mentionnaient « *la présence de Mme Mackabee à une série de discussion sur la conception d'une nouvelle machine de Crypto AG en 1975* ».

Le but de ces interventions était de s'assurer que le système de codage paraisse sûr aux autres cryptologues, sans l'être pour autant. La solution de la NSA fut de concevoir la machine de façon à ce qu'elle livre la clef utilisée (choisie par l'utilisateur de la machine et donc inconnue de tous) lors de l'interception du message ! De plus, pour éviter que cela ne soit trop transparent aux utilisateurs avertis, il fallait que la clef soit envoyée en code ; un code différent et uniquement connu de la NSA.

Station de Loèche (CH)

Ainsi, lors de chaque interception d'un message émanant de ces machines, la NSA commençait par lire sa propre partie, codée, du message (les *hilfsinformationen*) afin d'en extraire le clef utilisée par la cible et de lire le message.

L'affaire Swisscom-Verestar

Le 18 novembre 2000, la presse helvétique révéla que, le 4 octobre de la même année, Swisscom a vendu à une société américaine – Verestar — des antennes paraboliques de Loèche, en Valais, et de sept autres stations à Genève, Bâle et Zurich. Cette compagnie américaine serait liée à la NSA ; le risque existerait donc que la Suisse puisse être espionnée grâce à aux installations, qu'elle a elle-même construites, ou qu'elle serve de base à ce type d'activités.

Or, un accord signé le 20 mars prévoyait que toute vente importante effectuée par Swisscom soit précédée d'un feu vert de la Confédération : Swisscom doit soumettre pour approbation tout contrat pouvant remettre en question « l'intérêt public et la politique de sécurité ». Pourtant, la société n'aurait jamais informé les militaires de la vente des antennes de Loèche.

Pour Verestar, qui se présente comme un spécialiste de « la transmission de la voix et de données ainsi que des services Internet à l'intention du Gouvernement américain et des navires de croisière », l'acquisition des antennes de Loèche est « un premier point d'ancrage en Europe » et permettra « de faire la liaison avec tous les satellites situés au-dessus de l'océan Indien », a affirmé lors de l'achat Alan Box, vice-président et directeur général de Verestar.

Les liens troubles de Verestar

Verestar est un provider spécialiste de l'Internet et de la communication sans fil. Cette filiale d'American Tower Corporation (Boston, Massachusetts) — qui possède quant à elle 10 300 relais terrestres de communications électroniques — ne semble pas directement connectée, de prime abord, avec les activités d'écoute des services secrets américains.

Pourtant, Verestar a acquis, ces dernières années, plusieurs stations terriennes de transmission par satellite (SNAP). C'est un de ces SNAP qu'elle a acheté à Swisscom à Loèche. Elle en possède maintenant une dizaine dans le monde. Verestar gère également 160 stations de plus petite taille, dont les sept achetées à Swisscom, à Bâle, Zurich et Genève.

La seule collaboration avouée entre Verestar et le Gouvernement américain est un contrat liant sa division des télécommunications maritimes et la marine américaine, l'US Navy. Elle lui fournit des services téléphoniques pour déployer sa flotte.

Contactée pour commenter ses affaires avec la marine américaine et ses achats à Swisscom, Verestar, basée à Fairfax (Virginie), n'a pas répondu.

Plus intéressant, Verestar fournit des connexions directes à des hubs[130] majeurs de communication Internet, les Metropolitan Area Ethernets (MAE). Dans un récent rapport intitulé « *Capacités d'interception 2000* », le Parlement européen a pointé le doigt sur ces MAE et sur d'autres sites Internet comme étant les « *oreilles indiscrètes* » de la National Security Agency (NSA) sur l'internet.

Enfin, Verestar travaille aussi pour I'US Navy, via son Maritime Telecommunications Network (MTN).

Pour un ancien haut fonctionnaire du Gouvernement américain, le contrat entre Verestar et Swisscom pourrait démontrer que la NSA a décidé d'outsourcer[131] certaines de ses activités à des compagnies privées. Il assimile ces opérations à une sorte de « privatisation des renseignements électroniques ». Sous l'appellation « *opération Groundbreaker* », la NSA a déjà délégué nombre de ses activités « non critiques » au secteur privé. Elle anticipe ainsi sa privatisation qui devrait commencer en juillet 2001.

Épilogue

Finalement, dans un communiqué du 14 décembre, Swisscom annonce : « le secteur Broadcasting (BCS), qui emploie environ 200 personnes et possède des émetteurs et des réémetteurs sur plus de 400

[130] Le mot *hub* est un anglicisme qui signifie *concentrateur*, c'est un appareil permettant de créer un réseau informatique.

[131] Outsourcer : confier à un tiers l'éxecution d'une prestation de service récurrente.

sites, restera la propriété de Swisscom.. L'activité spécialisée de Broadcasting continuera à se développer dans le cadre d'une filiale. Rappelons qu'elle représente aujourd'hui moins de 2 % du chiffre d'affaires du groupe Swisscom ».

Pourtant, le 10 février 2001, à Washington, un cadre de la société Swisscom a affirmé au correspondant du *Monde du Renseignement* que la NSA était vivement intervenue en faveur de cet achat, estimé à 100 millions de francs suisses. L'Agence souhaitait disposer de contacts privilégiés avec l'opérateur de ces stations satellitaires.

Les activités de Swisscom A.G. à Loeche présentaient plusieurs intérêts stratégiques. En effet, les satellites de communication (de type Intelsat) possèdent un nombre variable de canaux. Chaque canal peut acheminer des centaines de communications (voix et données).

Jusqu'à maintenant, en fonction de la participation financière des pays, on attribuait aux opérateurs nationaux un nombre de canaux précis, couvrant des zones géographiques déterminées. Ainsi, Swisscom, via son centre de Loeche, gérait notamment une grande partie du trafic des communications par satellite entre l'Europe et la région de l'océan Indien, mais aussi entre l'Europe et certaines zones du Moyen-Orient.

Une station d'écoute du projet Satos (Suisse)

Le projet Satos 3

La Confédération développe son propre système de surveillance grâce à des antennes similaires à Loèche dans le cadre du projet Satos 3, destiné à prévenir « les menaces liées à la technologie, au terrorisme et à la prolifération nucléaire ».

Station de Zimmerwald (Suisse)

Station d'Heimenschwand (Suisse)

Il s'agit d'un projet initié dans les années 1990 par Peter Regli, l'ancien chef des services secrets mis à pied après l'affaire Dino Bellasi[132]. Il vise à doter la Suisse de son propre système d'écoute des satellites de télécommunications. Un système identique à celui d'Echelon, mais en modèle réduit. Les antennes nécessaires, qui proviennent de Grande-Bretagne (!), seront installées à Loèche (VS), juste à côté de celles de Verestar, à Zimmerwald et à Heimenschwand (BE), pour un montant estimé entre 50 et 100 millions de francs.

[132] Comptable au Service de Renseignements Suisse, accusé, semble-t-il à tort, d'avoir été une « taupe » de la NSA.

Officiellement, il ne sera utilisé que pour des écoutes à l'extérieur des frontières, puisque la législation en la matière a été durcie en Suisse.

Dans les faits, rien n'empêcherait pourtant Satos 3 de rejoindre le réseau Echelon, même si Adolf Ogi, chef de la défense (DDPS), a toujours assuré qu'il n'y aurait pas de collaboration avec des pays étrangers.

Selon Duncan Campbell, Satos 3 pourrait être un des nouveaux maillons d'Echelon.

Taiwan

Dans son édition du 23 janvier 2001, le *Jane's Defence Weekly* révèle l'existence d'une base SIGINT appartenant au Réseau Échelon.

Elle se situerait dans les montagnes de Yangmingstan, au nord de Taipeh, et serait gérée conjointement par la NSA et le « Military Intelligence Bureau » taïwanais (MIB). Sa mission essentielle, vu son emplacement, est l'interception des communications de la République Populaire de Chine.

Une fois collectées, les informations seraient transmises à Fort Meade, près de Washington. Mais, il semble admis que les militaires taïwanais les utiliseraient également.

Depuis cinq ans environ, les systèmes d'écoutes taïwanais ont subi une complète modernisation tant en ce qui concerne les méthodes que pour les équipements.

On apprend également dans cet article que se trouverait sur place une société de communication du Maryland (où se situe également Fort Meade, siège de la NSA) dont la particularité est de n'employer que des retraités des services secrets américains. Il s'agit vraisemblablement d'un paravent commercial de la NSA. En effet, les relations diplomatiques entre la Chine et les États-Unis empêchent la présence d'agents officiels américains sur le sol taïwanais. Plusieurs dizaines de ces employés-retraités s'affairent sur le site même.

L'enrôlement de Taiwan par la NSA est aussi en droite ligne avec les nouvelles méthodes d'intelligence et de surveillance au 21e siècle, dressées récemment par Washington dans un rapport officiel.

Sources

Ce document vient du *Monde Diplomatique* ; il revient sur l'échec du renseignement électronique au regard des attentats du 11 septembre. Il est signé par N. HAGER et date du mois de novembre 2001.

Au cœur du renseignement américain

La NSA, de l'anticommunisme à l'antiterrorisme

Incapables de prévenir les attaques du 11 septembre 2001, les services de renseignement des États-Unis ont-ils failli à leur mission ? Pourquoi Echelon, le système d'écoute planétaire de la National Security Agency (NSA), n'a-t-il été d'aucun secours ? C'est que le véritable objectif de cette très secrète agence, depuis la fin de la Seconde Guerre mondiale, n'a pas été d'assurer la sécurité des États-Unis, mais de se garantir un « accès global » aux communications du monde entier afin d'accroître la prééminence du pays sur tous les plans, tant militaire qu'économique et politique.

Par Nicky Hager

Écrivain et chercheur néo-zélandais. Auteur de *Secret Power*. New Zealand's Role in the International Spy Network, Craig Potton Publishing, Nelson, Nouvelle-Zélande, 1996.

Réunis à l'Opéra de San Francisco en avril 1945, les délégués de plus de cinquante pays s'engageaient à épargner aux générations futures le fléau de la guerre. Les Nations Unies allaient reposer sur le principe de « l'égalité des droits des nations, grandes et petites (...), cohabitant dans la paix et le bon voisinage ». Le président américain Franklin D. Roosevelt avait insisté pour que les États-Unis accueillent la conférence. Générosité ? Il s'agissait aussi de permettre à ses agents d'espionner les délégués et de surveiller les messages qu'ils échangeaient avec leurs capitales.

Recueillis par les compagnies télégraphiques, leurs télégrammes, cryptés, furent décodés par des officiers opérant vingt-quatre heures sur vingt-quatre, puis transmis aux négociateurs américains. Ce fut un succès total...

Élaborées contre les puissances de l'Axe — puis contre l'Union soviétique —, les capacités américaines de renseignement électronique allaient être regroupées au sein de la National Security Agency (NSA).

De cette agence, on ignora tout jusqu'à la publication, en 1982, de *The Puzzle Palace*, dans lequel le journaliste américain James Bamford décrivait son fonctionnement. Dans son nouvel ouvrage, *Body of Secrets* (voir plus loin), il dévoile de nouveaux pans de cette histoire secrète. La NSA, révèle-t-il, dispose d'un budget annuel de plus de 7 milliards de dollars, sans compter les sommes affectées aux satellites-espions. Elle emploie plus de 60 000 personnes — plus que la CIA et le FBI réunis.

Les affaires du monde se traitant de plus en plus par la voie des communications électroniques (par radio, puis par Internet), la surveillance de ces échanges est primordiale. La NSA est chargée de ce « renseignement de signaux » (SigInt, par opposition à HumInt, le renseignement humain), en étroite collaboration avec ses homologues — et subordonnées — britannique, canadienne, australienne et néo-zélandaise, qui forment l'alliance « UKUSA ».

Ancien directeur de l'agence, M. William Studeman résumait ainsi son rôle : le soutien aux opérations militaires « est fondamental, et la nécessité d'un accès global accru [aux communications électroniques] se fait de plus en plus sentir. C'est sur ces deux métiers que la NSA doit solidement s'appuyer ».

Opérations à géométrie variable

Bien que sophistiqués et puissants, les systèmes de surveillance de la NSA ont montré leurs limites le 11 septembre 2001. Tout comme un système de défense antimissile n'aurait rien pu contre des attaques menées à l'aide d'avions de ligne, les systèmes de surveillance avancés se révèlent peu efficaces contre les moyens de communication rudimentaires (boîtes à lettres anonymes, intermédiaires sûrs, etc.) utilisés par une cellule bien organisée. « *La NSA écoute régulièrement les appels non cryptés passés par le terroriste présumé Oussama Ben Laden [via le réseau satellitaire Inmarsat], souligne Bamford. Pour impressionner ses visiteurs, elle leur passe parfois les échanges entre Ben Laden et sa mère. (...) Celui-ci sait que les États-Unis écoutent ses communications internationales, mais il semble n'en avoir cure.* »

Retraçant l'histoire de cette surveillance électronique planétaire, James Bamford convainc que sa mise en place n'avait pas pour vocation première de protéger les États-Unis contre des menaces extérieures, mais, le plus souvent, de réunir des informations servant à promouvoir la guerre en tant qu'instrument politique et à saper les « droits fondamentaux » des autres pays.

Dans l'immédiat après-guerre, au siège de l'ONU — truffé d'écoutes —, on débattait de la partition de la Palestine — une mesure qui a transformé la région depuis en l'un des principaux foyers d'instabilité et de violence politique du monde. Les États-Unis exercèrent une pression extrême pour que soit votée la partition, et pesèrent notamment de tout leur poids sur trois petits pays — le Liberia, Haïti et les Philippines — qu'ils forcèrent à changer de position à la veille de la décision finale.

James Forrestal, alors secrétaire américain à la défense, écrit à l'époque, dans son journal personnel, que « *les moyens de coercition exercés sur ces pays confinaient au scandale* ».

Dès 1945, les agents américains et britanniques avaient engagé une course de vitesse avec leurs homologues soviétiques pour déchiffrer les codes de l'armée allemande. Les États-Unis devancèrent largement l'Union soviétique, mais l'avantage fut de courte durée. Dans le courant des années 1950, des avions-espions survolèrent l'Union soviétique, à l'instar de ceux qui survolèrent, en avril 2001, l'île de Hainan, en Chine ; dès la fin des années 1980, la NSA avait encerclé l'URSS de stations d'écoute, d'avions, de navires et de sous-marins.

Après l'échec de l'invasion anticastriste de la baie des Cochons, en avril 1961, les chefs de l'état-major américain concoctèrent un projet étrange. Leur stratégie, mise au jour par Bamford, consistait à lancer une « campagne de terreur » à l'encontre des citoyens américains et à l'imputer à Cuba afin de justifier une invasion généralisée de l'île. Un rapport secret avançait que « *la publication de la liste des victimes dans les journaux américains provoquerait dans le pays une vague d'indignation instrumentalisable* ».

Baptisé « Northwood Operation », ce plan prévoyait des détournements d'avions et des attentats à la bombe à Miami et à Washington. Les documents préparatoires précisaient qu'il fallait « *donner au monde l'image d'un gouvernement cubain représentant (...) une menace grave et imprévisible pour la paix dans l'hémisphère occidental* ».

L'administration Kennedy n'approuva pas l'opération Northwood, mais, deux ans plus tard, un « incident » similaire dans le golfe du Tonkin déclenchait la guerre du Vietnam.

Des agents de renseignements britanniques, australiens et néo-zélandais se rallièrent à une vaste opération des services secrets américains au Vietnam, les aidant notamment à localiser des cibles afin que soient remplis les quotas quotidiens des missions de bombardement des B-52.

L'histoire de l'agence fait apparaître une grande variabilité dans l'attitude des États-Unis. Un exemple éloquent en est l'attaque par Israël du navire-espion Liberty de la NSA lors de la guerre de six jours.

Le 8 juin 1967, après avoir surveillé étroitement, six heures durant, le Liberty qui patrouillait au large, l'armée israélienne lança des attaques par voie aérienne et par torpilleur jusqu'à ce que la plupart des membres de l'équipage soient morts (34 hommes) ou blessés (171) et que le navire soit quasiment détruit. Les canots de sauvetage furent coulés sitôt mis à la mer. Israël prétendit après coup qu'il s'agissait

d'une erreur. Alors que la NSA disposait des preuves du contraire, le gouvernement américain accepta cette explication et n'ouvrit jamais d'enquête.[133]

De façon convaincante, Bamford démontre que les militaires israéliens savaient pertinemment qu'ils attaquaient un navire-espion américain. Il suggère que le but de l'attaque était d'empêcher la collecte d'informations sur les atrocités militaires commises à 20 kilomètres de là seulement, dans la ville égyptienne d'El Arish, où des soldats israéliens étaient en train de fusiller des centaines de civils et de prisonniers ligotés. Le Pentagone décréta un black-out médiatique total, et les membres de l'équipage furent menacés de prison s'ils parlaient de l'attaque.

Le président américain Lyndon Johnson aurait déclaré que « *peu [lui] importait que le navire coule, il ne mettrait pas ses alliés dans l'embarras* ».

En Nouvelle-Zélande, comme dans d'autres pays, la guerre du Vietnam retourna l'opinion publique contre la politique étrangère de Washington. Dans la région, elle ajouta au désenchantement général provoqué par le soutien américain aux régimes Suharto en Indonésie et Marcos aux Philippines, et leur soutien occulte de l'invasion indonésienne du Timor-Oriental en 1975.

Le recours à la guerre et un respect à géométrie variable des droits des autres pays heurtèrent ceux qui portaient sur le monde le regard d'un « petit pays ». Mais, si l'opinion publique néo-zélandaise souhaitait une politique étrangère plus indépendante, ses services de renseignement continuèrent de servir d'avant-poste au système américain. Ainsi, alors que la majorité des Néo-zélandais soutenaient l'indépendance du Timor-Oriental, les services de renseignement de leur pays participèrent avec l'Australie à la surveillance de la population de l'île, pour le compte des gouvernements américain et britannique — à une époque où ceux-ci collaboraient avec les services secrets indonésiens.

L'inégalité des rapports au sein de l'alliance UKUSA n'est plus à démontrer. Les services secrets néo-zélandais fournissent les renseignements que la NSA leur demande, sans trop insister sur ce qu'ils veulent en échange — et même si cela va à l'encontre de l'intérêt national ou de la politique de leur propre pays. Par ailleurs, ils considèrent que le fait d'espionner leurs amis, voisins et partenaires commerciaux équivaut à payer un bien petit prix pour préserver une relation privilégiée — une déférence qui traduit un profond sentiment d'insécurité. Sans doute les services secrets britanniques voient-ils les choses de la même manière.

Les membres des services de renseignement néo-zélandais traitent les milliers de rapports arrivant chaque semaine de la NSA. Les cibles indiquées reflètent les priorités et les préoccupations du gouvernement américain. Durant les années 1980, les téléscripteurs déversèrent ainsi une avalanche de commu-

---

[133] L'étrange affaire du « Liberty » (*Histoire mondiale de l'espionnage*)
Le 8 juin 1967, quatrième jour des opérations, un peu avant neuf heures du matin, l'USS Liberty naviguait au large d'El Arish, face à la péninsule du Sinaï, quand il fut survolé à plusieurs reprises par des avions israéliens apparemment à la recherche d'une flottille de vedettes lance-torpilles égyptiennes. Armé par la National Security Agency, le Liberty était chargé de suivre, grâce à ses équipements perfectionnés, l'évolution des combats. Quelques heures après le passage des avions de reconnaissance, le navire américain était attaqué par quatre Mirage III de Tsahal qui devaient le bombarder durant une demi-heure. Au terme de cette attaque, des vedettes israéliennes prirent le relais. À quinze heures, c'est sous la protection de deux navires de guerre... russes que le Liberty rallia la 6e Flotte américaine. Les installations électroniques du bateau étaient détruites (le navire lui-même devait être mis à la ferraille) et les Américains comptaient 34 morts et 171 blessés !
Officiellement, tant les Américains que les Israéliens, ont retenu la thèse de la méprise : le Liberty aurait été confondu avec un vaisseau ennemi. Une explication peu plausible : la bannière américaine arborée par le bateau était parfaitement visible et ses communications avaient été brouillées dès le début de l'agression. Certains experts estiment que c'est pour couper les Américains d'une source de renseignements de première main que l'attaque fut menée, de manière délibérée.
Washington commençait à exercer des pressions assez fortes sur Tel Aviv pour mettre fin à des hostilités qui, poussées trop loin, risquaient de déstabiliser toute ta région. Or, Tsahal préparait, pour le lendemain, la prise du plateau du Golan, l'un des objectifs majeurs de la guerre préventive menée par Israël.

nications interceptées en Afghanistan, collectées afin d'aider les « combattants de la liberté » — dont M. Oussama Ben Laden — dans leur lutte contre les Soviétiques.

Certains de ces officiers collectaient des renseignements dans la zone Pacifique en fonction des requêtes de la NSA. Non, ils ne traquaient pas des terroristes. Ils ciblaient en revanche tous les aspects de la vie politique, économique et militaire de la région — cabinets ministériels, police, armée, partis d'opposition et organisations non gouvernementales —, dans chaque pays, de façon méthodique et permanente. Toutes les organisations régionales, toutes les conférences commerciales et toutes les agences des Nations unies de la zone sont également placées sous étroite surveillance.

L'un de ces analystes mentionna le cas d'une opération de surveillance contre l'État insulaire de Kiribati. La pêche constitue la principale ressource de cette nation à l'économie fragile. Après avoir subi de longues années durant le braconnage des bateaux américains de pêche au thon, le gouvernement de Kiribati avait trouvé une entreprise soviétique disposée à verser des droits pour avoir accès aux pêcheries. Bien que la guerre froide approchât alors du dégel, l'alarme anticommuniste retentit au sein des agences de renseignement. Les officiels néo-zélandais surveillèrent chaque communication reçue par ou émanant de Kiribati, qu'ils transmirent ensuite aux États-Unis, lesquels s'en servirent dans le cadre d'une campagne diplomatique qui fit avorter le projet.

L'événement ne changea pas le cours de l'histoire mondiale, mais eut un impact très néfaste sur ce micro-Etat.

Les négociateurs sur écoute

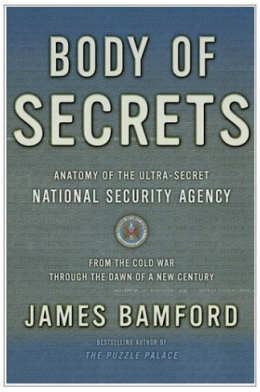
Ces officiers néo-zélandais font état d'un autre déluge de communications lors des négociations de l'Accord général sur les tarifs douaniers et le commerce (GATT), à propos duquel responsables américains et européens se livrèrent bataille au cours des années 1980 et 1990.

Bamford, de son côté, indique qu'une équipe de la NSA fut dépêchée à Genève en 1995 afin d'espionner les cadres japonais de Toyota et de Nissan lors des négociations nippo-américaines sur les droits de douane appliqués à l'automobile. Ancien agent du renseignement canadien, Mme Jane Shorten a en outre révélé la mise sur écoute des délégués mexicains lors des négociations de l'Accord de libre-échange nord-américain (Alena) en 1992.

L'espionnage d'après-guerre aurait pu être mis au service des espoirs nourris par les fondateurs des Nations Unies : garantir l'égalité des droits des nations, et épargner au monde le fléau de la guerre. Or, l'histoire montre surtout le contraire. Ces opérations servent à accentuer les inégalités de pouvoir.

La NSA et ses alliés se complaisent dans leur image de héros combattant les despotes et les terroristes. Parfois, cette image est juste. La plupart de leurs cibles, toutefois, ne représentent aucune menace.

Certaines opérations de renseignement sont de fait destinées à soutenir des despotes, d'autres créent un climat propice au développement du terrorisme. Les gouvernements ayant misé massivement sur l'espionnage des signaux en retirent un sentiment de sécurité trompeur. Il est peu probable que le problème puisse être résolu en injectant des ressources supplémentaires à la NSA.



Ce document provient du site et de la liste de diffusion d'*Automates Intelligents*. Il date du 15 novembre 2001.

Body of Secret

James Bamford, Editions Doubleday, 2001.

Présentation et commentaires par Jean-Claude Empereur

James Bamford, qui s'est spécialisé comme auteur enquêteur dans le déchiffrage des secrets de la puissante et mystérieuse Agence Nationale de Sécurité NSA (livre précédent : *The Puzzle Palace*), nous livre un nouvel ouvrage de plus de 600 pages sur ce même sujet.

La NSA est décrite dans un style très vivant, presque romanesque, mais qui s'appuie sur des sources apparemment très sûres (près de 200 pages de notes documentaires). L'histoire de l'Agence est décrite depuis les temps héroïques de la guerre froide, jusqu'à nos jours. Il y apparaît clairement qu'Internet est devenu l'outil favori du renseignement pour ce type d'organisme et de missions.

L'auteur laisse même entendre que le réseau mondial a été conçu à cette fin par les autorités américaines. L'avenir est également sans ambiguïté. Grâce à un Internet de plus en plus ramifié et fréquenté, grâce aux systèmes d'écoutes dont le plus connu est Echelon, grâce aussi aux robots hyper intelligents existants ou en cours de développement afin de transformer en informations exploitables les milliards de communications interceptées, la domination du cerveau américain sur le monde — et sur les acteurs de la mondialisation — ne fera que se renforcer.

Vers le « monitoring » de la mondialisation ?

« *In God, we trust, all others we monitor* ». Cette phrase est placée en exergue du livre très intéressant et très documenté de James Bamford — « Body of Secrets » — Anatomy of the ultra secret National Security Agency, from the cold war through the dawn of a new century.

Rendre compte d'un livre consacré au renseignement, à l'espionnage électronique, ses moyens, ses méthodes, ses objectifs implique nécessairement prudence et circonspection, tant le risque est grand de manipulation et de désinformation.

S'agissant de la NSA, la plus secrète, la plus puissante, la plus technique, la plus mystérieuse aussi des agences de renseignement, la circonspection s'impose d'autant plus.

Toutefois, malgré ces réserves, le livre de J. Bamford — une véritable « somme » — mérite la plus grande attention[134].

Lorsqu'on imagine, que, pour d'évidentes raisons, il ne concerne sans doute que « les dix pour cent émergés de l'iceberg », l'on ne sait ce qui doit l'emporter de l'inquiétude ou de la stupéfaction. En effet, l'histoire déjà longue de la NSA illustre et confirme la détermination et la volonté des États-Unis de contrôler « informationnellement » le monde.

La NSA est à la fois la toile et l'araignée du Web. On savait la NSA puissante et tentaculaire, on ne l'imaginait pas à ce point.

Dans la perspective qui est la nôtre, qui consiste à détecter, par l'analyse des conséquences de l'utilisation massive des technologies de l'information (ordinateurs, logiciels et réseaux), ce qui, dans la conduite des sociétés, fait appel aux processus « d'automatisation », le livre de J. Bamford est particulièrement éclairant.

Un système planétaire d'acquisition de l'information

L'auteur montre tout d'abord comment, dès la Seconde Guerre mondiale, puis tout au long de la guerre froide, enfin après l'effondrement de l'Union Soviétique, se construit année après année, pièce par pièce, un système global, intégré d'écoute (eavesdropping) à l'échelle de la planète au seul profit du monde anglo-saxon.

Le système comprend des ordinateurs, des réseaux, des satellites, des stations d'écoute, des dizaines de milliers d'agents : mathématiciens, linguistes, concepteurs ou casseurs de codes, informaticiens, physiciens, militaires, civils, etc. recrutés au moyen des méthodes les plus sophistiquées qui soient, pour la plupart d'entre eux formés dans une université « maison », pratiquant au quotidien une véritable culture du secret et vivant au cœur de ce que Bambord appel « Crypto-City ».

[134] Body of Secrets se compose de 14 chapitres intitulés Memory, Sweat, Nerves, Fists, Eyes, Ears, Blood, Spine, Adrenaline, Fat, Muscle, Heart, Soul, Brain. Il y a chez Bamford une perception « hobbesienne » de la NSA. LEVIATHAN, voire ALIEN ne sont pas loin !

Le livre fourmille d'anecdotes, de réflexions, d'interrogations, toutes plus intéressantes les unes que les autres.

Sur un point qui a récemment frappé l'opinion ainsi que le Parlement Européen — le Système Echelon — l'auteur lève le voile sur l'ampleur et les objectifs de ce projet dont on est sans doute encore loin, aujourd'hui, d'avoir mis en évidence toutes les potentialités.

Écoutons l'auteur :

« Depuis la signature du UK/USA Communications Intelligence Agreement, le 5 mars 1946, le partenariat [UK, USA, NEW-ZEALAND, CANDA, AUSTRALIA], s'est développé en permanence. A la fin des années 80, il n'y avait pas un seul endroit du monde sur terre, qui ne soit couvert par une station d'écoute appartenant à l'un de ses membres ou par un satellite américain. Les principales nations anglophones scellèrent à partir de 1977 un accord ultrasecret leur permettant d'écouter, de par le monde, leurs amis comme leurs ennemis.

Le partenariat UK/USA devint ainsi une entité supranationale, avec ses propres lois, ses codes, ses prestations de serment, ses langages, tous ultrasecrets et cachés du public. L'UK/USA se comporte en « nation virtuelle » avec CRYPTO-CITY comme capitale et FORT MEADE comme quartier général. Le logiciel faisant fonctionner le système reçut le nom d'Echelon » (pp 403-404).

Grâce à ces quelques citations, on mesure bien l'enjeu géopolitique : mettre sur écoute le monde non anglo-saxon. En cinquante ans, le réseau s'est très fortement développé et diversifié. Il continue dans cette voie.

Voilà pour la dimension « horizontale » du système : couvrir la planète. Qu'en est-il de la dimension « verticale » : accéder le plus instantanément possible au plus grand nombre de données ? Sur ce plan également, l'ouvrage est très éclairant.

Le renseignement, moteur de l'industrie des technologies de l'information

On mesure à un point qu'on ne soupçonnait pas combien la NSA a joué un rôle essentiel depuis les origines dans la conception et le développement des ordinateurs aux États-Unis, et en particulier des supercalculateurs ainsi bien entendu que de leur logiciel.

Du STRETCH[135], dont les services américains d'IBM disaient, à l'époque, en 1955, qu'il ne pouvait avoir que deux clients, la NSA et l'Atomic Energy Commission (AEC) au CRAY 2 trente ans plus tard, dont l'auteur qui tout au long de son livre développe une conception anthropomorphique de la NSA, dit qu'il ressemblait à un être humain, parcouru par une sorte de « plasma sanguin » (blood plasma) rouge et pétillant, irriguant l'ensemble de la machine, elle-même constellée de lumières clignotantes, l'agence pilote tous les projets, etc.

L'ordinateur STRETCH d'IBM

Non sans humour, J. Bamford écrit : « SEYMOUR CRAY's latest masterpiece, looked more like bordello furniture than a super number cruncher in a code breaking

[135] Le STRETCH est le premier ordinateur à transistors produit par IBM. Il comporte 150 000 transistors et a une vitesse de traitement de 200 instructions à la seconde. C'est le plus rapide de son époque, affirme IBM C'est à l'occasion de la mise au point du STRETCH que le mot octet est employé pour la première fois. Un octet égale 8 unités binaires. Un octet désigne communément un caractère alphanumérique car chaque lettre ou chaque nombre est représenté par une série de 8 zéros ou uns. Un Ko (kilo-octet) = 1 024 octets. Un Mo (méga-octet) = 1 024 Ko. Un Go (giga-octet) = 1 024 Mo.

factory » (Le dernier chef d'œuvre de SEYMOUR CRAY, regardé plutôt comme des meubles de bordel que comme une machine à calculer superbe à casser les codes, p.592).

Plus tard, dans les années 1980, lorsque les Américains, libéralisme oblige, choisiront de recourir presque exclusivement aux composants japonais, la NSA, consciente du danger que représentait cette politique, décide de fabriquer elle-même avec l'aide de National Semi Conductor, les composants nécessaires à ses propres ordinateurs. Au cours des années 90, la NSA est toujours présente, en 1992 est conçu le CRAY 3 Super Scalable System, destiné à devenir le cerveau de ce qui est déjà surnommé « the world's ultimate spying machine »[136].

Aujourd'hui, avec l'appui des centres de recherche internes de la NSA (Communication and Computing Center, ex-NSA Research Institute ; Laboratory for Physical Sciences, LPS, etc.) les recherches se développent sur les supercalculateurs et se poursuivent avec la mise en chantier du CRAY T3 E - 1200 disposant de 1088 processeurs, et pouvant atteindre ainsi une vitesse de pointe de traitement de 1,3 téraflops, soit 1,3 trillion d'opérations par seconde…

Le « data mining[137] » quant à lui, qui est la raison d'être de la NSA, se poursuivra avec d'autant plus d'efficacité qu'on lui fournit dès aujourd'hui, selon l'auteur, l'assistance d'un système de stockage des données capable d'engranger l'équivalent de 1.500.000 années du Wall Street Journal… ou d'un mur de livres empilés par 11 sur une distance allant de New York à Los Angeles.

En addition à ces moyens de stockage a été mis en place un nouveau système fonctionnant en réseau reliant plusieurs ordinateurs de la taille d'un portable et capables de stocker 5 trillions de pages, accessibles simultanément, soit l'équivalent en quantité d'informations d'une pile de feuilles de papier de 240 Km de haut !…

Aujourd'hui, les chercheurs de la NSA utilisent les techniques de « portes logiques », moléculaires, ou atomiques, développant les recherches, alliant l'électronique au biologique, travaillent sur des projets de calculateurs plusieurs milliers de fois plus rapides que ceux qui existent actuellement. L'objectif avoué étant d'aller explorer tous les recoins d'Internet en moins d'une ½ heure (a search engine that could examine every nook and cranny of the INTERNET in half an hour…[a kind] of brute force decoder[138] » … p. 610).

Par ailleurs, la NSA utilise pour ses besoins et ceux de ses principaux clients un super Internet ultra protégé et ultra sécurisé, INTERLINK.

Quand on sait que la Defense Advanced Research Project Agency (DARPA) qui a conçu il y a trente ans Internet, est le partenaire habituel de la NSA, on mesure à quel point le « renseignement » est au « cœur du cœur » du complexe militaro-industriel américain.

Vers la « Surveillance » de la planète

Je pense qu'il fallait s'étendre un peu sur ces rappels technologiques, pour prendre conscience du rôle stratégique de la NSA dans la mise en œuvre d'une véritable politique de « control and command » de la planète pour reprendre l'expression militaire américaine. L'axe central de cette stratégie, c'est sinon l'automatisation de la mondialisation, du moins, pour reprendre la phrase citée en exergue, son « monitoring ».

L'automatisation, voire la « cérébralisation », viendront plus tard…

---

[136] Seymour Roger Cray (28 septembre 1925 à Chippewa Fall dans le Wisconsin — 5 octobre 1996), ingénieur de génie, conçut plusieurs super ordinateurs et fonda la société qui porte son nom, Cray Research. Pendant trois décennies la réponse rapide à la question : « Quelle entreprise fabrique l'ordinateur le plus rapide ? » fut : « Celle où est impliqué Seymour Cray. » Le Cray 3 ne fut jamais produit, et la société fit faillite.

[137] Exploitation des données

[138] Un système de recherche qui pourrait examiner chaque recoin et niche de l'Internet dans une demi-heure… une sorte de décodeur à force brutale.

La NSA est l'un des centres, peut-être même le « centre », de la puissance américaine. Elle observe, photographie (satellites, avions-espions, drones), écoute, décrypte, extrait (data mining), analyse, commente et délivre l'information à ses « clients », les principaux d'entre eux étant le Gouvernement Fédéral (NSC, CIA, etc.) mais aussi selon toute vraisemblance, l'ensemble du « complexe ».

A leur tour, ces « clients » exploitent, informent, désinforment, déstabilisent, manipulent l'opinion, les médias, l'industrie culturelle. Les résultats de cette information/désinformation/manipulation sont ensuite mesurés, analysés, réinjectés dans le système par voie d'enquêtes, de sondages, transformés en discours, prises de position, actes diplomatiques ou militaires, etc.

La boucle est bouclée. Une sorte de « couplage sociétal » s'établit et finit par se développer de lui-même, avec à la limite le risque d'échapper à tout contrôle.

Présentation simpliste direz-vous, par trop mécaniste, certes, mais la tendance est là, la dérive est positive[139]. Petit à petit, c'est ainsi que s'édifie la cyberplanète et que s'élabore à l'échelle mondiale une intelligence collective (en l'occurrence au double sens du terme).

Il ne sert à rien, me semble-t-il, de critiquer cette politique américaine du renseignement. Il est normal que les USA cherchent à se protéger et à influencer à leur profit le reste du monde. C'est une logique de puissance bien naturelle. Toute récrimination à cet égard me paraît sans objet et semble inspirée par le dépit et le reflet d'un complexe d'infériorité.

Ce qui est en revanche anormal, c'est que les Européens dûment avertis (cf. le rapport du Parlement Européen) ne cherchent pas de leur côté à bâtir leur propre système.

Les événements du 11 septembre conduisent à ce que la dimension protection/renseignement/recherche militaire devienne dans les mois et les années à venir, l'un des axes majeurs de la construction européenne. De ce point de vue, il est essentiel pour les Européens de comprendre que cette dimension trop négligée jusqu'à maintenant implique un effort aussi important que celui qu'ils ont engagé jadis dans l'aérospatial ou le nucléaire.

Au-delà de l'indépendance qu'il leur fait défaut, de la souveraineté qu'il leur faut retrouver, c'est bien de leur survie qu'il s'agit.

Il faut lire « *Body of Secrets* » : ce livre fourmille d'informations qui seront très utiles à ceux qui pensent que le monde multipolaire de demain sera le théâtre d'une âpre compétition sinon entre « grands automates sociétaux », mais, à tout le moins, entre grands systèmes d'information stratégiques avec tout ce que ceci comporte en termes de recherche fondamentale et appliquée, de techno science, de créativité industrielle, d'investissement public, d'effort financier et budgétaire et, finalement, de volonté politique. En sommes-nous réellement conscients, en sommes-nous capables ?

Du « Grand Jeu » au « Grand Échiquier », si les données n'ont pas changé, les méthodes se sont sophistiquées et les moyens multipliés de manière inimaginable, l'information — son acquisition, son traitement, son analyse, son exploitation — est au cœur de la mondialisation. Dans ce domaine comme dans d'autres, il faut à la GRANDE EUROPE une grande politique.

Ce document provient du journal *Libération* et date du 5 février 2003.

Ce que voient les espions, Jean-Dominique Merchet

Comment les différentes agences américaines recueillent des renseignements et, parfois, se fourvoient, ne voient rien, et surtout ne disent rien.

Le renseignement n'est pas une science exacte. En dépit des moyens considérables dont ils disposent, les services américains sont à la merci de fourvoiements, graves ou parfois cocasses.

[139] Il est vrai qu'il y a des failles. Les événements du 11 septembre l'ont montré. L'Histoire dira peut-être un jour si ce sont les systèmes de renseignement qui ont fait défaut, ou si c'est l'exploitation de leurs informations au plus haut niveau qui a échoué. C'est tout le problème de ce que les experts du renseignement appellent le « *basic missing link* ».

Ainsi, en mai 1998, la CIA n'avait absolument pas vu venir les essais nucléaires indiens — un pays dans lequel il est pourtant plus commode de travailler que dans l'Irak de Saddam Hussein. Ne pas voir... ou trop en voir.

« Dans les années 70, des photos aériennes montraient des filets sur les côtes cubaines, raconte l'historien Alexis Debat, qui prépare un ouvrage sur la CIA. Pour les experts, il s'agissait d'un camouflage de batteries antiaériennes. On s'est finalement aperçu que c'était simplement des filets de pêcheurs mis à sécher ! » Trop en voir et parfois même forger des informations de toutes pièces. Comme en février 1954, lorsque la CIA avait déposé des armes soviétiques sur les côtes du Nicaragua pour attirer l'attention sur le danger communiste en Amérique centrale.

Ces échecs et ces coups tordus ne doivent pas masquer les vrais succès. Ceux-ci sont rarement publics, car les « services » travaillent « pour les yeux seulement » des gouvernements. Comme mercredi à New York, les États peuvent choisir de mettre des informations classifiées sur la place publique.

Devant le Conseil de sécurité des Nations Unies, les États-Unis l'avaient déjà fait... le 22 octobre 1962. L'ambassadeur américain Adlaï Stevenson avait alors montré les photos des missiles russes installés à Cuba. Au grand dam de Valerian Zorine, l'ambassadeur soviétique, qui niait l'évidence.

En règle générale, les « services » n'aiment guère voir leurs renseignements utilisés ainsi. Car s'ils en apprennent un peu à l'opinion publique, ils en révèlent surtout beaucoup au pays espionné. Non pas sur le fond, mais sur la manière dont les informations sont recueillies. En révélant des conversations téléphoniques, une agence spécialisée comme la NSA (National Security Agency) indique à l'Irak le type de lignes téléphoniques sécurisées qu'elle est capable d'écouter et de décrypter.

Évidemment, les Irakiens cesseront aussitôt d'utiliser ses lignes, privant les États-Unis de nouvelles informations.

Depuis des semaines, la CIA et les autres agences traînaient les pieds, refusant de lâcher publiquement leurs renseignements. La présence du patron de la CIA, George Tenet, aux côtés de Colin Powell, indique que la Maison Blanche a finalement donné des ordres qui ne se discutaient plus.

Cela ne suffira pas à aplanir les profondes différences d'analyse entre les agences spécialisées américaines. D'un côté, les militaires de la Defence Intelligence Agency (DIA) sont les plus va-t'en guerre. Leurs principales sources sont les exilés et les opposants irakiens, « *dont les informations sont peu fiables* », constate un spécialiste européen. Plus modérée dans ses conclusions, la CIA travaille surtout avec d'autres services de renseignements bien implantés en Irak : ceux de Jordanie, d'Israël, de Russie et même d'Iran.

Reste le renseignement technique, avec toutes les limites qu'on lui connaît. Contre l'Irak, les États-Unis utilisent toute leur panoplie. Les satellites Key-Hole (photos et infrarouge) et Lacrosse (radar) scrutent le pays, alors que les grandes oreilles de la NSA écoutent sans relâche les communications. Mais Big Brother n'existe pas. Gros comme un autobus, un satellite KH-11 permet de compter les bidons que transporte une camionnette, mais pas de savoir ce qu'ils contiennent. Et la NSA bute toujours sur les informations qui transitent par fibre optique. Une tâche d'autant plus compliquée que les Irakiens, aidés par les Yougoslaves, sont passés maîtres dans l'art russe de la « maskirovska », le camouflage. Le renseignement fournit rarement des preuves, seulement la « meilleure vérité ».

Ce document provient du site du *Monde.* Il date du 7 février 2003.

Comment semer la zizanie à Washington, avec un AK-47 et un peu de cocaïne, Jacques Isnard

Le professeur Christopher Simpson, de l'American University de New York, pouvait-il se douter que la National Security Agency (NSA), la plus grande agence de renseignement des États-Unis, s'irriterait de ses propos révélant quelques-uns des mots-clés grâce auxquels le réseau d'espionnage Echelon écoute la planète entière ? Ses indiscrétions, en tout cas, ont eu de redoutables effets, qui expliquent la colère des responsables de la NSA, une agence fédérale que dirige le général Michaël Haydon depuis Fort George

Meade, dans le Maryland, et qui emploie 38000 personnes à travers le monde, aux États-Unis, bien sûr, mais aussi au Canada, au Royaume-Uni, en Australie et en Nouvelle-Zélande, pour s'en tenir aux sites principaux.

Selon un spécialiste de l'espionnage, Jacques Baud, la NSA contrôle une vraie « multinationale » du renseignement, baptisée Echelon, « qui a fait éclater la notion traditionnelle d'écoutes téléphoniques ».

Ce réseau peut intercepter l'ensemble des transmissions et transferts de données (fax, email, télex, téléphone) qui transitent par le moyen des satellites de communication dans le monde et dont le contenu est conservé sous forme de bibliothèques informatiques. Une cinquantaine de puissants ordinateurs, du type Super-Cray, traitent et analysent en temps utile les informations ainsi recueillies, en se servant d'un dictionnaire, distribué aux agents d'exploitation dans les stations, qui contient des mots-clés permettant à un logiciel spécial, dénommé Oratory, d'aller repérer automatiquement le message intéressant dans la galaxie des communications interceptées.

Echelon ramène, dit-on, chaque demi-journée, l'équivalent en information de toute la bibliothèque du Congrès américain, soit 1 000 milliards de bits. Les mots-clés, une fois identifiés, servent à sélectionner, dans les messages, l'information de nature diplomatique, économique, militaire ou autre, voire privée, qui est censée intéresser le gouvernement fédéral. Le professeur Simpson a livré quelques-uns de ces mots-clés. « AK-47 » (l'autre nom du fusil d'assaut Kalachnikov), « Cocaïne », « Stinger » (du nom du missile antiaérien portable), « TWA 800 » (l'identification du vol du Boeing qui a explosé au-dessus de l'Atlantique en 1996), « Militia », « Davidian » (le surnom de la secte de Waco en 1993) ou « Vince Foster » (un ami de Bill Clinton travaillant à la Maison Blanche qui s'est donné la mort en 1993) constituent autant de mots-clés qui permettent aux ordinateurs de la NSA de gagner du temps, dès qu'ils sont détectés dans la traque des messages qui auraient un rapport, par exemple, avec le commerce des armes, le trafic de drogue, des actes de terrorisme ou avec de mystérieux « proches » de M. Clinton.

Depuis, et c'est ce qui explique la colère de la NSA, ces mots-clés sont repris par des services secrets étrangers, des chancelleries ou par des particuliers « internautes » qui en émaillent systématiquement leurs communications ou leurs conversations. Avec cet espoir — jubilatoire — de saturer les ordinateurs de la NSA, de prendre à son propre piège tout le réseau américain d'espionnage et de perturber, en les noyant sous les messages à décrypter, le travail des analystes attachés à Echelon. Plus qu'un jeu, sans doute, c'est un moyen utilisé pour déclencher inutilement l'interception, le tri et l'exploitation du renseignement ainsi réuni. Nul ne doute que la NSA cherche déjà à inventer la parade à cette « cyberwar ».

Ce document vient de *Valeurs Actuelles*, n°3413 paru le 26 Avril 2002. Il met en garde les entreprises françaises sur les liens unissant les cabinets de conseil US et l'administration fédérale américaine.

Consultants : Attention aux Américains !

Une entreprise française ou européenne peut-elle faire confiance aux sociétés américaines spécialisées ? Rappel de quelques réalités pratiques avant de signer un contrat.

Les grands cabinets américains de sécurité ont un argument choc face à la concurrence européenne, et française en particulier qui est celui de la richesse des services qu'ils offrent. Appuyées sur un vaste champ d'expérience, leurs méthodes de travail permettent de répondre efficacement et discrètement aux exigences de leurs clients.

À l'instar de *Pinkerton*, ils renouent avec la tradition des premiers cabinets d'enquêtes aux États-Unis. La qualité du renseignement économique est l'un de leurs atouts. Les sociétés y baignent dans une culture de guerre et de sécurité économique propre aux États-Unis.

Les relations nouées entre les cabinets d'analyse de risques et l'administration fédérale sont clairement établies. Origine de la plupart des collaborateurs de ces sociétés l'illustre : NSA, NRO, CIA, FBI.

Beaucoup d'entre eux sont encore assermentés auprès de leur service d'origine pour des questions de défense et de sécurité. Ces transfuges du monde du renseignement passés au monde économique illustrent le durcissement des relations économiques internationales.

Aux États-Unis, de nombreux cadres des agences fédérales ont rejoint des postes clés dans de grandes multinationales comme 3M, Kodak, ATT ou McDonnell Douglas. Le 14 janvier dernier, Larry Cockell, directeur adjoint du Secret Service (chargé notamment de la protection des plus hautes personnalités politiques fédérales), a été nommé directeur de la sécurité et vice-président du groupe AOL-Time Warner.

La SCIP (Society of Competitive Intelligence Professionnels), forte de plus de cinq mille membres, compte dans ses rangs beaucoup d'ex-cadres des services spéciaux. La majorité s'est reclassée dans le consulting dans des cabinets prestigieux, dans l'industrie chimique et pharmaceutique et dans les technologies de pointe. Les passerelles entre le gouvernement fédéral et le secteur privé sont nombreuses, comme le démontre le journaliste d'investigation écossais Duncan Campbell, spécialiste du système Echelon d'écoutes et d'interceptions planétaires, auteur du livre *Surveillance électronique planétaire*.

Les agences fédérales américaines concentrent leurs efforts sur la collecte des renseignements économiques, œuvrant ainsi au succès des entreprises outre-Atlantique en livrant quasiment à la demande des informations aux sociétés. Ces études fouillées sont très loin du simple « avis d'opportunité » que ces agences assurent livrer aux entreprises. Il s'agit d'un soutien actif.

C'est ainsi qu'au nom de la lutte antiterroriste le Sénat américain n'a pas hésité à voter le Patriot Act[140], le 24 novembre 2001 : ce texte vise à renforcer les moyens d'écoutes, de surveillance et de contrôle

[140] Tout d'abord l'intitulé de l'USA Patriot Act :
« *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* » (Unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme).
Cet intitulé indique très précisément sa nature et son esprit : cette loi autorise l'arrestation, la déportation et la mise à l'isolement de suspects. Elle supprime toute délégation judiciaire (l'autorisation préalable d'un juge) pour procéder à des perquisitions, à des écoutes téléphoniques ou contrôler le courrier et les communications par Internet.
Le 21 juillet 2005, la Chambre a approuvé à une large majorité la prolongation de l'application des mesures du Patriot Act par 257 voix contre 171. Parmi les seize dispositions du Patriot Act venant à expiration au 31 décembre 2005, quatorze devraient ainsi être rendues permanentes. Les deux autres dispositions, concernant les écoutes téléphoniques et l'accès aux fichiers personnels comme les emprunts dans les bibliothèques, devraient être prolongées pour 10 années, alors qu'une série d'amendements ont été adoptés pour apporter des garanties dans l'application de la loi. Le jeudi 17 août 2006, la juge fédérale américaine Anna Diggs Taylor a déclaré inconstitutionelles ces écoutes téléphoniques et a ordonné l'arrêt immédiat du programme secret de surveillance intérieure mené par l'Agence nationale de sécurité.
Le Sénat s'est également prononcé favorablement sur la prolongation du Patriot Act le 29 juillet 2005. Le vote est intervenu par une procédure de « consentement unanime », sur base d'un texte préparé par la commission des affaires judiciaires. Il n'y a pas eu de débats ni de dépôt d'amendement, les démocrates (le parti minoritaire) ayant approuvé le document préparatoire en commission, estimant notamment que ce texte donnait un rôle accru à la justice pour contrôler l'action des services de police. De plus, alors que la Chambre avait voté pour une prolongation de deux dispositions durant dix ans, le Sénat lui se prononce pour une prolongation de quatre ans. Les deux versions du texte, celle de la Chambre et celle du Sénat, devaient être harmonisées avant que seize des dispositions de cette loi ne viennent à expiration le 31 décembre 2005. La plus grande organisation de défense des droits civiques du pays, l'American Civil Liberties Union (ACLU), a salué les garanties apportées par le Sénat, tout en regrettant qu'elles n'aillent pas encore assez loin.
Après un vote définitif d'acceptation de la Chambre, le Sénat américain a bloqué le 15 décembre 2005, dans le cadre d'une technique de blocage du vote dite, en anglais, « filibuster », la reconduction du Patriot Act. Le texte d'harmonisation réalisé au départ des dispositions votées par la Chambre et le Sénat en juillet 2005 prévoyait *in fine* que quatorze des seize dispositions venant à échéance devenaient permanentes, tandis que les deux autres devaient être prorogées jusqu'en 2009. Le blocage du Sénat a été levé, le 21 décembre, à la suite d'un accord prorogeant les dispositions du Patriot Act actuel pour 6 mois à compter du 31 décembre 2005, afin de continuer les négociations. Mais lorsque le texte est revenu une dernière fois à la Chambre, le 22 décembre, pour valider cet accord concernant la prorogation de six mois, une nouvelle proposition est apparue : prolonger le Patriot Act actuel de seulement cinq semaines, jusqu'au 3 février 2006. La Chambre haute du Congrès où siègent sénateurs et députés a avalisé cette dernière proposition et le président Bush l'a entérinée. Cependant, la situation restant bloquée, le premier février 2006, la Chambre vote une nouvelle prolongation de cinq semaines, jusqu'au 10 mars 2006. Le Sénat a ensuite approuvé cette proposition puis le président Bush a signé le texte de prolongation du Patriot Act dans sa version actuelle

des communications du territoire national par l'emploi du système Carnivore (rebaptisé DCS 1000), complément amélioré du système Echelon. Le Patriot Act est un pas de plus dans la tentative de maîtrise totale de l'information.

Les cabinets américains sont au cœur de cette machine politico-financière dont les entreprises françaises sont bien souvent les cibles. C'est pourquoi il serait naïf de feindre d'ignorer la partialité de ces sociétés qui, ne perdent jamais de vue l'intérêt national des États-Unis.

Ce document est un dossier de *Courrier International* ; il portait comme introduction :

Créé en 1947, le réseau d'écoute « Echelon » devait intercepter les télécommunications du bloc de l'Est. Depuis la chute du Mur, ce réseau serait utilisé par les États-Unis et leurs partenaires à des fins d'espionnage commercial.

Le parlement européen s'est saisi de la question. Elle sera à l'ordre du jour du conseil des ministres de l'Intérieur de l'Union européenne le 29 mai. En France, l'Assemblée nationale souhaite aussi ouvrir une enquête.

Echelon : *les plus grandes oreilles du monde*

Enquête sur un réseau secret d'espionnage anglo-saxon.

Dans le cadre du pacte UKUSA, chapeauté par la NSA — une agence indépendante, placée sous la responsabilité du directeur de la CIA —, les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande, filtre conversations téléphoniques, fax et emails dans le monde entier.

Surveillance du contenu des messages électroniques, écoutes téléphoniques, satellites-espions. On sait depuis longtemps que le système de télécommunications utilisé chaque jour par les particuliers, les entreprises, mais aussi les ambassades ou les gouvernements n'est pas d'une confidentialité à toute épreuve. On sait aussi que l'on s'espionne et que l'on se contrôle entre pays amis et alliés.

Tout cela fait partie d'un jeu complexe et délicat d'après-guerre froide, dans lequel chacun est plus ou moins ami et concurrent de tous. On sait encore qu'il y a un joueur plus malin et plus fort que les autres : les États-Unis. Mais, jusqu'à présent, seuls quelques dirigeants et spécialistes connaissaient l'existence d'un réseau de surveillance globale d'une puissance et d'une étendue extraordinaires, que les États-Unis gèrent avec la collaboration de quatre autres pays anglophones : le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.

Son existence a été très récemment révélée par un rapport officiel du *Scientific and Technological Options Assessment* (STOA — Commission d'évaluation des choix technologiques et scientifiques, présidée par Alain Pompidou) de la Direction générale de la recherche au Parlement européen. Intitulé « Évaluation des technologies de contrôle politique », ce texte décrit le mécanisme. « *En Europe, tous les appels téléphoniques, les fax et les textes transmis par courrier électronique (emails) sont régulièrement interceptés, et les informations présentant un intérêt quelconque sont retransmises par le centre stratégique britannique de Menwith Hill vers le quartier général de la National Security Agency (NSA), l'agence américaine d'espionnage électronique.* »

Selon ce document, tous les appels, cryptés ou non, peuvent être sélectionnés, décodés et intégrés dans une très puissante banque de données commune aux cinq pays en question.

Cet incroyable aspirateur à communications, baptisé Echelon, est le fruit de la technologie mise au point par l'UKUSA Security Agreement, un pacte de collaboration pour la collecte de Signal Intelligence

jusqu'au 10 mars 2006. La Chambre des représentants américaine a définitivement adopté, le 7 mars 2006, par une majorité de 280 voix contre 138, la version définitive d'un texte reconduisant les mesures antiterroristes de la loi *Patriot Act*, marquant l'épilogue d'un difficile débat sur les moyens de la guerre contre le terrorisme. Ce vote permet au président George W. Bush de pérenniser la plupart des moyens accordés aux forces de l'ordre pour leurs enquêtes antiterroristes depuis la loi adoptée cinq semaines après les attentats du 11 septembre 2001.

(renseignement électronique), conclu en 1948 et dont l'existence n'a jamais été officiellement confirmée par ses participants. « *Le plus frappant, c'est que pendant toutes ces années aucun gouvernement, dans aucun des cinq pays membres, n'a jamais rien dit ou admis à propos de ce pacte* », dit le chercheur Nicky Hager, auteur de *Secret Power*, un livre publié en Nouvelle-Zélande qui rompt pour la première fois le silence sur UKUSA et sur Echelon.

Source : *Il Mondo* (08/04/1998)

Une véritable mainmise sur British Telecom.

Le Royaume-Uni est traditionnellement tiraillé entre son appartenance à l'Union Européenne et ses liens privilégiés avec les États-Unis. Mais, avec le système Echelon, on passe de l'ambivalence au conflit d'intérêts. Directeur de *Privacy International*, organisation qui lutte pour la défense des droits civiques, l'Anglais Simon Davies, en visite à la London School of Economics, est le premier à le reconnaître.

Croyez-vous qu'au nom de l'UE Londres puisse renoncer à son rapport préférentiel avec les États-Unis ?

Simon Davies : Non, c'est pratiquement impossible : ce rapport est trop étroit. En matière de sécurité nationale notamment, un éventuel retrait d'UKUSA provoquerait un choc épouvantable.

— A Bruxelles et dans les capitales européennes, le rapport du Parlement de Strasbourg n'a guère provoqué de réactions. Comment l'expliquez-vous ?

— La logique des activités d'espionnage veut que la sécurité nationale soit sacrée, donc qu'elle reste libre de toute interférence. Tant que l'on considérera Echelon comme un système lié à la sécurité nationale, personne n'osera dire quoi que ce soit. De plus, Echelon reste mystérieux. On commence à mieux comprendre son fonctionnement, mais on a du mal à en saisir l'ampleur.

— Qu'en savez-vous aujourd'hui ?

— Le moindre appel téléphonique, le moindre fax ou message électronique partant par onde ou par câble d'Italie vers le Royaume-Uni (et vice versa) peut faire l'objet d'une interception. N'importe quelle télécommunication par satellite peut l'être aussi. Le plus important, c'est qu'Echelon est loin d'être statique. Le système évolue parallèlement à la technologie. Le moindre progrès du réseau de télécommunications international, le moindre changement entraînent un réajustement d'Echelon.

Prenez la base d'UKUSA de Menwith Hill, en Cornouailles. Elle s'est développée jusqu'à devenir partie intégrante des télécoms britanniques. Chaque fois que British Telecom (BT) a procédé à une modification, il a d'abord consulté Menwith Hill, qui s'est adapté. Et, chaque fois que BT a dû modifier son infrastructure, il a demandé l'accord du Service de renseignement électronique. Si Londres veut vraiment poursuivre le processus entamé à Maastricht, tout cela doit cesser.

Source : *Il Mondo* (08/04/1998)

Deux millions de conversations captées à la minute.

Glynn Ford (de la Direction générale de la recherche, au Parlement européen) accuse : *des sociétés américaines ont profité du système* Echelon *pour contrer leurs concurrents européens et nippons*.

Selon le rapport STOA, « en Europe, tous les emails, fax et appels téléphoniques sont contrôlés systématiquement par la NSA ». Vous confirmez ?

Glynn Ford : D'après ce que j'ai pu comprendre, les communications sont interceptées grâce à des réseaux satellites. Des ordinateurs permettent de tout surveiller de façon systématique. Ce qui ne veut pas dire que toutes les conversations téléphoniques sont interceptées. Mais il existe des ordinateurs capables de surveiller deux millions de conversations par minute.

— Qu'est-ce qui vous choque le plus ?

— Greenpeace et Amnesty International figurent parmi les mots clés du système Echelon. Je comprendrais pour le terme Armée rouge, mais pourquoi écouter des conversations qui évoquent Greenpeace ou Amnesty ?

— Que pensez-vous du fait que les téléphones portables servent aussi à espionner la population ?

— Ce n'est pas le fait d'utiliser des appareils mobiles pour surveiller des individus suspects qui me dérange. Le problème, c'est que ce type de surveillance a été étendu à l'échelle mondiale de façon sauvage. On ne parle plus d'un nombre limité de « cibles » ; n'importe quelle organisation peut être surveillée. C'est pourquoi il faut instaurer un organisme de contrôle, qui pourrait dresser une liste de « cibles », définir les catégories de personnes ou de groupes susceptibles d'être surveillés et, enfin, s'assurer que les informations recueillies sont bien utilisées à des fins légitimes, et non illégales comme c'est souvent le cas. Apparemment, des informations captées par les États-Unis ont été exploitées par des sociétés américaines au mépris des lois de la concurrence et aux dépens de sociétés européennes et japonaises.

— Que comptez-vous faire dans l'immédiat ?

— La Commission des libertés civiques du Parlement européen a réclamé une enquête sur le système Echelon et ses retombées en Europe. Dans quelques semaines, nous devrions décider à qui confier cette enquête.

Source : *Il Mondo* (08/04/1998)

Echelon *et les secrets des grandes oreilles*

Les pratiques de la National Security Agency, l'agence américaine chargée d'intercepter les communications — avec notamment son programme Echelon —, posent des questions inquiétantes, restées jusqu'à présent sans réponse.

Des congressistes américains, le Parlement européen et des groupes de défense des libertés civiques commencent à poser des questions embarrassantes sur l'interception par la National Security Agency (NSA) des appels téléphoniques, des fax et des courriers électroniques à l'étranger. Depuis un rapport soumis l'année dernière aux représentants des quinze pays siégeant au Parlement européen, l'inquiétude de l'opinion publique n'a cessé de croître au sujet d'Echelon, le nom de code désignant le réseau mondial de surveillance mis en place par la NSA et ses partenaires au Royaume-Uni, en Australie, au Canada et en Nouvelle-Zélande. [...]

Les inquiétudes d'un autre élu républicain, Robert L. Barr, eurent leur écho en Europe avec la publication d'un second rapport encore plus détaillé sur la surveillance électronique, adressé cette fois à l'Union européenne. L'auteur, le journaliste et physicien britannique Duncan Campbell, y écrivait que non seulement les États-Unis, mais des dizaines de pays ont désormais la capacité d'intercepter « *tout type moderne de communication à haut débit* », y compris les messages papier, les appels de téléphones mobiles et le courrier électronique sur Internet. Campbell ajoutait que « *les gouvernements de grands pays ont régulièrement recours à l'interception des communications afin d'assurer des avantages commerciaux à certaines entreprises* ». Mais il notait également dans son rapport que la NSA et d'autres agences d'espionnage s'efforçaient de trouver la parade à l'utilisation croissante du cryptage, des fibres optiques et d'autres nouvelles technologies. « *Cette histoire d'*Echelon *satisfait un besoin largement répandu de croire que le gouvernement échappe à tout contrôle* », souligne Steven Aftergood, directeur d'un projet de recherche sur le secret gouvernemental mené par la *Federation of American Scientists*, un organisme indépendant. « *Mais derrière cela est posé un problème politique important, à savoir que lorsqu'un nombre significatif de citoyens américains s'inquiètent d'une question politique concernant les activités de renseignement, ils sont en droit de recevoir une réponse. Or, jusqu'ici, ils n'en ont pas eu.* »

Source : *The Washington Post* (09/12/1999)

Ce document vient d'*Amnistia* et date du 9 mars 2001. Il s'agit d'un des éléments d'un dossier intitulé « *USA : la conquête de l'Europe* ».

Echelon *et le business US*

« Je ne sais pas si ce système s'appelle Echelon ou pas, mais une chose est sûre, un tel système existe et il permet d'écouter au niveau planétaire toutes les conversations effectuées à travers tous les systèmes de télécommunication habituels. Cela dit, nous ne disposons d'aucune preuve que ce système a été utilisé par les États-Unis pour fournir des informations économiques réservées à leurs propres entreprises ».

Voici les conclusions que Gerhard Schmid, rapporteur de la commission d'enquête du Parlement européen sur « *le cas* Echelon » a présentées à la presse lors d'une conférence qu'il a donnée mercredi 7 mars à Bruxelles.

« Pour mettre en œuvre un tel système d'interception mondial, il faut impérativement disposer d'au moins trois bases d'écoute. Une située sur l'Océan Atlantique, une deuxième sur l'Océan Indien et une troisième sur l'Océan Pacifique. Et, nous savons que dans toutes ces zones géographiques il existe des bases d'écoute gérées par les États-Unis ».

Nous pouvons rajouter que ces bases d'écoutes, dont la création remonte à l'immédiat après-guerre lors de la signature, en 1947, de l'accord UKUSA entre le Royaume-Uni (UK), les États-Unis (USA), le Canada, l'Australie et la Nouvelle-Zélande, n'ont cessé de se multiplier.

Quant à « l'absence de preuves » concernant l'utilisation des interceptions à des fins commerciales pour favoriser les intérêts des entreprises américaines, cela nous fait penser à une délicieuse esquive diplomatique de la part du rapporteur parlementaire européen. Les exemples concernant l'utilisation des informations interceptées par les services secrets américains à des fins commerciales sont bel et bien multiples et... publics !

En effet, il suffit de se procurer le rapport IC 2000 (*Interception Capabilities* de Duncan Campbell édité en France par les éditions Allia sous le titre *Surveillance électronique planétaire*) qui fut présenté au Parlement européen en février 2000, pour lire que : « *Des rapports publiés par le Bureau de soutien du Département du Commerce US dressent la liste de centaines de contrats où le gouvernement américain affirme avoir remporté des marchés au détriment de concurrents étrangers en intervenant dans l'intérêt du commerce américain* ».

Tableau 2: Contrats remportés grâce à la politique américaine de "soutien"

ANNÉE	SECTEUR INDUSTRIEL	PAYS ACHETEUR	VALEUR (MILLIONS DE $)	COMPAGNIE AMÉRICAINE VICTORIEUSE	GROUPE FRANÇAIS OU EUROPÉEN VAINCU
1994	Protection environnementale SIVAM	Brésil	1 400	Raytheon	Thomson CSF
1994	Satellites de télécommunications	Arabie Saoudite	4 000	AT&T	"Dure compétition des français"
1994	Câbles de fibres optiques FLAG	International	1 400	Nynex	"Dure compétition d'un consortium de la France et de Singapour"
1994	Electricité – Paiton	Indonésie	2 600	Mission Energy	Non spécifié
1995	Electricité	Tunisie	120	General Electric	"Compétition intense de firmes françaises"
1995	Avions de ligne	Arabie Saoudite	6 000	Boeing et Mac-Donnell Douglas	Airbus Industrie
1995	Télécommunications – MILNET	Emirats Arabes Unis	119	AT&T	Alcatel
1996	Incinération d'ordures	Taïwan	226	Westinghouse Electric	"a vaincu.... un oligopole européen"
1996	Environnement	Liban	0,3	Ecodit	Anglais, Néerlandais, Danois, Français
1996	Electricité	Israël	300	Mid Atlantic Energy	"Compétition intense de compagnies européennes"
1997	Système de contrôle du trafic aérien	Pérou	12	Northrop Grumman	Thomson CSF

Le 3 décembre 1995, soit deux ans avant que les parlementaires européens ne se penchent pour la première fois sur le cas « Echelon », le *Baltimore Sun* révélait qu'« *à partir d'un satellite de communications commerciales, la NSA s'empara de tous les fax et appels téléphoniques entre le consortium européen Airbus, la compagnie aérienne nationale de l'Arabie Saoudite et le gouvernement saoudien. L'agence découvrit que les agents d'Airbus offraient des pots-de-vin à un officiel saoudien. Elle transmit l'information aux officiels américains qui appuyaient l'enchère de Boeing C°. et McDonnell Douglas Corp., lesquels triomphèrent l'année dernière (1994) dans la compétition à six milliards de dollars* ».

Toujours en 1994, Thomson CSF était sur le point de conclure un contrat avec l'état du Brésil. Il s'agissait de la mise en œuvre d'un système de surveillance pour la forêt amazonienne.

Soudainement, les Brésiliens changèrent d'avis et confièrent ce marché à l'entreprise américaine Raytheon Corporation, qui se trouve être un des principaux partenaires de la NSA dans le système Echelon. « *Le Département du Commerce a travaillé dur pour soutenir l'industrie américaine dans ce »projet* » peut-on lire dans le dossier de presse de la Raytheon Corporation, qui est fièrement affiché sur leur site web. Effectivement, la NSA avait intercepté des appels téléphoniques entre Thomson et le Brésil. L'entreprise française fut accusée par les Américains d'avoir corrompu des membres du comité de sélection du gouvernement brésilien, et voilà comment ce contrat estime à 1,4 milliard de dollars atterrit directement dans la poche de la Raytheon Corporation. En toute transparence.

Ce document provient du journal « *Le monde du Renseignement* », Numéro 405, en date du 10 mai 2001.

La place de la NSA en Europe

Depuis ce 25 avril, la célèbre plaisanterie qui consistait à traduire l'acronyme NSA par la formule « Never Say Anything » appartient définitivement au passé. Comme l'annonçait en exclusivité *Le Monde du Renseignement* dès le 8 février, les derniers documents de l'enquêteur James Bamford, sortis ce jour-là, révèlent des pans entiers de l'histoire de l'agence de renseignement souvent parfaitement inconnus. Un coup de maître. Après avoir publié en 1982 *Puzzle Palace* : le premier livre à présenter globalement les activités de la NSA, Bamford réitère donc avec *Body of Secrets* (disponible aux États-Unis, ISBN : 0385499078), premier ouvrage du genre à énumérer très précisément les missions les plus importantes menées par la NSA au cours des trente dernières années. Ses descriptions s'appuient sur quantité de documents confidentiels, et sur plusieurs témoignages d'anciens officiers.

Alors que la Commission temporaire sur le système Echelon du Parlement européen se déplace cette semaine à Washington pour entendre des responsables politiques au sujet des écoutes effectuées par l'agence sur des décideurs européens, ces révélations fournissent quantité d'arguments à ceux qui souhaitent un large débat sur la portée des moyens de la NSA.

À propos des types d'objectifs assignés à l'agence de renseignement, Bamford lève un tabou en confirmant l'existence d'opérations de surveillance sur des sociétés et des diplomates de pays alliés. Évoquant les tensions récurrentes entre la France et les États-Unis sur ces questions d'espionnage, il explique que les communications des membres de la diplomatie française sont régulièrement et massivement interceptées. Selon lui, dans les rapports d'écoutes de l'agence qui retranscrivent les communications, celles-ci sont désignées par les lettres FRD (pour French Diplomatie).

Au sujet des entreprises, *Body Secret* reconstitue les opérations exécutées par la NSA contre la firme *Microturbo SA*, installée à Toulouse, dans le sud-ouest de la France. Une société de haute technologie, spécialisée dans la conception de turbines à gaz de très faibles dimensions, généralement employées pour les missiles ou les drones. Les dirigeants de cette filiale de la Snecma ont été placés sous surveillance par la NSA de mai à novembre 1997. Pour les personnalités proches de l'agence interrogées par Bamford, cette opération s'expliquait par une vente de turbines à l'Iran réalisée par *Microturbo* dans les années 80,

et destinée à équiper des missiles que Téhéran venait d'acquérir en Chine. Explication étonnante... Pour des écoutes diligentées dix ans après les faits censés les justifier.

Pourtant, à la même époque, d'autres activités de *Microturbo SA* ne manquaient pas d'intéresser le Pentagone — donneur d'ordre de la NSA. Ainsi, entre mai et novembre 1997, l'entreprise développait le système de propulsion du futur missile de croisière Scalp EC. Un engin novateur dont l'ensemble des composants dépend d'industriels européens, donc commercialisable à l'export sans négociations préalables avec des pays tiers.

Parmi les nombreuses autres révélations du document de James Bamford : les liens très particuliers de la NSA avec *Cisco*, leader mondial des systèmes de routage pour Internet. Le quartier général de Fort Meade considère en effet cet industriel comme une cible prioritaire, puisqu'il gère aujourd'hui la majeure partie des nœuds de communication (les routeurs) de la planète sur lesquels fonctionne l'lnternet.

À cet égard, le travail de l'agence consiste depuis plusieurs années à implanter et entretenir des systèmes de « reverse engineering », c'est-à-dire des dispositifs d'interception agissant directement au niveau de ces entonnoirs de communication que constituent les routeurs pour un pays ou un continent.

Pour preuve des fortes relations de confiance existant entre la multinationale et l'agence étatique, Bamford cite le cas d'un ingénieur de *Cisco*, récemment recruté par la NSA comme conseiller senior, afin de coordonner le programme de modernisation de ses systèmes d'écoutes, répondant au nom de code de *Project Trailblazert*.

Ce document portait comme indication « *Extraits d'un article paru dans Junge Freiheit*, n°26/99 ».

Quand les alliés des États-Unis sont aussi (et surtout) leurs concurrents : *Le rôle d'espionnage universel d'*Echelon.

Début 1998, Steve Wright, membre d'OMEGA, une association britannique pour les droits des citoyens basée à Manchester, constate dans un rapport qu'il adresse au Parlement Européen, que tous les courriers électroniques, les conversations téléphoniques et les fax sont enregistrés par routine par le service de renseignement américain NSA (National Security Agency). La NSA fait suivre toutes ces données récoltées en Europe à l'adresse du Quartier Général de la NSA aux États-Unis, à Fort Meade dans le Maryland. Avec raison, Wright conclut que la NSA a installé un système de surveillance global, dont le but est de sonder les satellites par lesquels transite la plus grande partie des communications internationales. À la différence des systèmes de surveillance électroniques, utilisés lors de la guerre froide pour sonder des organismes militaires, le système de surveillance Echelon sert essentiellement à espionner des cibles civiles : des gouvernements, des organisations de toutes sortes ou des entreprises commerciales ou industrielles.

Quatre pays, explique Wright, se partagent, avec les États-Unis, les résultats de cet espionnage global : la Grande-Bretagne, le Canada, la Nouvelle-Zélande et l'Australie. Les services secrets de ces quatre pays n'agissent en fait que comme fournisseurs subalternes de renseignements. En d'autres termes : seuls les Américains contrôlent complètement le réseau d'espionnage Echelon. Ensuite, dans le rapport de Wright, on apprend également que la plus grande station d'écoute du monde se trouve à Menwith Hill, en Angleterre dans le Comté du Yorkshire. Cette station serait en mesure d'écouter la plupart des communications en Europe et dans les pays de l'ex-URSS

Dans ce rapport de Wright, pour la première fois, on apprend officiellement dans l'Union Européenne (UE) qu'un système d'écoute global et électronique, dont le nom est Echelon, existe ! Pendant des années, seules des informations fortuites et superficielles circulaient à propos d'Echelon.

Le premier à avoir parlé du concept même d' Echelon a été le journaliste britannique, spécialisé dans les affaires d'espionnage, Duncan Campbell. Dans un article pour le magazine New Statesman du 12 août 1988. Il y a onze ans, Campbell révélait qu' Echelon permettait de surveiller toutes les communications venant et arrivant en Grande-Bretagne, à la condition que cette surveillance serve l'intérêt

national ou favorise l'économie britannique. Récemment, Campbell a lui-même rédigé un rapport à la demande d'un groupe de travail de l'UE, le STOA (Scientific and Technological Options Assessments). Le titre de son rapport : *Interception Capabilities 2000* (soit : État des techniques d'écoutes en l'an 2000). Il traitait en détail d'Echelon. Les gouvernements décident de l'utilisation du matériel récolté

Campbell montre notamment dans son rapport que chaque État, participant à Echelon, a autorisé ses services secrets ou certains ministères, de consulter tout matériel récolté ayant une importance d'ordre économique ou de les commander. Grâce aux informations ainsi engrangées, des objectifs très divers peuvent être poursuivis. Campbell ajoute que la décision d'exploiter ou d'utiliser ces informations acquises par espionnage ne relève pas des services secrets impliqués, mais des gouvernements.

Ce rapport ne manque pas de piquant : en effet, la Grande-Bretagne est membre de l'UE et participe à l'espionnage généralisé de tous ses partenaires. Rappelons à ce propos deux faits : le journal anglais *The Independant* du 11 avril 1998 constate, vu la participation de la Grande-Bretagne à Echelon, que celle-ci participe à un consortium de services électroniques de renseignements, qui espionne systématiquement les secrets économiques et commerciaux des États de l'UE. Le journal citait l'avocat français Jean-Pierre Millet, spécialisé en criminalité informatique. *Les partenaires de la Grande-Bretagne*, disait Millet, *auraient raison d'en vouloir aux Britanniques, parce que ceux-ci n'ont pas abandonné leur coopération avec les Américains.*

Disons aussi en passant que la France, en matière d'espionnage économique, n'est pas un enfant de chœur. Ainsi, par exemple, l'ancien chef des services secrets français, Pierre Marion, avait déclaré que la guerre faisait toujours rage, y compris entre pays alliés, dès qu'il s'agissait d'affaires (cf. *Spectator*, 9 avril 1994).

La grogne des Français, dans ce contexte, se justifiait non pas tant parce que la Grande-Bretagne faisait partie du cartel d' Echelon, mais parce que la France ne pouvait pas participer à cette gigantesque machine globale à fouiner.

Le nom de code Echelon découle du terme militaire français « échelon ». Echelon a été au départ conçu par les services de renseignements pour surveiller l'Union Soviétique. Après l'effondrement de celle-ci, ce projet, qui a coûté des milliards, devait servir à combattre officiellement le terrorisme international. Mais cette justification n'est qu'un rideau de fumée, destiné à dissimuler le véritable objectif. D'après les informations dont on dispose, on peut désormais affirmer qu' Echelon a bel et bien été conçu prioritairement pour l'espionnage industriel et économique à grande échelle. L'allié militaire officiel peut être l'ennemi économique réel…

Dans un rapport du 29 mars de cette année, *Der Spiegel* évoquait que les termes-clefs, avec lesquels Echelon fonctionne, proviennent avant tout du domaine économique américain. Indice supplémentaire que les Américains ne se gênent nullement pour combattre les concurrents étrangers de leurs entreprises par tous les moyens, même illicites. Cela leur est complètement égal de savoir si la firme espionnée appartient à un pays allié ou ennemi.

Deux auteurs ont bien mis cela en exergue, Selig S. Harrison et Clyde V. Prestowitz, dans un article du périodique *Foreign Policy* (79/90) : les alliés militaires des États-Unis sont ses ennemis économiques. Il est fort probable que les États-Unis nieront qu'une rivalité fondamentale les oppose aux autres puissances occidentales sur les plans des relations commerciales internationales, ce qui les empêchera, par la même occasion, de réagir adéquatement au niveau des règles de la concurrence.

L'ancien directeur du FBI, William Sessions, voit les choses de la même façon : dans un entretien, il a expliqué qu'aujourd'hui déjà, et, a fortiori dans l'avenir, une puissance est ou sera l'alliée ou l'ennemie des États-Unis, non seulement selon les nécessités militaires, mais aussi et surtout selon les résultats des observations que les États-Unis obtiendront de leurs services de renseignement dans les domaines scientifiques, technologiques, politiques et économiques (cf. *Washington Times*, 30 avril 1992) (NDLR : autrement dit, aucune puissance européenne ou asiatique ne pourra désormais développer un program-

me de recherches scientifiques ou technologiques, et réussir des applications pratiques, sans risquer d'encourir les foudres des États-Unis et d'être décrite dans les médias comme « totalitaire », « dictatoriale », « communiste » ou « fasciste », ou « rouge-brune »).

L'espionnage scientifique renforce la mainmise politique. Philip Zelikov est encore plus clair dans son ouvrage *American Intelligence and the World Economy* (New York, 1996). La victoire dans la bataille pour être compétitif sur les marchés du monde est le premier point à l'ordre du jour dans l'agenda de la sécurité américaine.

Même vision chez Lester Thurow, célèbre économiste américain du MIT (*Massachusetts Institute of Technology*), auteur de *Head to Head* : *The Co-ming Battle between Japan, Europe and America* (New York, 1992). Sans s'embarrasser de circonlocutions, Thurow écrit que les États qui dominent les plus grands marchés définissent également les règles. Il en a toujours été ainsi. Raison pour laquelle les Américains refusent même aux États qui participent au réseau Echelon d'accéder à toutes les données récoltées.

Ce genre de restriction est également habituel. Ainsi, par exemple, Mark Urban, dans son livre *UK Eyes Alpha. The Inside Story of British Intelligence* (Londres, 1996), évoque la coopération entre les services secrets britanniques et américains et constate que les Américains n'ont jamais cessé de retenir des informations, de les garder pour eux seuls. Il s'agissait surtout des informations relatives aux affaires commerciales.

Ce détail et cette pratique de rétention expliquent les véritables motivations des Américains et de leurs partenaires dans le réseau d'écoute global Echelon. Pourtant, il serait inexact et insuffisant d'affirmer que le seul but d' Echelon est l'espionnage économique. Comme auparavant, l'intelligence militaire et politique occupe une large part des activités de ce réseau. En priorité, Echelon sert à faire valoir ses propres intérêts de manière plus efficace.

Les révélations du Néo-Zélandais Nicky Hager

D'après les explications du Néo-Zélandais Nicky Hager, qui, avec son livre *Secret Power*. *New Zealand's Role in the International Spy Network* (1996), a permis de mieux savoir comment fonctionnait Echelon, ce système d'espionnage n'est pas agencé de façon à contrôler et à copier chaque courrier électronique ou chaque télécopie. Le système vise plutôt à trier et à sonder de grandes quantités de communications électroniques. Les ordinateurs d' Echelon filtrent au départ de mots-clefs ou de concepts-clefs, consignés dans des « dictionnaires » et, à partir de la masse d'informations récoltées, trient ce qui est intéressant pour les divers services de renseignement.

Dans cette pratique, écrit Hager dans son article du magazine *Covert Action Quarterly* (56/96-97), le système de filtrage « Memex », élaboré par la firme britannique *Memex Technology*, joue un rôle primordial. Memex est en mesure de rechercher de grandes quantités de données au départ de concepts-clefs. Ces concepts-clefs englobent les noms de certaines personnalités, d'organisations, de désignations de pays ou de termes scientifiques ou spécialisés. Parmi ces concepts-clefs, on trouve les numéros de fax et les adresses électroniques de certains individus, d'organisations ou d'institutions étatiques.

Une chaîne mondiale d'installations d'écoute (comme, par exemple, Menwith Hill ou Bad Aibling en Bavière) a été placée tout autour du globe, pour pomper les réseaux internationaux de télécommunications. Echelon relie entre elles toutes ces installations d'écoute, qui permettent aux États-Unis et à leurs alliés de surveiller une bonne part des communications qui s'effectuent sur la Terre.

Ce qui est substantiellement nouveau dans Echelon n'est pas tant le fait que des ordinateurs sont utilisés pour exploiter des renseignements électroniques à l'aide de certains concepts-clefs (car c'était déjà possible dans les années 70), mais c'est surtout la capacité d'Echelon et de la NSA de pouvoir placer en réseau tous les ordinateurs mis en œuvre et cela, à grande échelle.

Cette mise en réseau permet aux diverses stations d'écoute de travailler comme autant de composantes d'un système global intégré. La NSA, le service secret néo-zélandais GCSB (*Government Communications Security Bureau*), le service secret britannique GCHQ (*Government Communications Head Quarters*), le service secret canadien CSE (*Communications Security Establishment*) et le service secret australien DSD (*Defence Signals Directorate*) sont les partenaires contractuels de l'UKUSA Signals Intelligence, un pacte entre les divers services de renseignements des puissances anglo-saxonnes. Cette alliance s'explique par ses origines : elle date de la coopération entre ces services pendant la Seconde Guerre mondiale. Au départ, elle visait à faire surveiller l'URSS par les services de renseignement.

Pomper les satellites

Grosso modo, Echelon poursuit trois objectifs : d'abord, contrôler les satellites permettant les communications internationales qu'utilisent les sociétés téléphoniques de la plupart des États du monde. Un anneau de tels satellites entoure la Terre. En règle générale, ces satellites sont positionnés à hauteur de l'Équateur. D'après ce que nous en dit Nicky Hager, cinq stations d'écoutes du réseau Echelon servent à pomper ce que contiennent ces satellites.

Deuxième objectif : espionner les satellites qui n'appartiennent pas à Intelsat. Il s'agit surtout de satellites russes, mais aussi d'autres satellites régionaux de communications. Les stations qui surveillent ces satellites-là sont, d'après Hager, Menwith Hill (Angleterre), Shoal Bay (Australie), Bad Aibling (Bavière/RFA), Misawa (Nord du Japon) et Leitrim (Canada). Cette dernière s'occupe principalement des satellites latino-américains.

Enfin, troisième objectif d' Echelon : coordonner les stations qui s'occupent des systèmes de communications terrestres. Celles-ci sont spécialement intéressantes, car elles s'effectuent par l'intermédiaire de câbles transocéaniques et d'une technique de haute fréquence, et véhiculent d'énormes quantités de communications officielles, commerciales ou gouvernementales.

Le gouvernement allemand tolère cette surveillance tous azimuts La station d'écoute très puissante de Menwith Hill dans le nord de l'Angleterre disposerait de 22 stations satellitaires de réception. Menwith Hill sert en première instance la NSA, en tant que station terrestre des satellites-espions américains. Ceux-ci surveillent les télécommunications à rayon réduit comme par exemple les émetteurs militaires ou les « walkies-talkies ».

Les stations terrestres d'Alice Springs (Australie) et de Bad Aibling (Bavière) ont une fonction analogue. En Allemagne, les autorités officielles ne veulent rien entendre de tout cela. Ainsi, l'ancien Secrétaire d'État Eduard Lintner (CSU), en poste au ministère de l'Intérieur de Bonn, a répondu le 30 avril 1998 à une question écrite, posée par le député socialiste Graf, portant sur les activités de la NSA, que le gouvernement fédéral allemand ne savait rien de plus que ce qu'avait dit la presse à ce sujet !

En d'autres termes : le gouvernement fédéral allemand ne sait officiellement rien de cette incursion massive et de cette grave entorse à l'intégrité des États nationaux et des individus. Mais cette attaque vient d' « États amis » de l'Allemagne. C'est tout dire !

Ce document portait comme indication « *Les services spéciaux américains* », d'après V. Harchetti, J.D. Marks, CIA, Munich 1976.) ; sources : « *Panorama D.D.R.* » ; Envoi de « *Radio Berlin International* » 12 avril 1989.

Les pratiques des services spéciaux américains

La CIA est en quelque sorte l'incarnation des services spéciaux américains et pourtant ce n'est qu'une partie et pas la plus importante des services d'espionnage et de contre-espionnage des États-Unis.

Considère-t-on les ressources financières et les effectifs, c'est la National Security Agengy, la « NSA » relevant du secrétariat d'État à la Défense, qui vient en tête. La différence avec la CIA, c'est que l'on n'en sait pratiquement rien, c'est le plus secret des services spéciaux américains.

Il y a un peu plus de quinze ans, dans le sillage du scandale provoqué par l'affaire du Watergate, un voile s'était levé, retombé bien vite, mais voici que l'on reparle beaucoup de la NSA, surtout en République fédérale d'Allemagne, suite à la découverte d'un système de surveillance de toutes les communications téléphoniques.

Et il ne s'agit que d'une petite partie seulement des activités de la NSA

À l'écoute des communications radiotélégraphiques

Tous les pays civilisés et démocratiques ont inscrit le secret des communications téléphoniques dans leurs Constitutions. Au même titre que le secret des communications postales, il ne peut être levé que dans des circonstances exceptionnelles, circonstances précisées explicitement par la loi. Or, comme l'a révélé le magazine de RFA *Der Spiegel*, la NSA ne s'en tient nullement à ce droit proclamé par la Constitution des États-Unis et va même jusqu'à violer la souveraineté d'autres États : « *Jamais encore dans l'histoire de l'humanité, une puissance n'est parvenue à mettre en place un tel système d'écoute de tout ce qui se dit dans le monde.* » (*Der Spiegel*, Hambourg, nº 8, 1989.)

La densité est évidemment la plus grande en RFA et à Berlin Ouest. Les milieux les plus informés considèrent qu'il s'y trouve plus de 350 antennes des services spéciaux américains. Les services spéciaux ont des correspondants dans toutes les casernes et les dépôts d'armes, dans les aéroports et les agglomérations. Ils manipulent les équipements ultra-perfectionnés d'écoute, dirigés surtout en direction des États membres du Traité de Varsovie.

Les services d'écoutes de la NSA captent également les faisceaux directionnels de la poste de RFA qui retransmettent le tiers environ des communications téléphoniques. La NSA intervient directement dans le réseau téléphonique de la RFA. Les journalistes du *Spiegel* ont découvert à Francfort-sur-le-Main l'une de ces stations branchées directement sur le réseau téléphonique, Francfort-sur-le-Main est rappelons-le la plaque tournante des communications téléphoniques en RFA

« Le système est conçu pour capter toutes les informations transmises par satellite ou faisceau directionnel, par câbles de cuivre ou fibres optiques ou par réseau souterrain. »

D'après les indications d'informateurs dont l'identité est tue dans l'article, la station, qui se trouve à proximité de la gare centrale de Francfort et qui est protégée par d'épaisses portes blindées, gère une centaine d'ordinateurs. Il suffit de taper sur le clavier le numéro de téléphone pour que l'écoute se mette automatiquement en marche. Sur d'autres ordinateurs, il faut donner un numéro codé pour qu'ils enregistrent les conversations.

De cette façon, il est possible d'intervenir partout, de surveiller les conversations des particuliers, mais aussi les communications professionnelles, c'est-à-dire faire de l'espionnage industriel. A plusieurs reprises, les gestionnaires de firmes de RFA ont été étonnés de quelles informations détaillées disposaient leurs relations d'affaires aux États-Unis. Selon le *Spiegel* : « *La NSA surveille un nombre incalculable de communications de particuliers en RFA* ».

Les dossiers du Congrès américain établissent que l'on s'intéresse au même titre aux informations de nature économique qu'aux détails de la vie privée des personnalités de la vie publique ; on écoute aussi les conversations des particuliers impliqués dans « *des actions de protestation contre leur gouvernement.* »

Les services spéciaux de la RFA profitent dans une certaine mesure des écoutes téléphoniques des services américains. Régulièrement l'office fédéral de protection de la Constitution à Cologne, dont la mission est la surveillance politique de la population ouest-allemande, et l'office fédéral de police de Wiesbaden, reçoivent communication d'informations sur les « menées terroristes » et les « courants

extrémistes », ce qui ne veut pas dire uniquement les activités politiques des forces démocratiques et de l'opposition en RFA. Grâce à cette aide d'une nature très spéciale, les services d'espionnage et la police de RFA accédant à des informations au mépris du secret des communications téléphoniques inscrit dans la Constitution.

La NSA a au moins neuf stations d'écoute des communications téléphoniques en RFA et à Berlin (ouest), qui échappent absolument à tout contrôle. La révélation des pratiques des services spéciaux du pays et de certaines puissances extérieures a provoqué un vif émoi en RFA. Comme le gouvernement fédéral refuse de donner la moindre réponse à ces reproches et nie même qu'il y ait écoute téléphonique, le groupe S.P.D. au Bundestag a posé une grande question orale sur le fait que les services spéciaux des puissances occidentales alliées seraient habilités « *à surveiller les communications postales et téléphoniques en République fédérale d'Allemagne, en particulier ouvrir les envois tombant sous le coup du secret des communications télex et à mémoriser les informations collectées de cette manière.* » (*Neues Deutschland*, Berlin, 10 mars 1989.)

Comme le gouvernement fédéral n'était pas disposé à donner des réponses précises, l'Union humanitaire a adressé une lettre ouverte au président fédéral, H. Richard von Weizsäcker pour lui demander de vérifier s'il était vrai que les services spéciaux américains de la NSA avaient violé les droits de l'homme en RFA. L'Union demandait du président de la RFA qu'il intervienne « *pour interdire les atteintes aux droits de l'homme des citoyens de la République fédérale par les services spéciaux de puissances alliées* » et disait que le président avait justement pour mission « *de faire respecter la souveraineté de notre pays* » et qu'il avait les moyens de parvenir « à une clarification complète de cette affaire » (*Frankfurter Rundchau*, Francfort-sur-le-Main, 30 mars 1989.)

La population de RFA attend jusqu'à aujourd'hui cette clarification complète.

Le système d'écoute

L'espionnage comme on l'entend traditionnellement repose sur l'activité des correspondants et résidents. La NSA elle, utilise des moyens et des méthodes tout autres, ce sont les équipements installés à terre, sur les navires, les satellites et les avions. Ses espions sont des techniciens des télécommunications et des informaticiens.

La NSA a les moyens de capter les signaux électromagnétiques : impulsions radar, signaux télégraphiques et communications téléphoniques pour en retirer les informations qu'elle juge utiles. On observe ainsi avec la même intensité les amis et les adversaires, encore que l'essentiel de cette activité soit concentré en direction de l'Union soviétique et des autres États du traité de Varsovie. Le territoire de la RFA joue dans ces activités un rôle particulier.

La République fédérale est le pays occidental le mieux adapté pour une écoute de l'adversaire à l'Est. (*Der Spiegel*, Hambourg, nº 8, 1989.)

Deux raisons au moins plaident pour ce système :

— premièrement : la position géographique de la RFA au point de contact du Traité de Varsovie et de l'OTAN. À cela vient s'ajouter qu'aucun massif montagneux ne vient faire obstacle, ce qui permet une pénétration en profondeur jusque très loin en territoire soviétique.

— deuxièmement : le gouvernement de la RFA se montre extrêmement tolérant vis-à-vis des activités d'espionnage des services spéciaux étrangers sur son territoire et leur donne tous les moyens de pratiquer leurs activités à l'abri des regards indiscrets.

La NSA a au moins huit centres d'écoute le long de la frontière entre la RFA et la R.D.A. et à Berlin (Ouest), ceux à la frontière avec la Tchécoslovaquie, tous tournés contre le Traité de Varsovie. Neuf autres stations sont tournées vers l'ouest, ce qui donne aux États-Unis la possibilité de surveiller pratiquement toute l'Europe. D'autres stations existent à Harrogate en Angleterre, à Edzelf en Écosse et à Chypre.

La plupart sont dissimulées dans les forêts et protégées par plusieurs réseaux d'obstacles et sont des périmètres marqués par les panneaux « Restricting Areas Warning » (Zone interdite Attention). Tout y est interdit : photographier, prendre des notes écrites, établir des dessins, des cartes et des relevés topographiques. Tous les supports d'information de cette nature sont saisis. Les personnes contrevenant à ces dispositions sont passibles d'une peine « en vertu des lois des États-Unis et/ou de la République fédérale d'Allemagne ».

Station de Gablingen (Allemagne)

Ceux qui ont pu observer de loin des stations, par exemple à Bad Gadling en Haute-Bavière, disent qu'il s'agit de gigantesques coupoles d'aluminium ou d'un immense réseau d'antennes de 300 mètres de longueur et d'une hauteur de 100 m pour les équipements de la plaine de Lech près de Gablingen, ou encore une série de pylônes d'acier comme sur la colline du Teufelsberq, à Berlin (Ouest).

Des missions différentes correspondent à ces différences de structure. La vocation exacte des différentes stations est un secret total..

On sait qu'il existe des stations identiques dans l'émirat d'Oman et dans le désert d'Australie centrale, non loin d'Alice Springs. Les spécialistes estiment à 4000 le nombre des services d'écoute répartis sur les différents continents, principalement dans les bases de l'armée de terre, de l'aviation et sur les appareils de la Navy.

À cela vient s'ajouter les satellites, les bâtiments et les avions d'espionnage et de reconnaissance qui transmettent les informations directement à la centrale de la NSA aux États-Unis dans les collines du Maryland, à une trentaine de kilomètres au nord-est de Washington, ou bien au quartier général pour l'Europe à Francfort-sur-le-Main. Sur place, les informations sont traitées sur des ordinateurs qui établissent les dossiers et les mémorisent.

Les spécialistes de RFA donnent cette indication sur la place de la NSA parmi les services spéciaux américains : « La CIA ne livre que 5 % des informations utiles ; la NSA par contre 95 %. À Berlin-Ouest par exemple il n'y a plus que 60 résidents de la CIA contre 600 pour la NSA » (*Der Spiegel*, Hambourg, N° 8, 1989.)

Formidable avance des techniques militaires

Le quartier général de la NSA est établi sur le périmètre de la base militaire de Fort Meade dans l'état du Maryland et il y a 186 000 m^2 de bureaux, soit autant que le quartier général de la CIA et le Capitole réunis. La NSA dispose des systèmes informatiques les plus puissants et les plus évolués.

Le général Marshall Carter, à l'époque directeur de la NSA, disait déjà à la fin des années soixante : « *J'avais deux hectares et demi d'ordinateurs* ». Dix ans plus tard, on atteignait une surface deux fois plus grande et il faut estimer que les dix dernières années ont vu s'accroître considérablement les équipements, même si, compte tenu des progrès de la miniaturisation, la surface occupée ne s'est pas agrandie au même rythme.

La NSA fait travailler des centaines d'hommes parmi les meilleurs mathématiciens, techniciens et informaticiens des États-Unis. La NSA entretient ses laboratoires à l'Université de Princeton (État de New Jersey). Les experts considèrent que la NSA est en avance de cinq ans au moins sur les techniques civiles. La NSA commande pour des sommes astronomiques des ordinateurs à l'industrie et aux universités.

Les laboratoires travaillent actuellement sur la mise au point d'un synthétiseur automatique de la parole capable de traduire et d'imprimer les conversations enregistrées. La NSA fait valoir jalousement ses prérogatives quand apparaissent de nouvelles innovations en informatique théorique et appliquée et c'est elle qui décide si les travaux peuvent être poursuivis pour des fins civiles.

Les laboratoires « d'analyse de systèmes » de la NSA mettent au point eux-mêmes les équipements électroniques les plus perfectionnés : caméras, capteurs, microphones et amplificateurs ou effectuent les essais dans les laboratoires civils. La NSA réalise en particulier les capteurs pour la surveillance des routes maritimes, les photos aériennes et !es photos satellites, se charge de l'analyse et confectionne les équipements techniques pour la guerre des ondes acoustiques.

Grâce aux moyens financiers dont elle dispose, la NSA est toujours en avance sur le secteur civil, ce qui soit dit en passant réfute la thèse selon laquelle la recherche dans le secteur militaire est toujours payante pour le secteur civil. C'est le contraire qui est vrai. Conséquence du secret militaire, il n'est pas rare que certaines techniques soient bloquées pendant des années pour le secteur civil et l'industrie.

Un acte constitutif resté secret jusqu'à aujourd'hui

Le 24 octobre 1952, le Président Truman signait un texte de sept pages, dont le contenu est resté secret jusqu'à aujourd'hui (déclassifié depuis, voir en annexe). En droit américain, l'acte constitutif n'avait pas à être ratifié par le Congrès.

On savait qu'aux États-Unis et à l'extérieur, même si ce n'était pas dans les moindres détails, ce que font le F.B.P. (chargé du renseignement à l'intérieur) et la CIA (espionnage hors des frontières) mais il a fallu attendre octobre 1975 pour qu'on entende parler de la NSA quand le directeur, à l'époque le général Lew Allen, a été entendu par une sous-commission du Congrès sur les activités illégales des services spéciaux américains.

Au mépris du droit américain, mais avec l'assentiment des services de la justice et de la défense, la NSA avait espionné des milliers de ressortissants américains pour le compte du F.B.I. et de la C.I.A. : écoute de conversations téléphoniques, surveillance des télégrammes et des télex, lettres décachetées, itinéraires de déplacements mis à jour. Des milliers de dossiers avaient été établis au nom des militants des droits civiques, des journalistes, des députés du Congrès, des personnalités de gauche qui, dans le pays qui se proclame le phare des libertés, avaient une opinion autre sur Cuba par exemple.

Les mesures d'investigation étaient encore plus poussées dans le cas des personnes soupçonnées de « menacer la sécurité nationale » parce qu'elles s'opposaient à la guerre du Vietnam. Des centaines de milliers de personnes ont été ainsi espionnées. La CIA se servait de ces informations dans son opération « *chaos* » destinée à observer 300 000 adversaires de la guerre du Vietnam.

Le directeur de la NSA a promis devant la sous-commission parlementaire d'enquête que la NSA n'interviendrait plus qu'à l'extérieur et l'on a renoncé à une poursuite de l'enquête sur les activités illégales. Les procès intentés par certains opposants ne donnèrent aucun résultat. La NSA disparut dans l'anonymat et pourtant elle a enregistré le taux de croissance le plus fort de toutes les institutions américaines durant les quinze dernières années.

Budget :

— en 1975, la NSA avait un budget de 1,2 milliard de dollars, contre 15 milliards de nos jours d'après les milieux informés, c'est-à-dire dix fois plus. Par comparaison, le budget de la ClA est passé durant la même période de 750 000 à 1,5 - 2 milliards de dollars, soit tout au plus un triplement.

Effectifs :

— les effectifs ont évolué dans des proportions comparables. Ils sont passés de 24 000 vers 1975 â 16 500 à 20 000 - 25 000 pour la ClA. Au quartier général de la NSA dans le Maryland vivent 35 000

hommes, derrière un réseau de protection redoutable fait d'une enceinte de trois mètres de hauteur. Sur place, le personnel trouve absolument tout ce dont il a besoin pour vivre.

On y trie les informations en provenance du monde entier pour faire la répartition entre ce qui ne présente aucun intérêt et les informations pertinentes. On y produit en moyenne annuelle 24 000 tonnes de documents ultras confidentiels. Le stockage s'effectue ailleurs, par exemple dans des immeubles de l'aéroport international de Baltinore-Washington. Il s'agit surtout de supports magnétiques, de photos et de dossiers. La destruction du matériel inutilisable est une opération encore plus délicate que le stockage. On traite chaque jour 40 tonnes de papier.

Quels sont les critères de sélection du personnel ? Les fonctionnaires de la NSA sont des personnes convaincues, qui ont passé des tests psychologiques et physiques. On retient surtout les candidatures de patriotes issus de familles établies depuis des générations aux États-Unis, qui idolâtrent leur pays et soupçonnent les autres d'avoir un pacte avec le malin.(*Der Spiegel* N° 8, 1989.)

Les noms des collaborateurs de la NSA sont tout aussi secrets que l'institution elle-même. Les ressources financières de la NSA sont dissimulées dans les budgets de plusieurs ministères. La NSA relève du Pentagone et peut solliciter pour certaines opérations le concours de personnels militaires, sans qu'ils sachent toujours pour qui ils agissent. En principe, tous les soldats américains stationnés à l'étranger peuvent être chargés d'une mission pour le compte de la NSA, d'autant plus facilement que chacune des armes a elle-même son propre système d'espionnage.

Aucun autre pays n'a un tel système spécialisé et gigantesque d'espionnage et d'informations, disposant de moyens financiers, techniques et humains de cette importance. Tout ceci pour se procurer des informations au mépris de la souveraineté des autres États et garantir à Washington un rôle politique, militaire et économique dirigeant dans le monde. La NSA est implantée dans 2 000 bases américaines disséminées dans le monde entier.

Ce document provient du site du *Monde.* Il date du 25 février 2003.

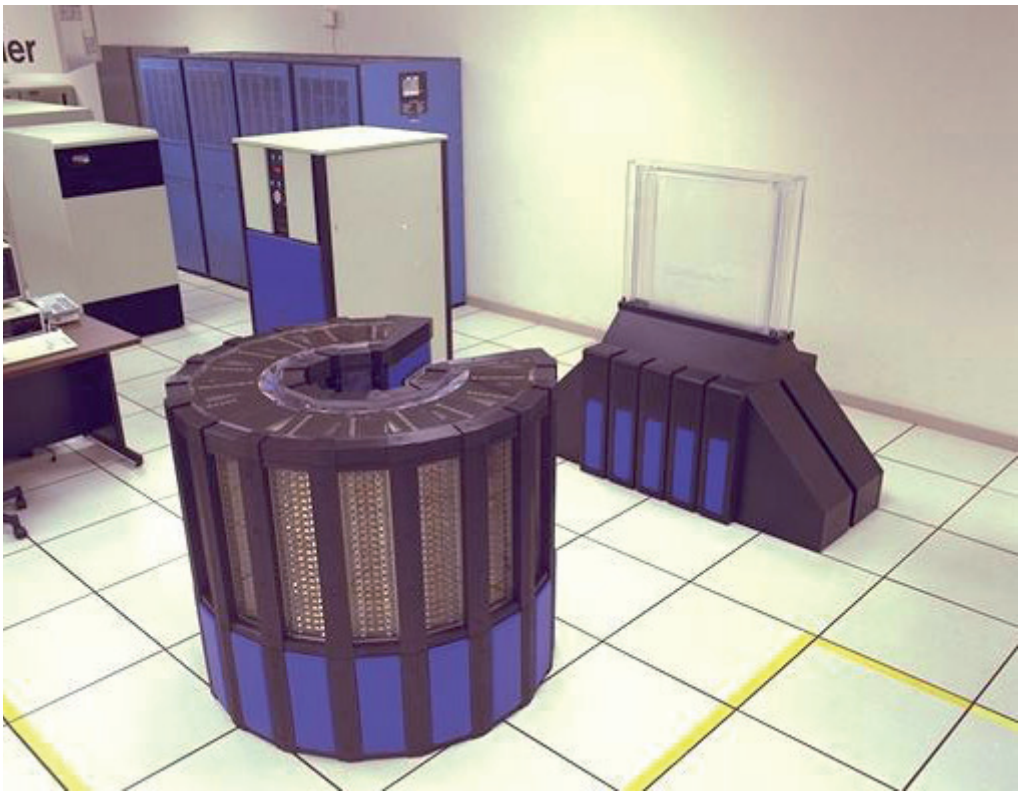
Les supercalculateurs doivent concilier puissance et rentabilité, Michel Alberganti

Deux architectures de superordinateurs, les vectoriels de Cray et les superscalaires[141] d'IBM, s'affrontent sur le marché étroit du calcul scientifique intensif. Les fabricants visent pour 2010 le pétaflops, soit un million de milliards d'opérations par seconde. D'un côté, les machines vectorielles de Cray, de l'autre les ordinateurs superscalaires d'IBM. Deux conceptions s'affrontent sur le marché étroit, mais stratégique du calcul scientifique intensif.

Cray a mis en production fin 2002 son nouveau système X1 qui affiche une puissance de crête de 819,2 gigaflops (milliard d'opérations à virgule flottante par seconde) par module de 64 processeurs. Le fabricant propose des configurations rassemblant 4 000 puces pour atteindre les 52,4 téraflops (million de millions

[141] Un processeur est dit superscalaire s'il est capable d'exécuter plusieurs instructions simultanément, chacune dans un *pipeline* différent. En architecture des processeurs, un *pipeline* est une technique de conception des processeurs où l'exécution de plusieurs instructions se chevauchent à l'intérieur même du processeur. Le premier ordinateur à utiliser cette technique est l'IBM Stretch, conçu en 1958. Architecture vectorielle : Sur de tels processeurs, une instruction va s'appliquer à un ensemble de données, appelé vecteur. Une seule instruction va donc exécuter la même opération de façon parallèle sur tout le vecteur. Ce genre d'architecture est efficace pour les applications de calcul scientifique et s'est notamment trouvée dans les superordinateurs comme les Cray.

d'opérations à virgule flottante par seconde). Cray annonce simultanément son objectif d'atteindre le pétaflops, soit 1015 opérations par seconde, en 2010. S'il y parvient, le constructeur aura réussi à passer du gigaflops, lancé en 1990, au pétaflops (million de milliards), soit une puissance de calcul multipliée par un million en vingt ans...



Supercalculateur Cray-2

L'entreprise créée par Seymour Cray en 1972, rachetée en 1996 par Silicon Graphics quelques mois avant la disparition de son fondateur et vendue à Tera Computer en mars 2000, renaît de ses cendres grâce à l'appui de son premier client. Le gouvernement américain a en effet financé plus de la moitié des 100 millions de dollars dépensés pour développer le nouveau modèle de Cray, le X1. « *Le gouvernement voulait un tel système pour assurer des missions critiques* », explique James Rottsolk, P.D.G. de Cray, qui ne conteste pas que les applications visées sont militaires.

Les États-Unis doivent mettre au point les prochaines générations de d'armes nucléaires sans faire appel à des essais réels. En fait, la première machine livrée par Cray semble destinée à une autre tâche particulièrement sensible : le décryptage, activité phare de la National Security Agency.

L'importance stratégique de tels supercalculateurs capables de simuler une explosion nucléaire ou de casser n'importe quel code secret constitue une chance pour Cray dont les machines restent fidèles à l'architecture vectorielle abandonnée par la plupart des fabricants, en dehors de NEC. « *Cray reste la seule entreprise spécialisée dans les supercalculateurs, affirme James Rottsolk pour justifier l'aide de l'État. Les autres sont orientés vers le marché des ordinateurs de bureau et fabriquent des supercalculateurs en réalisant des assemblages de machines individuelles (clusters). Le X1, lui, est conçu comme une entité à part entière dont les processeurs partagent les données et travaillent ensemble* ».

Les tenants du scalaire

Preuve que le vectoriel n'est pas mort, le supercalculateur le plus puissant du monde que NEC a fabriqué pour le projet Earth Simulator l'utilise. En deuxième position dans la liste du Top 500 mondial,

on trouve les deux machines installées par Hewlett-Packard au laboratoire de Los Alamos et dont la puissance de crête dépasse à peine les 10 téraflops.

Concurrent historique de Cray aux États-Unis, IBM a abandonné le vectoriel au profit de l'architecture scalaire formant des clusters. « Le scalaire s'applique plus facilement que le vectoriel à des problèmes différents », explique Luigi Brochard, architecte pour le calcul scientifique pour l'Europe chez IBM.

Derrière les raisons techniques du choix du scalaire, se profilent de solides motivations économiques. En effet, les machines développées par IBM et les tenants du scalaire sont adaptées aux applications de gestion, ce qui élargit considérablement leur marché en réduisant les prix de vente. « *Le développement des puces revient extrêmement cher et nous avons besoin de nombreux clients* », précise Eric Taillard, responsable des ventes Unix Linux chez IBM France. « *Les budgets des centres de calcul n'augmentent pas alors que leurs besoins de puissance explosent avec la simulation et la conception virtuelle* », ajoute-t-il..

De nombreux laboratoires ont donc adapté leur stratégie au réalisme économique prôné par IBM. Ainsi, en France, le centre de calcul du CNRS à Orsay, l'Idris, a tourné casaque fin 2001 en remplaçant le T3E vectoriel acheté en 1996 à Cray par un cluster de 8 machines scalaires IBM Power4 (1,3 téraflops, 92e dans le Top 500).

Même choix pour la direction des applications militaires (DAM) du CEA[142] qui a fait l'acquisition, fin 2001, du supercalculateur Tera fabriqué par Compaq, devenu Hewlett-Packard depuis, et qui arrive en septième position mondiale et occupe la première en Europe avec une puissance de crête de 50 téraflops. Destiné au développement des armes nucléaires et à la simulation de leur fonctionnement et de leurs effets, cette machine est dix fois moins puissante que la configuration proposée par Cray avec le X1 et vingt fois moins que le système annoncé par IBM en novembre 2002. En effet, Big Blue n'a laissé que cinq jours à Cray pour s'attribuer la commercialisation du supercalculateur le plus puissant du monde. Le 19 novembre 2002, IBM révélait que le département américain de l'énergie (DOE) avait passé commande de deux machines : l'ASCI Purple (100 téraflops) ; Blue Gene/L (367 téraflops).

Ces chiffres astronomiques n'impressionnent guère Cray, qui met le doigt sur l'une des faiblesses majeures des clusters de machines scalaires : leur efficacité en application réelle. « Suivant les cas, le rendement des supercalculateurs scalaires varie de 1 % à 10 % dans le meilleur des cas, quand les supercalculateurs vectoriels peuvent atteindre 25 % à 50 % », assure Steve Scott, directeur scientifique de Cray, qui explique cette différence par les fondements mêmes de l'architecture scalaire. « Les données s'y déplacent difficilement et les processeurs se retrouvent souvent à cours d'information à traiter », souligne-t-il. Chez IBM, Luigi Brochard ne conteste pas cette faiblesse, mais il en limite l'impact. « Nous oscillons entre 10 % et 75 % d'efficacité », estime-t-il, en indiquant que les calculs de prévisions météo se situent dans le bas de la fourchette. L'écart entre chiffres annoncés et puissance effective demeure très important, particulièrement avec les clusters de machines scalaires. « C'est pourquoi nous travaillons beaucoup, reconnaît Luigi Brochard , à augmenter les 10 % ».

Des calculs plus fins grâce au pétaflops

Pour quelles applications peut-on avoir besoin de la phénoménale puissance de calcul de 1 million de milliards (10^{15}) d'opérations par seconde ? Comme les activités militaires dont les besoins semblent

[142] La direction des applications militaires (DAM) du CEA vient de réceptionner le supercalculateur TERA-10, d'une puissance de plus de 50 téraflops (50 000 milliards d'opérations à la seconde). Cette machine, fabriquée par Bull, est constituée de 4352 processeurs double cœur Intel® Montecito (8704 cœurs) reliés par un réseau d'interconnexion hautes performances Quadrics.
Ce supercalculateur, le plus puissant d'Europe et l'un des plus performants au monde est, avec la machine radiographique Airix et le laser Mégajoule (LMJ), l'un des trois équipements majeurs du programme Simulation dont l'objectif est de garantir, en l'absence d'essais nucléaires, la sûreté et la fiabilité des armes nucléaires françaises. La machine Tera-10 est installée sur le Centre DAM/Ile de France à Bruyères le Châtel, au sein du Complexe de calcul scientifique du CEA.

sans limites, les activités scientifiques se heurtent parfois à des problèmes d'une complexité telle qu'ils justifient de recourir à la puissance des supercalculateurs.

Deux grands domaines sont ouverts à de telles machines : les sciences de la vie et la climatologie. Dans le premier, il s'agit, par exemple, de comprendre comment une cellule fonctionne. Dans le second, la précision du résultat dépend de la finesse du calcul, c'est-à-dire de la réduction de la résolution du maillage du phénomène modélisé. C'est le cas avec les 10 km que doit atteindre *Earth Simulator*. Enfin, la simulation s'étend à des domaines de plus en plus nombreux (espace, aéronautique, automobile...) à travers le développement rapide du prototypage virtuel qui permet de visualiser et de valider une conception sans fabriquer d'objet réel.

Article de *La Tribune* du 13 janvier 1999 sur les enjeux de la guerre de l'information au regard des capacités d'Echelon.

L'information, nouveau champ de bataille planétaire

Informer et se protéger des détournements ou des manipulations d'information à l'échelle de la planète, tel est l'enjeu technologique des guerres de demain.

Stupeur. Au printemps dernier, le quotidien italien *Il Mondo* révèle que le Royaume-Uni a participé et participe peut-être encore au réseau américain Echelon, dans le cadre du programme UKUSA réunissant également le Canada, l'Australie et la Nouvelle-Zélande, sans que ses homologues européens en aient été informés. Un réseau capable d'espionner, trier, décrypter, archiver et traiter 3 millions de communications téléphoniques satellitaires à la minute, c'est-à-dire les conversations, les fax, les messages Internet ou EDI (échanges de données informatisées). Pour mener cette tâche énorme, la NSA (National Scientific Association) américaine dispose d'un bataillon de 40.000 personnes.

L'existence de ce réseau anglo-saxon a été mise en exergue par Alain Pompidou dans son rapport à la Commission européenne intitulé « *Évaluation des techniques de contrôle politique* » dans lequel il dénonce l'interception et la transmission vers les États-Unis des messages européens par le centre stratégique britannique de Menwith Hill. Une histoire symptomatique des enjeux technologiques qui se cachent derrière la maîtrise de l'information dans les conflits du futur.

« *Terrain économique* »

« *J'ai appris l'existence d'*Echelon *par la presse et par Internet* », reconnaît François Fayard, directeur du Celar (Centre d'Électronique de l'Armement). Basé à Bruz près de Rennes et présenté comme le pôle français de compétence en matière de guerre électronique, celui-ci a soufflé ses trente bougies en octobre dernier.

Le Celar

Fort d'un budget annuel de 650 millions de francs (99,1 millions d'euros) pour 750 personnes, dont 300 ingénieurs et 250 techniciens, le Celar développe des algorithmes mathématiques de cryptage des données, des leurres électroniques antimissiles et des protections pour les réseaux informatiques des sys-

tèmes de commandement. À la différence des États-Unis qui se permettent, sous le couvert des autorités, d'écouter leurs concurrents commerciaux, la France, quant à elle, prétend ne pas se l'autoriser.

« *Mais il y a un vrai débat. Nous nous protégeons grâce à des technologies que nous développons. Sans attaquer. Reste que le programme Echelon semble se développer à présent sur un terrain plus économique que militaire* », s'inquiète François Fayard.

Informé des détails de la proposition d'une compagnie nippone de téléphonie à un appel d'offres lancé par la Malaisie, le géant américain des télécommunications AT & T aurait réussi à souffler le marché avec une proposition plus agressive. L'opacité de la guerre de l'information pousse le danger plus loin : « *Près d'un tiers des transactions boursières dans le monde sont d'origine mafieuse* », soulève un responsable à la DGA (Délégation générale pour l'armement).

« *Technologies civiles* »

Cette guerre électronique de l'information, qu'elle soit économique ou militaire, s'appuie sur des technologies adaptées des transmissions civiles. « *Nous récupérons toutes les données possibles, de la voix, des données chiffrées, des cartes géographiques et des images haute définition pour les transmettre à l'état-major qui répercute les ordres aux unités de combat. C'est ce que l'on appelle le métasystème d'information* », reprend François Fayard. *Toutes ces informations utilisent des supports différents et sont très gourmandes en taille de fichiers informatiques. Il faut alors déplacer un matériel spécifique, des " autocommutateurs à roulettes " à base de technologies civiles. Tout l'art consiste à les intégrer astucieusement pour des débits satisfaisants.* »

Ensuite, le Celar développe des intranets privés, coupés du monde extérieur pour éviter l'interception des informations par l'adversaire et surtout l'intrusion de pirates informatiques qui pourraient diffuser de faux ordres, comme l'objectif d'un missile. « *On interdit l'usage d'Internet et des téléphones mobiles GSM dans notre théâtre d'opérations. Nous surveillons également les transactions informatiques sur nos serveurs. C'est un travail de fourmi.* »

Autre problème, les systèmes d'exploitation des serveurs, essentiellement Windows NT de chez Microsoft, sont des produits commerciaux vastement diffusés dans le monde. « *Ce qui est gênant, c'est que nous ne disposons pas des codes sources, donc nous ne savons pas s'il y a des virus dormants ou cachés. On peut très bien imaginer qu'une bombe logicielle y réside et soit activable à distance* », estime le directeur du Celar.

Ce document portait comme indications : « *Une thèse de* : *Michael Van De Wiele, Université Catholique de Louvain, Faculté de Science Politique, SPOL 22* ».

Quelle stratégie doit adopter l'Union Européenne face à la menace économique que représente le réseau d'écoute Echelon ?

1. *Introduction*

L'espionnage et la surveillance de l'autre ont été de tout temps, une des activités favorites de chaque système politique, et ce, toujours au nom des mêmes idéologies : la Sécurité d'État et l'Intérêt National.

Dans notre monde actuel, tout est sujet de surveillance et de contrôle par un tiers, de toutes nos activités. Que nous payions par carte électronique, que nous téléphonions, que nous écrivions un mail, tout est surveillé. Chaque détail est un renseignement de plus sur notre vie privée qui vient s'ajouter à notre fichier central. Ce n'est pas pour cela qu'il faut verser dans la paranoïa, mais l'ampleur est telle que parfois, elle dépasse l'entendement.

Aujourd'hui, cet espionnage ne concerne plus seulement les domaines militaires et politiques, mais touche aussi le milieu économique. Pourquoi donc ?

Dans une globalisation et une mondialisation comme se plaisent à dire les économistes, la concurrence et les profits sont devenus les premiers enjeux d'un certain prestige, tant national qu'international. Et tous les moyens sont bons pour devancer son « adversaire ». C'est pourquoi certaines puissances n'hésitent pas à mettre leur système de surveillance au service de leur économie nationale.

Nous allons tenter d'analyser la situation, tout en cherchant à comprendre le problème et à en donner des pistes pour le résoudre.

Ce travail est une tâche ardue du fait du problème d'accès aux sources. Bien souvent et toujours au nom du même intérêt : la sécurité nationale, bon nombre de documents officiels sont interdits d'accès, car frappés de la mention « secret ». Il conviendra donc de distinguer la véritable information de l'intoxication, tâche que je me suis donné de faire. C'est pourquoi ce travail ne peut être qu'une ébauche de la réalité.

2. *Une brève définition*

Pour bien comprendre le sujet, il s'agit d'abord de distinguer certains termes entre eux pour éviter toute confusion. En effet, les mots *surveillance* et *espionnage*, bien qu'ils aient une même connotation, ont une signification très différente.

Surveillance : « Observer attentivement pour contrôler. »

C'est donc par un contrôle et pour un certain souci de sécurité, que la surveillance est opérée. Bien que le concept soit ambigu, il est largement rentré dans nos mœurs par l'avantage sécuritaire qu'il nous apporte à tous. C'est ainsi que l'on voit fleurir des toutes parts des caméras de surveillance dans les environnements publics et que la mise sur écoute de conversations téléphoniques est organisée dans le but d'intercepter de sombres conversations de criminels en tout genre. Mais ce contrôle ne peut être sans limites, il y a besoin d'instaurer des garde-fous au moyen d'une législation appropriée fixant les modalités de ces surveillances. On peut en conséquence, réduire la notion de surveillance au concept de sécurité nationale.

Espionnage : « Activité des espions ayant pour but de nuire à la sécurité d'une entreprise ou d'un pays au profit d'un autre. »

Ici, nous tombons dans le domaine du secret. On ne peut pas vraiment dire que c'est illégal, car aucune loi ne réglemente ce domaine, cependant dans l'ordre moral ce n'est pas très correct, mais ceci n'est pas le sujet de ce travail.

Il s'agit donc d'acquérir d'une manière peu scrupuleuse ce qui ne nous appartient pas tout au dépend de l'autre et cela au nom d'une prospérité nationale. En exemple, on se souviendra du triste épisode de l'avion supersonique soviétique, le Tupolev, sorti quasi en même temps que le Concorde européen, alors que le projet était secret, mais qui fut un véritable échec pour les autorités de Moscou suite à son écrasement dès le décollage. Jamais les autorités soviétiques n'admirent l'espionnage, mais celui-ci est un fait trop évident à nier

Le Concorde

Le Tupolev 144

Nous nous retrouvons donc ici face à un des grands dilemmes des relations internationales, celui « du beurre ou du canon » ou autrement, devoir choisir entre sa prospérité ou sa sécurité, bien que les deux ne soient pas opposés dans le cas de la relation espionnage-surveillance.

3. *Un état des lieux de nos technologies*

Nous vivons dans une ère où la technologie est devenue omniprésente et où la communication et l'information en sont les moteurs de développement. Aujourd'hui tout le monde communique, que ce soit par téléphone, par Internet ou par tout autre moyen de communication, et la majorité de ces communications sont électroniques, donc diffuses et facilement interceptables sans que l'on s'en rende compte. Ce qui peut amener à des abus.

Bien des tentatives ont été réalisées afin de protéger ces communications électroniques, mais dès qu'une technologie de cryptage est développée, celle-ci est déjà quasiment décryptée par quelqu'un d'autre.

Il faut savoir qu'actuellement, plus aucune technologie n'est à l'abri d'une quelconque intrusion. Voici quelques exemples :

Certains téléphones RNIS permettent d'écouter ce qui se dit dans une pièce quand le combiné est raccroché ; le logiciel gratuit d'écoute de CD musicaux *RealJukebox*, diffusé en Europe à des millions d'exemplaires transmettait à la maison mère américaine, de manière cryptée et à intervalles réguliers les index des CDROM qui étaient insérés dans le lecteur du PC.

Et il existe bien d'autres exemples encore, mais ce travail ne suffirait à les répertorier.

4. *La NSA*

En 1952, sous l'impulsion du président Truman, est créée aux États-Unis la NSA (National Security Agency), agence chargée du contre-espionnage et de la protection des communications gouvernementales et militaires (voir mémorandum en annexe).

Actuellement, on estime que cette agence se voit attribuer un budget annuel de 4 milliards de dollars pour un personnel de 50.000 personnes, ce qui représente à l'échelon national, le double en capacité financière et humaine d'une grande entreprise comme Belgacom.

Dans son site Internet, l'agence affiche très clairement son idéologie : « *Ces pages décrivent le plan stratégique de la NSA/(CSS) pour le 21e siècle et comment nous comptons atteindre notre but : la supériorité américaine dans bien des domaines et particulièrement dans celui de l'information.* »

Elle est mondialement reconnue pour sa technologie sophistiquée et pour son travail dans l'ombre de la présidence américaine. Sa capacité de décryptage, bien que non connue, est très importante. A titre d'illustration, d'un point de vue informatique pour le cryptage des données, une clef à 56 bits de chiffrage est utilisée. Ce qui exigerait un grand nombre d'ordinateurs et de temps pour pouvoir décoder ce chiffrage (à sa sortie, on estimait qu'il y avait besoin de 14000 PC tournant ensemble pendant 13 mois pour casser le codage).

Mais dernièrement, un petit groupe de pirates informatiques est parvenu à casser ce chiffrage en trois jours seulement et cela avec un seul ordinateur. On n'oserait imaginer ce que la NSA est capable de faire alors avec ses propres capacités. D'ailleurs pour simplifier la chose, la NSA a imposé la mesure suivante au gouvernement américain : aucune technologie de cryptage ne peut être exportée hors des États-Unis sans une licence gouvernementale et sans que l'agence ne possède la clef de décryptage.

C'est ainsi qu'à regret, le gouvernement suédois a constaté que tout son système informatique sensible et confidentiel récemment installé, était aisément déchiffrable par la NSA.

5. *Le réseau Echelon*

a. *Aspects juridiques*

Echelon est le nom de code donné au réseau d'écoutes mondiales instauré par le pacte secret UKUSA entre les États-Unis et la Grande-Bretagne au début de la guerre froide, en 1947. Son but est le « Commint » (communications intelligence), autrement dit l'espionnage planétaire par tous les moyens technologiques possibles, des communications des pays du bloc soviétique.

À ce moment-là, le réseau était chapeauté par la CIA pour les États-Unis et par le GCHQ pour les Britanniques. Par la suite, le Canada, la Nouvelle-Zélande et l'Australie vinrent rejoindre le pacte.

b. *Du fonctionnement*

Le réseau Echelon est composé d'unités spatiales (120 satellites), d'unités sous-marines (boîtiers de dérivation de câbles transocéaniques) et d'unités terrestres (stations d'écoutes) comme celle basée à Menwith Hill dans le Yorkshire en Grande-Bretagne et d'autres disséminées un peu partout à travers le globe (dont en Allemagne, au Japon,...). En tout, il serait disposés quelque 52 sites semblables à celui de Menwith Hill dispersés à travers une vingtaine de pays.

Ces grands dômes blancs sont en fait des antennes paraboliques protégées par un radôme perméable aux ondes électromagnétiques, mais qui dissimule l'orientation de l'antenne. Sur le site en Grande-Bretagne, on dénombre pas moins de 26 antennes paraboliques et de par sa position géographique, elles peuvent capter les communications de tous les satellites au-dessus de l'Europe, ainsi que ceux de la Fédération de Russie et ceux du Maghreb et du Moyen-Orient, bien que ces communications ne représentent que 1% des communications européenne.

Sont ainsi interceptées toutes les communications radio, téléphones, fax et autres pour être envoyées à Fort Meade, Maryland, USA, pour analyse et traitement.

Actuellement, il est estimé selon des documents officiels de la NSA, que 2000 personnes travailleraient sur le site de Menwith Hill, dont 1200 Américains pour seulement 600 Britanniques. Les parlementaires britanniques ont interrogé leur ministre à ce point, inquiets d'une ingérence américaine dans le système. Dans la réponse à une question parlementaire, le ministre de la Défense souligne que : « *Il y a actuellement 600 employés britanniques servant à chaque niveau de la base et 1200 employés américains.* »

Figure 41 : Menwith-Hill (G-B)

5.2 *Son développement*

On savait depuis l'époque de la guerre du Vietnam que la NSA mettait sous surveillance tous les dissidents opposés à cette guerre. Ceci fut l'ouverture qui permit le déclenchement des opérations de surveillance pour toutes les personnes physiques et morales ayant des contacts avec les pays de l'Est.

Ainsi, la surveillance ne se limitait plus seulement au territoire américain, mais aussi à travers le monde. C'est à cette occasion que la NSA demanda d'avoir accès au programme Echelon afin de pouvoir intercepter les communications satellites. En théorie, il est très aisé de capter le signal d'un satellite.

Un satellite n'émet pas seulement sur un endroit précis, mais sur une large zone diffuse, donc le signal du satellite est accessible à tous. Il suffit alors d'une simple antenne et d'un décodeur pour recevoir le signal. De plus sur Internet, il est très commode de trouver les programmes d'orientation de la plupart des satellites INTELSAT en orbite.

Mais aujourd'hui, vu le flot incessant et en éternelle croissance des communications, il est impossible de mettre sur écoute chaque communication, il faut les trier et sélectionner celles qui représentent une utilité. Est donc utilisé par Echelon, un système dit de reconnaissance vocale qui scrute chaque communication à la recherche de mots-clefs préalablement définis dans un *dictionnaire*, et enregistre la conversation une fois le mot trouvé. Mais cette technologie est encore assez peu performante pour reconnaître tous les mots en temps réel.

Parallèlement à cela est aussi utilisée la technologie d'empreinte vocale, beaucoup plus performante et plus sélective. Dans ce cas-ci, des échantillons de voix suspectes sont stockés dans un fichier et dès qu'une de ces voix est interceptée dans une communication, la mise sur écoute s'opère. On voit que le système est plus performant dans le sens où même si le sujet de la conversation est détourné (ex. : dire farine au lieu de dire drogue), le sujet ne peut échapper à la mise sur écoute par sa voix. Les points faibles de cette technologie restant les voix inconnues ou non identifiées et celles qui sont électroniquement modifiées.

Ainsi, le réseau Echelon est au service de la mise sur écoute de bien des conversations, qui sont ensuite envoyées au siège de la NSA, à Fort Meade aux USA pour analyse et pour être éventuellement communiquées aux partenaires du pacte UKUSA, si elle le juge bénéfique.

6. *De sa découverte par le grand public*

Le rebondissement survient quand le membre d'une association britannique pour les droits du citoyen, Steve Wright présente un rapport devant le Parlement européen début 1998 dans lequel il affirme que toutes les communications européennes, tant militaires que civiles, sont interceptées par un réseau mondial d'espionnage mené par les États-Unis, avec la complicité de la Grande-Bretagne.

Déjà vers 1988, un journaliste anglais, Duncan Campbell avait attiré l'attention en écrivant un article pour le *New Statesman* à ce sujet. Et en 1996, le Néo-Zélandais Nicky Hager décrit très précisément dans son livre « *Secret Power. New Zeland's Role in the International Spy Work* » le système mis en place pour tracer les mots-clefs dans les conversations. Il y explique très clairement le fonctionnement du programme « *Memex* » mis au point par la société britannique *Memex Technology* pour la reconnaissance vocale.

Tout ceci fait office d'onde de choc au sein de la Communauté Européenne qui demande tout de suite au STOA (*Scientific and Technologic Options Assessements*) de prendre l'initiative en ce sens. Avec l'aide de Duncan Campbell, le groupe présente un nouveau rapport devant le Parlement où il met en exergue, les lacunes dans la protection des données au niveau européen. L'existence de la preuve d'espionnage industriel par Echelon n'est pas apportée, mais de sérieux indices en laissent la supposition. Et ce d'autant plus quand l'ex-directeur de la CIA James Woolsey lui-même confirma l' « *honnêteté intellectuelle* » du rapport. « *Suite a l'audition par le Parlement Européen de l'auteur Duncan Campbell, aucune critique sérieuse de ce rapport n'a d'ailleurs été formulée, même si l'auteur a été en défaut d'apporter des preuves formelles de tous les éléments de son rapport. Certains éléments de son rapport sont d'ailleurs basés sur des coupures de presse.* »

Par ailleurs, sur la très sérieuse émission d'investigation « *Sixthy Minutes* » de CBS, un ancien agent des services secrets canadiens, M. Frost a admis avoir été entraîné par la NSA à cette activité d'espionnage. Mais comme le souligne judicieusement M. Dinant dans le rapport du Comité R :

1. « Chaque activité humaine laisse de plus en plus de traces ; »

2. « le détenteur, la nature et le lieu de stockage de ces traces deviennent de moins en moins visibles par l'individu qui les laisse le plus souvent malgré lui ; »

3. « dans le même temps, la captation de ces traces invisibles laisse de moins en moins de traces visibles. »

Comme on le voit donc, il est très difficile de prouver non pas l'existence du réseau, mais son utilisation. Suite à ces déclarations, la réaction de la NSA ne se fit attendre. Le porte-parole du States Département, James P. Rubin, a nié toutes implications de la NSA dans l'espionnage industriel. « *The National Security Agency is not authorized to provide intelligence information to private firms. The agency acts in strict accordances with American law. […] U.S. intelligence agencies are not tasked to engage in industrial espionage or obtain trade secrets for the benefit of any U.S. company or companies.* » (ndlr : « l'Agence de Sécurité nationale n'est pas autorisée à fournir d'information d'intelligence aux sociétés privées. L'agence agit dans des accords stricts avec la loi américaine. […] des agences d'intelligence américaines ne sont pas autorisées à s'engager dans l'espionnage industriel ou obtenir des secrets de fabrication pour l'avantage de n'importe quelle société américaine ou compagnies. »)

7. *Du droit américain*

Le gouvernement américain répond aux allégeances européennes par le 4e amendement de la Constitution américaine compris dans le fameux Bill of Rights.

« *The right of the people to be secure in their persons, homes, papers and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be sized.* » (NDLR : « Le droit des citoyens d'être garantis dans leurs personnes, domiciles, papiers et effets, contre des perquisitions et saisies abusives ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est pour un motif plausible, soutenu par serment ou affirmation, ni sans qu'il décrive avec précision le lieu à fouiller et les personnes ou choses à saisir. »)

Cependant, il n'est pas certain que les États-Unis interprètent le texte selon les mêmes exigences imposées par la jurisprudence européenne. D'ailleurs comme nous l'avons vu plus haut, le contrôle politique de la NSA n'est pas direct et seulement effectué par la présidence et son office.

En conclusion, la protection américaine des citoyens en ce qu'elle est comparable aux modèles européens, n'existe que pour les citoyens américains. Ceci est d'autant plus significatif que les législations américaines de protections des citoyens, ainsi la Privacy Act de 1974 et le Freedom of Information Act de 1966, ne concernent également que les seuls citoyens américains.

8. *Des entreprises de pointes en Europe*

Après une longue période sombre de récessions, l'Europe se réveille économiquement et technologiquement. Surtout depuis que l'Euro a été instauré, une certaine solidité et un certain poids financier ont permis un nouveau décollage économique pour l'Europe. Nous sommes devenus les premiers concurrents des États-Unis et nous ne cessons de les fragiliser dans leur monopole mondial.

Et, à juste titre, de plus en plus d'entreprises européennes deviennent des leaders dans leur domaine d'activité, des fleurons de la nouvelle technologie et de la nouvelle économie. De plus en plus d'entreprises de pointe se développent sur le territoire européen, aidées par des investissements massifs et des politiques économiques avantageuses. Il en est de même pour la Belgique qui voit poindre sur son territoire des entreprises dites de nouvelles technologies ou de technologies de pointe. Tel est le cas d'IBA, société néo-louvaniste leader dans le marché du cyclotron et de la technologie d'imagerie médicale, ou bien d'autres sociétés spécialisées dans la biotechnologie, technologie dite très sensible à la concurrence et où la recherche de nouveaux procédés est le seul moteur de développement.

Le principe de ces technologies de pointe ou dites sensibles, est que celles-ci ne peuvent se développer que par la recherche scientifique et l'innovation, et non plus seulement par l'investissement économique comme ce fut le cas auparavant. On voit donc ici toute l'importance que revêt le secret professionnel et le

risque que représente la fuite des cerveaux ou de l'information. Mais dernièrement, plusieurs entreprises se plaignent d'avoir perdu de gros marché suite à une concurrence déloyale de la part de concurrents américains.

« En 1993, les participants français aux négociations du GATT sont tous espionnés et mis sur écoute.

En 1994, Thompson-CSF perd au Brésil un gigantesque contrat portant sur la création d'un système de surveillance des pluies en forêt amazonienne. Toutes les communications entre le groupe français et les autorités locales avaient été piratées, notamment celles concernant les pots-de-vin proposés à de nombreux officiels Brésiliens. Le bénéficiaire actuel de ce marché est Raytheon, une firme concurrente aux USA.

En 1995, échec d'une importante transaction entre Airbus et l'Arabie Saoudite, au profit de Boeing et de McDouglas. Ces mastodontes US, rivaux d'Airbus, avaient été informés de tous les coups de fil, de tous les fax échangés entre le consortium aéronautique européen et les Saoudiens, avec le détail des « cadeaux » proposés par Airbus aux « officiels », ce qui a permis aux firmes américaines d'être plus convaincantes. Bien évidemment, les sociétés françaises ne se sont pas vantées d'avoir subi une concurrence pour le moins déloyale. Protester revenait à avouer le versement illégal de pots-de-vin.

« Et chez nous en Belgique, très récemment, un ancien porte-parole de la société *Lernout & Hauspie* a admis devant les caméras de la RTBF, que sous la pression concurrentielle et sous la pression des bénéfices, ils avaient volontairement modifié les chiffres comptables pour avoir plus de liquidités, mais en gardant tout ceci au grand secret. L'étonnement pour l'entreprise, leader mondial de la technologie d'empreinte vocale et de reconnaissance vocale, fut l'ouverture d'une enquête contre elle pour fraude comptable. L'étonnement fut plus grand encore de savoir que cette instruction venait de Washington. Comment se fait-il qu'un parquet situé de l'autre côté de l'Atlantique soit au courant d'une telle manipulation financière ? Le doute persiste…

On voit donc combien il est crucial pour une entreprise de se protéger contre toute atteinte de l'extérieur, comme de l'intérieur. C'est pourquoi actuellement, la plupart du courrier électronique est filtré et sécurisé et qu'une étroite surveillance de l'information est organisée au sein des entreprises. Le problème restant de la sécurisation électronique. Il faut se rappeler que la NSA exige la clef de déchiffrement pour toute technologie de cryptage américaine destinée à l'exportation, et malheureusement, les États-Unis possèdent un monopole en la matière.

9. *Du point de vue juridique*

Dans la plupart des textes constituants européens, que ce soit dans les Constitutions, Traités, Lois fondamentales, les droits des individus sont protégés contre l'abus. Le rapport de 1999 du STOA fait un balayage de toutes les législations européennes en ce qui concerne la protection des individus ainsi que de la protection de données et des lois régissant les télécoms. Et il constate qu'à bien des égards, le réseau Echelon va à l'encontre de ces principes de droits. Il ne faut pas oublier non plus qu'il existe des lois dans certains pays de l'Union Européenne qui donnent un cadre aux surveillances et aux écoutes. Mais jamais ces lois ne peuvent servir à cautionner des abus comme c'est le cas actuellement avec le réseau Echelon. Seulement, un seul de ces pays cautionne le réseau, c'est la Grande-Bretagne. En effet, celle-ci en signant les accords du pacte UKUSA a donné son accord à l'espionnage européen mais en établissant des règles visant à protéger ses citoyens et ses firmes nationales. On voit donc ici, un viol des plus élémentaires de la Convention européenne des Droits de l'Homme et à l'article 6 du Traité d'Amsterdam relatif à la CEDH et à l'obligation qui incombe à chaque état membre de sécuriser les communications des ses nationaux ainsi que de tous les citoyens des autres pays membres.

Du point de vue belge, le parlement a adopté une loi organique des services de renseignement et de sécurité (Sénat 1-758/10,11 et 15 MB, 18 décembre 1988) qui transpose en droit belge les directives de

la Cour européenne des droits de l'homme, à maintes reprises réitérées par la jurisprudence du Conseil d'État, pour dénier tout droit de la Sûreté d'État et des services de renseignement à la collecte et aux traitements d'informations vis-à-vis de citoyens ou de manière plus large, d'individus. Malheureusement, cette loi n'est pas assez précise en son contenu sur l'application précise des écoutes téléphoniques.

Mais il faut dire que les principes à propos de la légitimité des interceptions de télécommunication sont récents et que la jurisprudence de la Cour européenne des droits de l'homme n'est constante que depuis la fin des années nonante. C'est ainsi que le Conseil de la Communauté européenne a adopté sous la pression américaine, le 17 janvier 1995, une résolution visant à faciliter les écoutes téléphoniques, à l'insu même du Parlement européen. On remarquera que cette résolution est précédée d'une déclaration signée conjointement par les autorités européennes et américaines. Le Conseil s'est justifié par le besoin d'une coopération entre le FBI et les polices nationales des pays membres dans une lutte contre la criminalité.

Suite à toutes ces révélations et les inquiétudes qu'elles ont provoquées, plusieurs parlements européens entamèrent des démarches afin d'approfondir le sujet. Les parlementaires britanniques posèrent plusieurs questions à la Chambre des Lords du Royaume-Uni dont leurs ministres ont donné à chaque fois des réponses assez vagues motivées par le secret défense.

La Chambre des Représentants de Belgique a commandé une enquête auprès du Comité R afin d'étudier la question des interceptions des communications belges par Echelon. A la remise de son rapport, le Comité R fit remarquer que ni la Sûreté d'État, ni les Services Généraux de Renseignement n'avaient mandat en cette matière et que de toute façon, ils n'ont pas assez de personnel et encore moins de personnes qualifiées pour étudier cette matière.

En France, une commission d'enquête fut crée par le député UDF Arthur Paecht afin de mener une enquête sur le sujet. Celle-ci, au moment de rendre son rapport au nom de la Commission de la Défense et des forces armées, sera obligée de conclure sur un échec suite aux fins de non-recevoir des États-Unis et de la Grande-Bretagne quant aux questions que la Commission leur a posées.

Pour ce qui en est des Communautés européennes, la création d'une commission d'enquête souleva tout d'abord de larges débats très houleux difficilement régulés par la Présidente du Parlement, Nicole Fontaine. Finalement à la clôture des débats, une commission d'enquête sans aucun pouvoir d'investigation sera créée par concession à la Présidente du Parlement, qui sous la pression américaine, ne voulait créer aucune commission.

Cette commission n'a rendu qu'un rapport exhaustif ce lundi 6 juin qui devra encore être soumis à l'approbation du Parlement. A l'heure où il est, je n'ai malheureusement pas encore pu consulter ce rapport entièrement. Mais déjà par les échos de la presse, nous pouvons considérer que ce rapport n'apporte aucune preuve formelle des activités d'Echelon, car les demandes d'information et de visites du siège de la NSA par les eurodéputés à Washington sont restées lettre morte.

10. *Des recommandations*

Le système Echelon représente un risque difficilement mesurable pour l'Europe. Ce risque dépend de nombreux paramètres dont certains ne sont pas connus comme la puissance de cryptage et l'ampleur des moyens techniques et humains mis en œuvre. Les experts du rapport du Comité R recommande donc d'appliquer le principe de précaution énoncé par N. de Saedeleer.

« *Le principe de précaution devrait aussi consolider l'approche préventive en forçant les pouvoirs publics à agir alors même qu'ils ne disposent pas de toutes les preuves justifiant le bien-fondé de leur action. […] Alors que la certitude appelle une attitude de prévention, l'incertitude requiert la précaution.* »

Souvent ce principe a été évoqué pour des domaines comme la santé ou de l'environnement, mais l'Organisation Mondiale du Commerce a déjà demandé que ce genre de principes soit appliqué aux informations personnelles et économiques, quitte à en limiter la liberté des échanges.

Il se pose aussi le problème de la souveraineté. Le message écouté se trouvant dans le domaine extra-atmosphérique et la station d'écoute se trouvant en domaine territorial étranger, il y a conflit de domaines dans le sens où aucun lien n'unit les deux et ce qui laisse un certain vide juridique. Peut-on permettre la captation de messages confidentiels sous le prétexte qu'ils se trouvent en dehors de la souveraineté du destinataire et de l'émetteur, et que donc ils n'appartiennent à personne et sont libres d'être saisis ? La question n'est pas tranchée.

Une autre recommandation serait de développer une technologie de chiffrement européen, libre de toute contrainte américaine et de pousser le cryptage jusqu'à ses plus fortes valeurs afin de rendre la tâche du décryptage illicite encore plus difficile (utiliser une clef à 128 bits au lieu d'une clef à 56 bits comme c'est le cas aujourd'hui). Il serait aussi très intéressant de créer un organisme européen des communications, à l'image de l'IBPT en Belgique, mais avec un pouvoir de contrôle des activités puissant pour la sécurité tout en laissant le jeu de la libre concurrence fonctionner.

Mais une des mesures les plus urgentes à faire, est déjà de renforcer les législations européennes contre les écoutes téléphoniques illégales selon les recommandations du STOA dans ses différents rapports. Améliorer la communication entre les États-Unis et l'Union européenne permettrait de faciliter aussi la chose, et surtout de clarifier certains points.

Enfin, à la mesure de la création d'un organisme européen des télécommunications, il serait intéressant de — sinon pas créer un organisme des services de renseignements européen — de pousser à la coopération accrue entre tous les services de renseignements des pays membres.

11. *Conclusion*

On comprend maintenant l'enjeu de la sécurité des communications, tant privées que publiques et des répercussions que peut avoir l'espionnage économique sur une entreprise. D'autant plus qu'avec le réseau Echelon, cet espionnage économique a pris une tout autre tournure et des proportions alarmantes et astronomiques. L'existence du réseau Echelon n'est plus à prouver, car maintes fois prouvée par des documents officiels ou des déclarations publiques, mais son activité reste toujours à prouver. Et tant que les États-Unis ne voudront pas clarifier la chose, il sera difficilement envisageable à la vue des technologies actuelles de prouver son activité, si illicite elle est vraiment.

Mais le risque est qu'une fois qu'une technologie soit découverte ou sur le point de l'être, qu'il soit possible que celle-ci soit déjà remplacée par une autre encore secrète et bien plus performante. D'ailleurs, on parle déjà du fait que les États-Unis fermeraient leurs bases au profit de l'usage de satellites dotés d'une nouvelle technologie bien supérieure à celle utilisée par Echelon. Mais c'est ici qu'il faut distinguer la réalité de l'imagination et de la paranoïa.

Comme je l'ai rappelé en début de cette étude, je n'ai eu accès qu'à des sources très limitées. C'est pourquoi je n'irai pas plus loin dans cette conclusion sans en savoir plus.

Ce document vient du site *Opération Fiat-Lux* ; c'est un des grands classiques quand on parle du Réseau Echelon et de l'action des Américains en la matière.

« *Pourquoi nous espionnons nos alliés* », par James Woolsey, ancien directeur de la CIA 1993-1995 (*Washington Post* du 17 mars 2000)

« À quoi rime cette agitation au sujet d'Echelon et des États-Unis espionnant les industries européennes ? Nous commencerons par un peu de franchise du côté américain. Oui, chers amis du continent européen, nous vous avons espionnés. Et il est vrai que nous utilisons des ordinateurs pour trier les données grâce à des mots clés. Vous êtes-vous posé la question de savoir ce que nous cherchons ?

Le récent rapport au Parlement européen sur Echelon, écrit par le journaliste britannique Duncan Campbell, a déclenché de furieuses accusations, en provenance de l'Europe continentale, selon lesquelles les services de renseignement américains volent les technologies avancées des compagnies européennes pour que nous puissions — notez-le — les donner aux compagnies américaines pour les aider à rester compétitives. Mes amis européens, redescendez sur terre. C'est vrai, dans une poignée de domaines, la technologie européenne surpasse l'américaine, mais, pour le dire aussi aimablement que possible, ces domaines sont en très, très, très petit nombre.

La plupart des technologies européennes ne méritent pas que nous les volions.

Pourquoi, donc, nous avons vous espionnés ? La réponse se trouve dans le rapport Campbell, dans l'analyse des deux seuls cas où il est dit que des compagnies européennes auraient été les cibles de la collecte américaine de renseignements. À propos de Thomson-CSF, le rapport indique : « *la compagnie était largement suspectée d'avoir corrompu des membres du comité de sélection du gouvernement brésilien.* ». D'Airbus, il dit que nous avons pu prouver que « *ses agents offraient des pots-de-vin à un officiel Saoudien.* » Ces faits sont systématiquement omis dans les articles de presse européens.

Eh oui, chers amis continentaux, nous vous avons espionnés parce que vous distribuez des pots-de-vin. Les produits de vos compagnies sont souvent plus coûteux, moins avancés sur le plan technologique, ou les deux à la fois, que ceux de vos concurrents américains. En conséquence de quoi vous pratiquez beaucoup la corruption. Vos gouvernements sont tellement complices que dans plusieurs pays européens les pots-de-vin sont encore déductibles des impôts.

Lorsque nous vous avons pris la main dans le sac, nous n'avons pas dit un mot aux compagnies américaines qui étaient vos concurrents. Nous sommes allés, au contraire, voir les gouvernements que vous soudoyez pour prévenir les officiels que nous ne prenions pas cette corruption à la légère. Ils réagissent souvent en accordant tout ou partie du contrat à l'offre la plus méritoire (parfois américaine, parfois non). Cela vous choque, crée parfois des tensions entre vos corrupteurs et les corrompus des autres pays, et devient à l'occasion un scandale public. Nous adorons cela.

Pourquoi faites-vous usage de la corruption ? Ce n'est pas parce que vos compagnies sont fondamentalement plus corrompues ; ni parce que votre technologie est moins bonne. C'est parce que votre Saint Patron économique est Jean-Baptiste Colbert, quand le nôtre est Adam Smith. En dépit de quelques récentes réformes, vos gouvernements dominent encore largement votre économie, ce qui fait que vous éprouvez des difficultés plus grandes que nous à innover, à encourager la mobilité du travail, à réduire les coûts, à attirer le capital vers les secteurs économiques les plus prometteurs et à vous adapter rapidement aux évolutions de l'environnement. Vous préféreriez ne pas avoir à affronter la difficulté du changement qui vous éloignerait du dirigisme. Il est tellement plus facile de continuer à verser des pots-de-vin…

La Central Intelligence Agency collecte d'autres renseignements d'ordre économique, mais dans leur vaste majorité ce ne sont pas des secrets volés. Il y a quatre ans, la Commission Aspin-Brown a montré qu'environ 95 % des informations des États-Unis provenaient de sources ouvertes.

Le rapport Campbell décrit une sinistre rencontre à Washington où — j'en frémis ! — du personnel de la CIA est présent et où les participants — tenez-vous bien – « *identifient les contrats majeurs ouverts à proposition* » en Indonésie. M. Campbell, je suppose, imagine quelque chose comme ceci : un espion malin sort à pas feutrés d'une maison sûre, change de tenue, vérifie qu'il n'est pas sous surveillance, se coordonne avec un satellite espion et... achète un journal indonésien.

Si vous autres Européens croyez réellement que nous allons jusqu'à l'absurde pour obtenir des informations disponibles de manière publique, pourquoi ne vous moquez-vous pas de nous au lieu de vous montrer offensés ?

Quels sont les secrets économiques, au-delà des tentatives de corruption, que nous avons voulu obtenir par l'espionnage ? Il s'agit par exemple des tentatives de certaines sociétés de masquer le transfert de technologies à usage dual. Nous suivons de près les ventes de superordinateurs et de certains produits

chimiques, car ils peuvent être utilisés non seulement pour des objectifs commerciaux, mais aussi pour produire des armes de destruction massive. Un autre concerne les activités économiques dans les pays soumis à des sanctions — l'activité bancaire serbe, le trafic de pétrole irakien.

Mais collectons-nous, ou même trions-nous des renseignements secrets au bénéfice de compagnies américaines spécifiques ? Même M. Campbell admet que nous ne le faisons pas, bien qu'il ne réussisse à le formuler qu'à l'aide d'une double négation : « *En général, ce n'est pas incorrect*. » La Commission Aspin-Brown était plus explicite : « *Les agences de renseignement américaines n'ont pas pour mission de s'engager dans "l'espionnage industriel" — c'est-à-dire d'obtenir des secrets industriels et commerciaux pour le compte d'une ou de plusieurs compagnies des États-Unis.* »

Le gouvernement français est en train de former une commission pour enquêter sur tout cela. J'espère que les enquêteurs viendront à Washington. Nous devrions organiser deux séminaires à leur intention. L'un aurait pour sujet notre *Foreign Corrupt Practice Act* et comment nous l'utilisons, assez efficacement, pour décourager les compagnies des États-Unis de corrompre des gouvernements étrangers. Le second aborderait la question de savoir pourquoi Adam Smith est un meilleur guide que Colbert pour les économies du XXI^{e} siècle. Puis nous pourrions parler d'espionnage industriel, et nos visiteurs pourraient nous expliquer, s'ils réussissent à garder leur sérieux, qu'ils ne le pratiquent pas. La prochaine commission s'intéressera-t-elle au manque de politesse des maîtres d'hôtel américains ?

Européens, soyez sérieux. Cessez de nous critiquer et réformez vos propres politiques économiques étatiques. Vos entreprises deviendront plus efficaces et innovantes, elles n'auront alors plus besoin de la corruption pour faire face à la concurrence.

Et nous, nous n'aurons plus besoin de vous espionner. »

Ce document portait comme introduction :

À la fin des années 80, les Américains prennent une décision qu'ils regrettent probablement : elle vise à inciter la Nouvelle-Zélande à adhérer à un nouveau et très secret système de renseignement mondial. L'enquête de Hager à l'intérieur du système et la découverte des dictionnaires Echelon l'ont mené à révéler l'un des plus grands projets de renseignement, la plus grande partie en étant tenue secrète. Le système permet aux agences d'espionnage d'être à l'écoute de la plupart des téléphones, email et communications par télex à travers le monde.

Le système de surveillance mondial démasqué

Pendant 40 années, la plus grande agence de renseignements de Nouvelle-Zélande, le Bureau de la Sécurité des Communications du Gouvernement (GCSB) l'équivalent de l'Agence de la Sécurité Nationale Américaine (NSA), avait aidé ses alliés de l'Ouest à espionner des pays de la région du Pacifique, sans que la population de la Nouvelle-Zélande ou même beaucoup de ses plus hauts fonctionnaires élus ne soient au courant.

Ce que la NSA ne savait pas c'est qu'à la fin des années 80, plusieurs membres du personnel des renseignements avaient décidé que ces activités avaient été tenues secrètes pendant trop longtemps, et me fournissaient des interviews et des documents qui exposaient les activités de renseignements de la Nouvelle-Zélande. Finalement, plus de 50 personnes qui travaillent ou ont travaillé dans les renseignements et dans des domaines apparentés ont consenti à être interviewées. Les activités qu'ils ont décrites, provenant du Pacifique Sud, permettent de se documenter, sur quelques systèmes d'alliances larges et projets qui ont été gardés secrets. Le système Echelon est de loin le plus important d'entre eux.

Conçu et coordonné par la NSA, le système Echelon est utilisé pour intercepter email, fax, télex, et communications téléphoniques transportés sur les réseaux de télécommunications mondiaux.

Contrairement à beaucoup de systèmes d'espionnage électronique développés pendant la Guerre Froide, le système Echelon est conçu à l'origine pour des cibles non militaires : il vise gouvernements, organisations, entreprises, et individus dans virtuellement chaque pays. Il affecte potentiellement chaque personne qui communique entre (et quelquefois dans) des pays n'importe où dans le monde.

Ce n'est bien sûr pas une nouveauté que les organisations de renseignements mettent sur écoute des emails et autres réseaux de télécommunications publics. Ce qui était nouveau en matière de fuite par le personnel des renseignements de la Nouvelle-Zélande était la précision de l'information sur où l'espionnage est fait, comment le système travaille, ses capacités et ses défauts, et beaucoup de détails tels que les noms de code.

Le système Echelon n'est pas conçu pour intercepter les emails ou les liaisons par fax d'un individu particulier. Le système travaille plutôt en interceptant de très grandes quantités de communications sans faire de distinction et en utilisant des ordinateurs afin d'identifier et d'extraire des messages dignes d'intérêt de la masse de ceux non désirés. Une chaîne d'installations d'interceptions secrètes a été établie autour du monde pour mettre sur écoute tous les composants majeurs des réseaux de télécommunications internationaux. Quelques-unes sont à l'écoute des satellites de communications, d'autres basées à terre à l'écoute des réseaux de communications, et enfin, d'autres à l'écoute des communications par radio. Le système Echelon lie toutes ces installations ensemble et fournit aux États-Unis et à ses alliés la capacité d'intercepter une grande proportion des communications sur la planète.

Les ordinateurs de chaque station dans le réseau Echelon recherchent automatiquement à travers les millions de messages interceptés ceux qui contiennent des mots-clés préprogrammés. Les mots-clés incluent tous les noms, localités, sujets qui peuvent être mentionnés, et ainsi de suite. Chaque mot de chaque message intercepté à chaque station est recherché automatiquement, qu'il s'agisse d'un numéro de téléphone spécifique ou d'une adresse email présents ou non sur la liste. Les milliers de messages reçus simultanément sont lus en temps réel au moment même où ils arrivent dans la station, heure après heure, jour après jour, et l'ordinateur trouve des renseignements : l'aiguille dans les meules de foin que représentent les télécommunications.

Quelqu'un écoute !

Les ordinateurs dans les stations autour du globe sont reliés entre eux, tout comme les *Dictionnaires* du système Echelon, dans la limite du réseau. Les ordinateurs peuvent rechercher automatiquement à travers le trafic des mots-clés qui existent depuis au moins les années 70, mais le système Echelon a été conçu par la NSA pour interconnecter tous ces ordinateurs et permettre aux stations de fonctionner comme composantes d'un tout intégré. La NSA et le GCSB sont liés par un accord anglo-américain sur les signaux de renseignements (SIGINT) regroupant cinq pays. Les trois autres partenaires avec des noms également obscurs sont les Quartiers généraux des Communications du Gouvernement (GCHQ) en Grande-Bretagne, l'Établissement de la Sécurité des Communications (CSE) au Canada, et le Conseil d'administration de Signaux de Défense (DSD) en Australie.

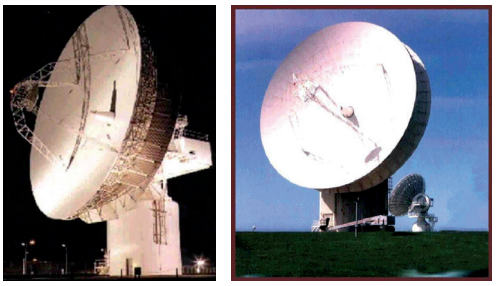
L'alliance, qui a grandi grâce à des efforts de coopération pour intercepter des transmissions radio pendant la Deuxième Guerre mondiale, a été organisée dans le cadre de l'accord anglo-américain en 1948 et était dirigée à l'origine contre l'URSS. Les cinq agences anglo-américaines sont aujourd'hui les plus grandes organisations de renseignements dans leurs pays respectifs. Avec le business mondial qui a lieu par fax, email, et téléphone, l'espionnage de ces communications reçoit la plus grosse partie des ressources du Renseignement.

Pendant les décennies qui précédèrent l'introduction du système Echelon, les alliés anglo-américains ont travaillé dans la collecte du renseignement pour l'un et pour l'autre, mais chaque agence avait pour habitude de traiter et d'analyser les interceptions de ses propres stations. Dans le cadre d'Echelon, un ordinateur *Dictionnaire* d'une station particulière contient non seulement les mots-clés choisis par son

agence mère, mais aussi des listes entrées par les autres agences. Dans la station d'interception satellite de Nouvelle-Zélande à Waihopai (dans l'Île du sud), par exemple, l'ordinateur a des listes de recherche distinctes pour la NSA, le GCHQ, le DSD, et le CSE en plus de la sienne. Quand le *Dictionnaire* rencontre un message contenant un des mots-clés des agences, il le sélectionne automatiquement et l'envoie directement aux quartiers généraux de l'agence intéressée. Personne en Nouvelle-Zélande ne filtre, ou même voit, les renseignements collectés par la station de Nouvelle-Zélande pour les agences étrangères. Par conséquent, les stations des plus jeunes alliés des Anglo-américains fonctionnent pour la NSA comme si ces stations étaient sur le sol américain.

Le premier composant du réseau Echelon est constitué des stations qui ont pour cible les satellites de télécommunications internationaux (Intelsat) utilisés par les compagnies de téléphone de la plupart des pays. Une ceinture de satellites Intelsat est placée autour du monde, stationnaires au-dessus de l'équateur, chacun desservant une station-relais pour des dizaines de milliers de coups de téléphone simultanés, fax, et emails. Cinq stations anglo-américaines ont été établies pour intercepter les communications transmises par l'Intelsat.

La station GCHQ britannique est localisée au sommet de hautes falaises surplombant la mer à Morwenstow dans la région des Cornouailles. À côté des tentaculaires bâtiments des opérations, les antennes paraboliques sont pointées en direction des satellites Intelsats au-dessus de l'Atlantique, de l'Europe et inclinées presque à l'horizontale pour l'Océan Indien.



Les antennes de Morwenstow

Une station de la NSA à Sugar Grove est implantée à 250 kilomètres au sud-ouest de Washington DC (District de Columbia), dans les montagnes de l'ouest de la Virginie, elle couvre les satellites Intelsat de l'Atlantique transmettant en direction de l'Amérique du Nord et du Sud. Une autre station de la NSA est dans l'État de Washington, à 200 kilomètres au sud-ouest de Seattle, à l'intérieur du Centre de tir Yakima de l'armée. Ses antennes paraboliques sont pointées en direction des satellites Intelsat du Pacifique et de l'Est.

Le travail d'interception des communications Intelsat du Pacifique qui ne peuvent être interceptées à Yakima revient à la Nouvelle-Zélande et à l'Australie. Leur emplacement dans le Pacifique Sud aide à assurer l'interception mondiale. La Nouvelle-Zélande fournit la station de Waihopai et l'Australie celle de Geraldton située dans l'ouest de l'Australie (laquelle cible les satellites Intelsat des océans Pacifique et Indien).

Chacun des ordinateurs *Dictionnaire* des cinq stations a un nom de code pour le distinguer des autres dans le réseau. La station de Yakima, par exemple, localisée dans une région désertique entre les Saddle Mountains et Rattlesnake Hills, a le *Dictionnaire COWBOY*, pendant que la station Waihopai a le *Dictionnaire FLINTLOCK*. Ces noms de code sont enregistrés au début de chaque message intercepté, avant qu'ils soient transmis au réseau Echelon et permettent aux analystes de reconnaître dans quelle station a eu lieu l'interception.

Le personnel des renseignements de Nouvelle-Zélande est impliqué de près avec la station Yakima de la NSA depuis 1981, quand la NSA a poussé le GCSB à contribuer à un projet d'interception des com-

munications diplomatiques japonaises. Depuis lors, l'ensemble des cinq agences anglo-américaines est responsable de l'écoute des câbles diplomatiques de tous les postes japonais dans la partie du globe qui leur est assignée. Jusqu'à l'intégration de la Nouvelle-Zélande dans le système Echelon avec l'ouverture de la station Waihopai en 1989, sa part de communications japonaises était interceptée à Yakima et envoyée non traitée aux quartiers généraux GCSB à Wellington pour décryptage, traduction, et transcription dans le format des rapports de renseignements (la NSA fournit le programme de décodage).

Communication par satellites

Un autre composant du système Echelon intercepte une gamme de communications par satellites qui ne sont pas transmises par Intelsat. En plus des stations anglo-américaines visant les satellites Intelsat, il y a encore cinq stations ou plus, pointées sur les satellites de communications de la Russie et d'autres régions du globe. Ces stations sont Menwith Hill dans le nord de l'Angleterre ; Shoal Bay, à l'extérieur de Darwin dans le nord de l'Australie (qui cible les satellites indonésiens) ; Leitrim, juste au sud d'Ottawa au Canada (qui semble intercepter les satellites latino-américains) ; Bad Aibling en Allemagne ; et Misawa dans le nord du Japon.

Un groupe d'installations basé à terre et qui se met directement à l'écoute des systèmes de télécommunications est le dernier élément du système Echelon. En plus des satellites et des communications radio, l'autre moyen important pour transmettre de grandes quantités de communications pour les particuliers, pour le business, et les gouvernements, est une combinaison de câbles déposés au fond des océans et des réseaux de micro-ondes sur terre. Les câbles lourds, déposés au fond des mers entre les pays, représentent un grand nombre de communications internationales à travers le monde. Lorsqu'ils sortent de l'eau pour rejoindre les réseaux de micro-ondes basés à terre, les câbles sont très vulnérables aux interceptions. Les réseaux de micro-ondes sont composés d'antennes situées au sommet de collines qui relaient des messages (toujours dans la ligne de vue) à travers la campagne. Ces réseaux transfèrent de grandes quantités de communications à travers un pays. L'interception de ces réseaux donne accès aux communications sous-marines internationales (une fois que les câbles refont surface) et aux communications interurbaines internationales à travers les continents. Ils sont aussi une cible évidente pour l'interception à grande échelle de communications domestiques.

Parce que les installations nécessitaient, pour intercepter les communications radio et satellite, l'utilisation de grandes antennes et paraboles qui sont difficiles à cacher, on est assez bien documenté sur ce réseau. Mais tout ce qui est nécessaire pour intercepter des réseaux de communication basés à terre est un bâtiment situé le long du chemin des micro-ondes ou un câble souterrain caché allant du réseau légitime à un quelconque bâtiment anonyme, peut-être prélevé loin. Bien que cela semble techniquement très difficile, l'interception des micro-ondes de l'espace par les satellites-espions des États-Unis a aussi lieu. Le réseau mondial d'installations pour intercepter ces communications est en grande partie non documenté, et comme le GCSB de la Nouvelle-Zélande ne participe pas à ce type d'interception, mes sources à l'intérieur du GCSB ne pouvaient pas non plus m'aider.

Ce document est extrait du Rapport du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon) de 2001.

Synthèse des apports de Nicky Hager

Dans le livre de l'auteur néo-zélandais, Nicky Hager, *Secret Powers – New Zealand's role in the international spy network*, paru en 1996, le système Echelon est décrit pour la première fois dans le détail. Il se base sur des entretiens avec plus de 50 personnes employées par le service de renseignement néo-zélandais ou engagés par ailleurs dans des activités de renseignement. De plus, il a analysé de nombreux documents provenant des archives nationales des journaux et d'autres sources publiques. D'après Hager,

le système est dénommé Echelon et les ordinateurs du réseau sont dénommés « *Dictionnaires* Echelon ».

Selon l'auteur, l'origine du système Echelon remonte à 1947, année où, dans le prolongement de la coopération de l'époque de guerre, le Royaume-Uni et les États-Unis sont convenus de poursuivre à l'échelle mondiale pour ainsi dire les activités de « renseignement transmissions » (COMINT). Ces deux pays devaient collaborer pour mettre en place un système d'interception autant que possible mondial, étant entendu qu'ils se partageraient les équipements spécifiques nécessaires à cet effet, ainsi que les dépenses occasionnées, et qu'ils auraient l'un et l'autre accès aux résultats.

Par la suite, le Canada, l'Australie et la Nouvelle-Zélande ont adhéré au pacte UKUSA.

Selon Hager, l'interception des communications satellitaires constitue l'élément central du système actuel. Dès les années 70, les communications acheminées par Intelsat — le premier système mondial de télécommunications par satellites — furent interceptées par des stations au sol. Ces informations étaient alors étudiées au moyen d'ordinateurs sur la base de mots-clés ou d'adresses préprogrammés pour filtrer les informations importantes. Par la suite, la surveillance a été étendue à d'autres satellites, comme par exemple ceux d'Inmarsat, organisation dont les activités concernent principalement les communications maritimes.

Hager signale dans son livre que l'interception des communications satellitaires ne constitue qu'une composante — certes importante — du système d'interception géant. Parallèlement, il existerait de nombreuses autres installations de surveillance du faisceau hertzien et des câbles, à propos desquelles les documents sont toutefois moins nombreux et dont il est difficile de prouver l'existence, dès lors que contrairement aux stations au sol, elles peuvent pratiquement passer inaperçues.

Echelon est ainsi devenu le synonyme d'un système d'interception mondial.

Dans l'exposé qu'il a fait le 24 avril 2001 devant la Commission temporaire sur Echelon, Hager a souligné que le système d'interception n'était pas tout puissant. Étant donné qu'il faut utiliser au mieux les ressources limitées, tout ne peut pas être intercepté : il faut se contenter de ce qui promet des informations importantes. Les objectifs sont donc en général constitués par des informations politiques et diplomatiques. Si l'interception a pour objectif d'obtenir des informations économiques, celles-ci s'inscrivent plus dans un contexte macroéconomique que microéconomique. S'agissant des méthodes de travail du système, chaque partenaire a ses propres listes de mots clés.

En outre, les communications sont également analysées sur la base de mots clés injectés dans le système par les États-Unis au moyen de « *Dictionnary managers* ». Les Britanniques n'ont aucun contrôle sur cet aspect et ignorent quelles informations sont collectées à Morwenstow parce que celles-ci sont directement transmises aux États-Unis.

Dans ce contexte, Hager a souligné le risque que peuvent constituer les stations d'interception britanniques pour l'Europe continentale. Citant de nombreux exemples, il a fait observer que les partenaires UKUSA du Pacifique espionnaient leurs alliés et leurs partenaires commerciaux. Les seules personnes qui échappaient à l'espionnage étaient les partenaires UKUSA.

Il a estimé que les services secrets britanniques et les Néo-zélandais seraient sans doute très réticents à compromettre le partenariat UKUSA en refusant de coopérer et d'écouter l'Europe continentale. Rien n'inciterait le Royaume-Uni à renoncer à des informations intéressantes et, étant donné qu'elles sont toujours secrètes, l'espionnage pratiqué dans le cadre UKUSA n'exclurait pas une politique officielle de loyauté vis-à-vis de l'Europe.

Ce document vient du site de notre partenaire *Intelligence Stratégique*. (revue de presse)

Surveillance électronique planétaire

Dispersées à la surface du globe, les bases militaires du réseau anglo-américain Echelon focalisent de nouvelles possibilités de surveillance planétaire. L'utilisation de satellites pour retransmettre les communications permet aux services secrets des principales puissances de capter, à la volée, les conversations téléphoniques, les fax, les courriers électroniques. Echelon intercepte plus de deux millions de conversations à la minute. « *En 1994, explique Duncan Campbell, la NSA (l'agence de sécurité nationale des États-Unis) a intercepté des appels téléphoniques entre Thomson CSF et le Brésil au sujet de Sivam, un système de surveillance pour la forêt amazonienne d'une valeur de 1,4 milliard de dollars. La compagnie française fut accusée par les Américains d'avoir versé des pots-de-vin à des membres du comité de sélection brésilien. À la suite de l'intervention américaine, le contrat fut finalement signé avec Raytheon, une société américaine.* » Duncan Campbell fut le premier journaliste à dénoncer, en 1988, l'existence de ce réseau ; il livre ici les clés d'Echelon — et en indique les limites.

Source : *Le Monde Diplomatique* (Août 2001)

USA vs World

Bien loin des jeunes loups BCBG qui délivrent du scoop à la demande, Duncan Campbell est un journaliste écossais aguerri à la quête d'informations. Peu de sensationnel dans ses propos, mais une analyse précise et documentée d'Echelon, grand automate de l'espionnage planétaire.

Rencontre avec le plus flegmatique des espions freelances.

Une des questions les plus simples porte sur l'existence même d'Echelon. La réponse est qu'Echelon existe pour le simple fait que nous le voyons. N'importe qui peut le voir. Et même si les Américains utilisent beaucoup de surnoms pour le nommer, nous savons qu'il existe un système de surveillance planétaire, quelle que soit sa dénomination. En décembre 1995, des documents de la CIA ont même donné des détails précis sur Echelon, même s'ils ont supprimé son nom de tous les documents mis à disposition du public. Dans ces pages, tous les sites d'Echelon étaient même précisés et les tâches de chaque site détaillées : Porto Rico, West Virginia, etc., tous ont des antennes satellites blanches, énormes, facilement repérables.

Tout au long des années 90, les informations ont circulé et les sites se sont graduellement révélés au grand public. Les missions même de chaque station Echelon sont clairement définies et accessibles à n'importe quel quidam dans les bibliothèques. Il y a ainsi beaucoup plus de preuves réelles de l'existence d'Echelon que pour nombres de projets des services secrets américains dont l'existence n'est jamais remise en cause. Il n'y a rien à rajouter à ces documents : ils parlent d'eux-mêmes.

Des amis se sont même introduits avec une simple échelle dans une station Echelon et ont pris des photos. Le paysage de l'intérieur est très ordinaire : des milliers d'ordinateurs et aucun être humain, car tout marche automatiquement. Ils ont réussi à pénétrer sur le site en franchissant tout simplement la barrière électrisée sans être touchés. Je sais parfaitement comment ils ont procédé, mais je n'ai pas le droit de dévoiler tous les détails, qui doivent rester secrets.

Sur les bureaux d'Echelon, des dizaines de manuels sur Internet et quelques cendriers vides...

Echelon, qualité filtre

Echelon est avant tout un énorme filtre planétaire. Le système filtre près de deux millions d'emails par heure pour n'en retenir que quatre environs. Le principe ? Un croisement de mots-clés qui permettent aux automates de traitement de dégager les emails intéressants à étudier en détail. Et même si Echelon filtre les données avec près de 10 000 mots-clés, il ne faut pas se leurrer : beaucoup de messages

passent à travers les mailles du filet. Mais le système est tout de même relativement intelligent : si trop de mots-clés polluent le message, Echelon ne les traite pas, ce qui exclue toute saturation du système par un *spamming* (note : envoi massif de messages) d'emails bardés de mots-clés.

Les cibles sont ainsi autant personnelles que généralistes. Tout le monde passe par Echelon, bien sûr, mais combien de messages sont réellement lus ? C'est en cela surtout qu'il faut modérer la paranoïa, même s'il faut rester vigilant. Echelon ne peut, de par le flot considérable de messages transitant dans le monde entier, voir et entendre tout le monde. Mais s'il y a des directives précises à propos d'un individu, effectivement, tout est alors possible.

Genèse des travaux

(...) J'ai commencé toutes ces recherches en 1988 aux États-Unis. Les services secrets en parlaient alors sous le numéro de code P415 mais rien n'a réellement filtré avant presque dix ans. C'était un travail effectué pour l'hebdomadaire britannique *The New Statesman*. J'ai poursuivi ce travail grâce aux fonds de la Communauté Européenne et la publication de mes premiers rapports a fait beaucoup de bruit dans le petit monde de l'intelligence économique. J'ai eu énormément de demandes suite à ces travaux, ce qui m'a permis de continuer dans de bonnes conditions. A chaque fois que j'allais donner une conférence dans un pays, je demandais toujours à aller visiter la station Echelon locale. Et presque toujours, il y en avait une dans les environs... J'ai sûrement été dans plus de stations Echelon qu'un espion américain moyen !

En 1997, le Parlement européen a publié un premier rapport sur Echelon effectué par Dr. Steve Wright (note : « *An apraisal of technologies of political control* »), où il consacrait dans cette large analyse une petite partie à Echelon. Et les gens se sont uniquement focalisés sur les passages évoquant le système d'écoute. Après que l'information ait circulé dans la presse européenne, le Parlement a voulu de nouvelles études sur le sujet. Seule une petite part m'a été commandée, mais sur les quatre rapports, c'est le mien qui a été remarqué, même s'il ne devait être qu'un rapport complémentaire aux trois autres. C'était le plus conséquent et le mieux documenté.

Méthodes de travail

Je travaille dans des conditions quasiment académiques. Comme un étudiant qui fait ses recherches en fait. Principalement seul, même si j'ai de nombreux contacts dans chaque pays. Par exemple, je n'ai accès qu'aux archives américaines disponibles au commun des mortels. Mais il y en a plus qu'on ne peut le penser au premier abord... Mes sources sont à la fois des faits révélés dans des livres, les journaux, etc., mais aussi des sources privées et académiques qui me sont transmises par des contacts. Ces personnes vont prendre des photographies, capter des signaux audio.

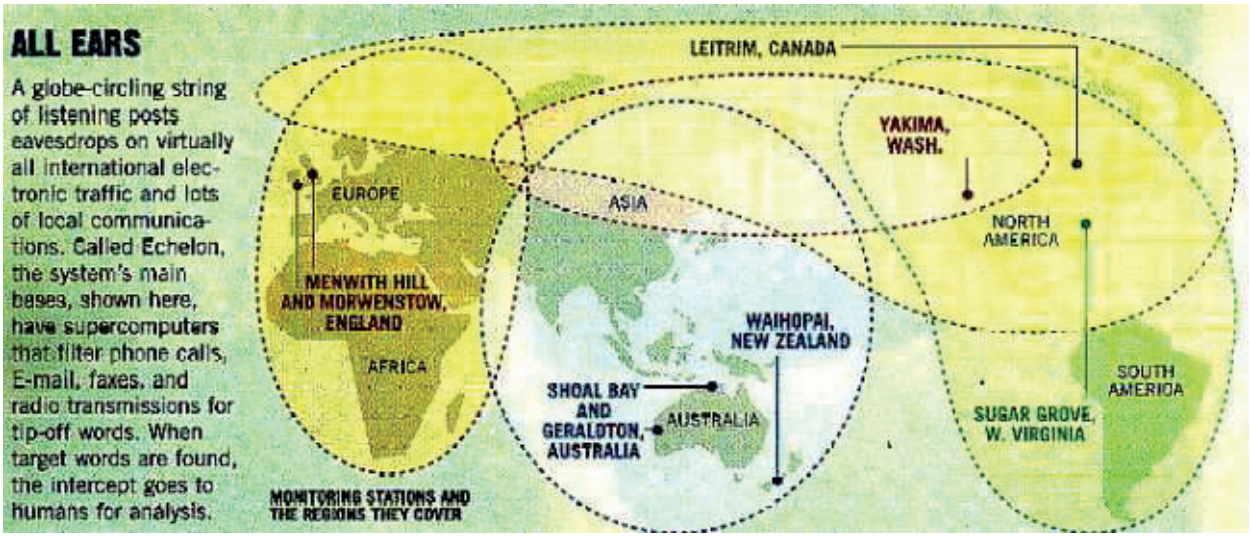
La guerre de l'information

Echelon n'est en aucun cas une conséquence de la guerre froide, malgré tout ce qu'on peut lire sur la question dans la presse. Depuis leur existence, les services secrets de tous les pays se sont espionnés mutuellement. C'est leur raison d'être.

Pendant la Première Guerre mondiale, les Anglais possédaient un système de déchiffrage automatique des télégrammes. Il a été institutionnalisé en 1920 et même présenté au Sénat américain par la suite ! Les Américains avaient d'ailleurs aussi utilisé le même procédé quelques années plus tard. Chaque pays utilise les mêmes méthodes, même si la puissance financière de l'état commanditaire est effectivement très influente sur l'efficacité des choses. Quand l'État français met en accusation les Américains pour l'avoir espionné, il faut savoir qu'il fait la même chose... Tout ceci est assez hypocrite. Ces agences de surveillance se sont totalement installées dans la bonne marche des États depuis la Deuxième Guerre mondiale. Elles ont d'ailleurs largement contribué à la défaite de l'Allemagne nazie et à la libération de la France. (...)

(...) À la fin des années 40, ces agences ont eu plus de lest et plus de fonds pour fonctionner. Mais ce n'était pas une nouveauté. La British Intelligence a par exemple systématiquement copié les codes secrets du Général de Gaulle pendant des années. Même pendant la guerre 39-45, les services secrets anglais et américains espionnaient mutuellement toutes leurs communications. Il n'y a pas de surprises : pendant la Révolution française, les insurgés attaquaient les messagers royaux pour se tenir au courant des communications du pouvoir. Le procédé est et restera toujours le même : arriver au même niveau d'information que l'ennemi. Pendant la guerre froide, cet espionnage a en effet été largement dirigé vers les pays du Bloc de l'Est. Mais le projet Echelon n'a commencé que dans les années 70 et n'a jamais été qu'un outil d'espionnage envers les pays du Bloc de l'Ouest. Les agences d'écoute se sont retrouvées avec des satellites et avec la tâche d'écouter tout le monde.

Bien sûr, ils se sont vite rendu compte de l'impossibilité de ce qu'on leur demandait et ont dû rapidement faire des choix. Les premières stations ont été construites près de Washington et dans les Cornouailles (1970), à l'ouest de l'Angleterre (1972). Rapidement, tout s'est organisé autour de trois pôles : Pacifique, Atlantique et Océan Indien, chacun relié à un satellite gravitant autour de ces points.



La couverture des stations d'écoute

Dans ces premières années, les Russes n'avaient pas cette organisation et ne présentaient ainsi aucun danger. Maintenant, les programmes d'Echelon demandent aux Chinois ou aux Russes de lancer leurs satellites !

Vers un projet européen

Tout le monde espionne tout le monde. Et le plus riche sera le mieux informé. Ces projets demandent énormément d'argent pour être menés à bien. Le projet européen est en marche et fait beaucoup de bruits aux USA, qui y sont farouchement opposés. La Grande-Bretagne doit d'abord s'affranchir de ses alliances avec les États-Unis, mais l'arrivée de Georges W. Bush devrait accélérer les choses. Nous n'en sommes donc qu'au début. En dehors des pays anglophones, il émerge un axe France-Allemagne au niveau de l'intelligence économique et l'espionnage. Les Américains essayent actuellement de partager Echelon avec le plus de pays européens possible tout en tenant à l'écart l'Allemagne et la France.

Le Danemark, la Suisse, la Finlande sont par exemple déjà du côté américain.

Pretty Good Privacy

Par le nom même de **PGP**, on comprend que ce logiciel de cryptage n'est pas le système de défense absolu contre la surveillance électronique. PGP, c'est Pretty Good Privacy (*une défense plutôt bonne*). Le nom est très bon. Il n'évoque pas la sécurité absolue. La différence entre envoyer un email normal et un email codé par PGP est la même qu'envoyer une carte postale ou une carte dans une enveloppe. L'email basique peut être lu par n'importe quelle personne qui l'intercepte. Pour l'enveloppe, il faut l'ouvrir et donc savoir auparavant qu'il y a quelque chose d'important dans l'enveloppe. Echelon ne peut pas ouvrir systématiquement tous les emails codés. A la limite, le problème de la clé d'encryptage (de 64 à 128 bits pour un encryptage professionnel) n'est que partiel. Si Echelon décide de décrypter un message, il peut le faire. Mais il faut qu'il prévoie de prendre beaucoup de temps (1 à 2 semaines environ) pour chaque message. Dès lors, comment filtrer a priori les messages dont le décodage est fastidieux ?

Voici la force de PGP : cacher aux yeux de tous si le contenu est intéressant ou non. Rien de plus.

Il ne faut pas non plus oublier que si les gens veulent vraiment intercepter les messages, ils peuvent se rendre directement à la source. Par exemple, j'ai un ordinateur portable avec énormément de données, cryptées ou non. Avec *Tempest*[143], par exemple, on peut voir mon écran à près de 100 mètres, grâce au rayonnement électromagnétique de l'écran et des câbles. S'ils veulent débarquer dans cette pièce pour me voler tout mon matériel, rien ne les en empêche. Et s'ils veulent voler les emails que j'envoie à mon ami Nicky Hager en Nouvelle-Zélande, pas de problème : il laisse la porte de sa maison ouverte toute la journée !

La défense de la vie privée par des moyens d'encryptage électronique n'est donc que partiellement efficace, car s'ils le désirent, les services d'espionnage peuvent aller chercher à la source de l'information. Et une clé, même à 128 bits, est toujours décryptable.

Source : *Chronicart* (02/2001)

Duncan Campbell — Surveillance électronique planétaire

Autant éviter toute confusion dès le départ : ceci n'est pas un essai. Encore moins un roman. Non, *Surveillance électronique planétaire* est un rapport commandé par la Communauté européenne sur le système de surveillance électronique Echelon.

Si l'idée peut paraître assez austère de prime abord, la lecture de ce petit livret de 140 pages s'avère passionnante. Quand ses confrères journalistes aiment à en rajouter dans le sensationnel cheap (bon marché), Duncan Campbell, vieux renard écossais du journalisme d'investigation, livre l'essentiel, rien que l'essentiel. Les preuves et les explications dans le texte. Bref, un document inégalable sur les grandes oreilles cyber de la NSA, agence « occulte » des services d'espionnage américains.

Découpée en de courts paragraphes, la réflexion de l'auteur décarcasse avec précision l'historique et les raisons d'être du système. Echelon, c'est le réseau de surveillance des réseaux, le grand *scan* interplanétaire, le rêve panoptique et démiurge des agences d'intelligence américaine. Non pas une police du Net, mais un grand filtre où transitent quasiment tous nos échanges (emails, chats, fichiers) électroniques. Sa tâche est celle d'une fourmi infatigable. Duncan Campbell, lui, débusque ce voyeur invisible et décrit tous ses travers. Echelon, grande machinerie d'état, est un amoncellement d'ordinateurs super puissants, d'antennes satellites scrutant l'espace et d'espions humains très faillibles.

[143] *Tempest* désigne une technique pour convertir en données intelligibles les rayonnements électromagnétiques émis par des ordinateurs à distance. Ces rayonnements peuvent être captés, comme n'importe quelle onde électromagnétique (radio, etc.), ce qui permet d'espionner un ordinateur à distance et sans avoir à le « pirater » (il n'est même pas nécessaire qu'il soit équipé d'un modem). Par exemple en détectant les rayonnements émis par les câbles électriques du clavier, on peut détecter les touches tapées. De même, avec le câble de l'écran, il est possible de connaître les images qui y sont affichées. Le nom Tempest a été inventé par les services américains (notamment la NSA) pour désigner ce phénomène et les mesures de sécurité pour les éviter.

Pourtant, Echelon n'est pas un enfant du baby-boom paranoïde de la guerre froide, mais un instrument du bloc USA/Royaume-Uni destiné prioritairement à surveiller les autres pays du bloc de l'Ouest. Une formidable façon pour les États-Unis de suivre les évolutions des bénéficiaires du Plan Marshall et d'acquérir en temps réel toute information plus ou moins confidentielle qui transiterait sur les ondes : fax, email, téléphone, tout y passe.

Les Français, dindons de la farce, tentent de rattraper le retard accumulé lors des années Balladur. A l'initiative du Parlement européen, ce rapport dense, mais très clair, car retravaillé entièrement pour un public de non-techniciens, démystifie la paranoïa très Roswellienne du mythe Echelon (« on nous ment, on ne nous dit rien ») pour la remplacer par un factuel très parlant : les services secrets américains ont pu pendant des années connaître ce qu'ils souhaitaient des secrets d'États locaux. Exit donc toute confidentialité économique ou politique ; pas besoin de ligne rouge vers le bureau ovale. Echelon, lui, écoutait tout. Avec la plainte internationale déposée par l'ancien juge d'instruction Thierry Jean-Pierre (aujourd'hui député européen), ce rapport très documenté devrait jeter un pavé dans la mare trop tranquille des relations Europe/États-Unis.

Source : *Chronicart* (02/2001)

Trois questions à Ducan Campbell

Journaliste écossais, il révèle le fonctionnement d'Echelon, système américain d'espionnage planétaire.

Big Brother s'appelle Echelon. Sous couvert de lutte contre le terrorisme et la criminalité, plus de 200 installations contrôlées par les Américains interceptent toutes les communications électroniques internationales, téléphone, fax, emails publics ou privés, depuis l'espace jusqu'au fond des océans.

Sollicité par le Parlement européen, Duncan Campbell, expert en matière d'espionnage, a remis un rapport explosif sur ces méthodes souvent attentatoires aux libertés individuelles.

— Echelon est-il capable de tout intercepter ?

Depuis 1920 et les débuts du téléphone, les Américains veulent surveiller tout ce qui se dit.

Aujourd'hui, la tâche est de plus en plus complexe et le tri, considérable : sur les deux millions de communications interceptées chaque heure par le réseau Echelon, seules quatre sont réellement analysées. Une activité qui mobilise 90 000 personnes et 20 milliards de dollars par an.

— On a parlé de reconnaissance de mots-clés comme « cocaïne » ou « terrorisme » qui déclencheraient automatiquement l'écoute...

C'est de la science-fiction pour les conversations téléphoniques, car les logiciels de reconnaissance vocale présentent des taux d'erreurs de l'ordre de 40%. Mais, si l'on possède des enregistrements de la voix de certains individus, il est possible d'indexer des machines capables de les repérer. On dit que Pablo Escobar s'est fait avoir par ce type de moyen. En revanche, pour les fax et les emails, le repérage des mots-clés est facile. Édouard Balladur a perdu un marché de 6 milliards de dollars d'armement et d'Airbus en 1994 avec l'Arabie Saoudite : les Américains avaient lu les télécopies qui mentionnaient ses conditions et Boeing a pu surenchérir...

Car cet espionnage, qui s'est longtemps focalisé sur la guerre froide, s'est recyclé, avec l'Administration Clinton, dans la collecte d'informations économiques et commerciales.

— Dans votre rapport, vous rappelez l'illégalité de la plupart de ces écoutes.

Les lois internationales sur la confidentialité des communications n'ont jamais été respectées par ce type d'agence. Officiellement, depuis la sortie de mon rapport, la DST mène une enquête. En fait, le contre-espionnage français agite un peu de fumée, mais ne creuse rien. Car ce que je dis là, les gouvernements le savent déjà, et beaucoup — dont la France avec ses centres d'écoute à Domme (Dordogne) mais aussi en Nouvelle-Calédonie et en Guyane —, font la même chose.

Pour que ces pratiques changent, il faut que les citoyens rappellent avec insistance quelques règles élémentaires. Il peut être légitime d'écouter tel ou tel pour lutter contre le terrorisme, l'argent sale, etc., mais il faut que ces pratiques soient encadrées. D'ici vingt ans peut-être...

Station de Domme (Dordogne)

Source : *Télérama* (07/02/2001)

Surveillance électronique planétaire : *on vous écoute, où que vous soyez...*

Produit par Duncan Campbell, journaliste et écrivain réputé, *Surveillance électronique planétaire* décrit les motifs et le fonctionnement du gigantesque réseau d'interception électronique connu à tort sous le nom d'Echelon. Un petit livre qui nous plonge rapidement et sans artifices au cœur de cette bête aux oreilles attentives.

Dès la fin de la Deuxième Guerre mondiale, la National Security Agency (NSA) américaine a amorcé la mise sur pied d'un gigantesque réseau planétaire d'interception de signaux. Elle a rapidement été rejointe par ses semblables de quatre pays, dont le Canada. C'est devant la menace grandissante que représentait ce réseau (qui englobe Echelon) à leur intégrité économique que les pays membres du Parlement européen ont commandé à Duncan Campbell un rapport sur les capacités d'interception de l'alliance présumée UKUSA (dont font partie les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande).

Remis en 1999 sous le titre *Interception Capabilities 2000*, ce rapport a déclenché l'ouverture d'une enquête internationale. *Surveillance électronique planétaire* est une traduction de ce rapport.

Digne des meilleurs scénarios hollywoodiens, *Surveillance électronique planétaire* relève presque de la tragédie par ses découvertes lourdes de conséquences.

Des années 50 à aujourd'hui, rares sont les communications, où que ce soit dans le monde, à l'abri des oreilles ou des yeux de la NSA et ses comparses.

Des ondes radio d'après-guerre aux câbles électromagnétiques encore grandement utilisés aujourd'hui, en passant par les ondes ultracourtes et les satellites, l'alliance UKUSA a constamment renouvelé ses techniques d'interception.

Bénéficiant de territoires amis bien répartis sur la planète (les cinq pays membres, dont les nombreuses bases militaires américaines dispersées un peu partout), l'alliance a des oreilles partout, peut-on lire. Quand ces territoires ne sont pas suffisants, l'alliance ne se gêne pas pour mettre sous écoute des câbles sous-marins à l'aide de sous-marins spécialisés. *Surveillance électronique planétaire* est étonnamment riche en détails.

Grâce à la loi d'accès à l'information prévalant dans plusieurs pays membres, dont les États-Unis, et à l'indiscrétion de certains anciens employés, Duncan Campbell révèle entre autres les noms de sous-marins impliqués dans l'écoute de câbles subaquatiques, d'entreprises américaines ayant bénéficié de l'aide de la NSA pour l'obtention de contrats et la nature de ces contrats, la localisation de nombreuses bases Echelon et leur affectation, etc.

Il détaille également certaines failles de sécurité introduites volontairement par la NSA et ses associés dans des logiciels tels que *Netscape Navigator, Internet Explorer, Lotus Notes* et les produits de la firme suisse de cryptographie *Crypto AG*.

Le document présente également une note « encourageante » en décrivant les difficultés de plus en plus nombreuses auxquelles doivent faire face les agences d'interception membres de l'alliance. La progression de la cryptographie dans le domaine public, et l'échec de l'effort de l'alliance pour créer un « dépôt de clés », causent énormément de problèmes. La libéralisation en janvier 2000 des règles d'exportation des produits de cryptographie par les États-Unis peut d'ailleurs être vue comme le lancer de l'éponge par le gouvernement américain dans ce domaine, selon Duncan Campbell.

La multiplication des transmissions par fibre optique rend également la tâche complexe pour ces agences, qui ne peuvent intercepter les signaux y voyageant qu'au moment où ils franchissent un amplificateur (obligatoires pour les longues distances). Si le branchement sur des fibres sous-marines ne pose pas problème, celui sur des fibres terrestres en pays étranger est beaucoup plus difficile et peu discret.

« *Surveillance électronique planétaire* » se veut un essentiel pour quiconque désire en savoir davantage sur les activités plus ou moins légales auxquelles sont en mesure de se livrer les membres de l'alliance UKUSA. On y apprend entre autres que le Centre de recherche informatique de Montréal (CRIM) et l'Université du Québec à Chicoutimi (UQAC) ont déjà été mandatés par la NSA canadienne, le Centre de la sécurité des télécommunications (CST), pour diverses recherches sur la reconnaissance vocale, ainsi que sur les motifs qui pourraient justifier l'investissement récent dans le réseau de satellites Iridium par le département américain de la Défense. Très instructif...

Source : *Multimedium* (05/02/2001)

Duncan Campbell, chasseur d'espions

Sorti le 19 janvier, *Surveillance électronique planétaire* est la version française et réactualisée du rapport qui révéla au grand public l'existence du programme d'écoutes Echelon.

Portrait de son auteur, Duncan Campbell, qui fouine depuis 20 ans dans les arcanes des services de renseignements. Avec son sac à dos et ses chemises à carreaux, Duncan Campbell a tout de l'universitaire écolo et bonhomme. Mais ne vous fiez pas aux apparences : l'écossais, qui court le monde et les conférences, est l'un des journalistes d'investigation les plus incisifs du Far-West high-tech. Planqué derrière des lunettes en cul de bouteille, il explique d'une voix posée que ses révélations sur Échelon, le réseau anglo-saxon d'interception des communications mondiales, reposent sur plus de 20 ans d'enquêtes. Et que son travail, qui a débouché sur une commission d'enquête du Parlement européen, n'a rien d'un délire paranoïaque, comme certains de ses détracteurs aimeraient le faire croire.

Le business de la N$A (sic)

Sa carrière de fouineur démarre dans les années 70. Campbell suit alors des études de physique à Oxford. Mais à l'atmosphère feutrée des labos universitaires, il préfère rapidement le terrain et tâte du journalisme. Au point d'être arrêté, en 1976, par le contre-espionnage britannique. Duncan a 24 ans et il vient de publier, dans le journal de gauche *Time Out*, une enquête sur une installation gouvernementale de surveillance électronique. Opiniâtre, l'étudiant a découvert un code utilisé pour désigner les bases secrètes de l'armée. L'affaire lui vaut 18 mois de poursuites judiciaires : les autorités britanniques, qui redoutent l'arrivée du « journalisme d'investigation à l'américaine », veulent faire un exemple. Mais cette punition a un effet inverse sur Campbell : il se lance sur les traces de ce que l'on connaît aujourd'hui

sous le nom d'Echelon. Il finit par démontrer, en 1988, l'existence de ce programme d'écoute des communications, dans lequel coopèrent les États-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, grâce, entre autres, aux confessions d'un ingénieur qui a travaillé pour des sociétés privées sous contrat avec la National Security Agency américaine (NSA).

En 1999, il a déjà signé nombre de papiers sur la question. Mais c'est le rapport que lui a commandé le Parlement européen qui révèlera à l'opinion publique internationale l'ampleur de ce Big Brother. À lui seul, l'espionnage industriel effectué via Echelon rapporterait, chaque année, 25 milliards de dollars (175 milliards de francs) de contrats aux firmes américaines. Au détriment, essentiellement, de leurs concurrents européens ou japonais... Pour autant, ses conclusions ne provoquent pas d'incident diplomatique : les principales puissances industrialisées collaborent toutes, de près ou de loin, au système. Quand elles n'ont pas développé le leur...

Plus de vie privée

Duncan Campbell ne limite pas ses enquêtes aux « grandes oreilles » de la NSA. À son actif, on compte aussi quelques brûlots dénonçant les pratiques frauduleuses de médecins et d'industriels envers les patients atteints du cancer et du sida, ou encore l'implication d'un ancien ministre britannique dans un trafic de cigarettes. Certains des reportages de Campbell, également producteur de télévision, ont été tout bonnement censurés et il soupçonne les services secrets de l'avoir mis sur écoutes pendant au moins dix ans : « *J'ai dû faire le deuil de ma vie privée* », confesse-t-il.

Malgré tout, ce journaliste continue d'envoyer ses articles aux rédactions par email non crypté, une semaine avant leur parution. Histoire de prévenir ceux dont la charge est de le surveiller.

Source : *Transfert* (01/02/2001)

Echelon mis à nu

Auteur de *Surveillance électronique planétaire* qui vient de sortir en librairie, le journaliste Duncan Campbell a révélé au grand public l'existence du programme anglo-saxon d'écoutes et d'interception des télécommunications.

Surveillance électronique planétaire vient de sortir en librairie. Il s'agit de la traduction française (et mise à jour) du rapport que le Parlement européen avait commandé en 1998 à Duncan Campbell. Une excellente présentation du programme anglo-saxon d'écoute et d'interception des télécommunications, connu sous le terme générique d'Echelon.

Les Américains commencent timidement à reconnaître l'existence d'Echelon... Rappelons d'abord qu'Echelon n'est qu'un sous-système du programme global de surveillance que maintiennent les Américains et les Anglais. Je pense, par ailleurs, qu'il est préférable de parler du système de surveillance UKUSA (du nom du pacte secret signé par les deux pays en 1947).

James Woolsey, qui dirigea la CIA de 1993 à 1995, déclara en mars 2000 au *Wall Street Journal* : « *Eh oui, chers amis continentaux, nous vous avons espionnés parce que vous pratiquez la corruption.* » Je ne sais si je dois en rire ou en pleurer, mais il louait également « *l'honnêteté intellectuelle* » de mon travail, parce que je précisais, dans mon rapport pour le Parlement européen, que les Américains justifiaient les cas d'espionnage industriel que j'avançais par des accusations de corruption visant à remporter les contrats. Ce que mentionnent rarement les journalistes quand ils parlent d'Echelon.

Cela dit, dans les quatre ou cinq exemples avérés d'espionnage industriel que je rapporte dans le rapport, dont les affaires, bien connues d'Airbus et Thomson CSF, il y en a aussi un qui n'a rien à voir avec la corruption. Par exemple, le Tornado, cet avion de chasse fabriqué par un consortium européen et vendu dans le monde entier, sans même parler de la surveillance effectuée par les Américains à l'occasion des négociations multilatérales...

A-t-on une idée de l'ampleur de l'espionnage industriel pratiqué ?

J'estime que les États-Unis font remporter aux firmes américaines quelque chose comme 25 milliards de dollars de contrat chaque année, aux dépens de leurs concurrents, essentiellement européens et japonais. Les principaux marchés visés sont ceux des télécommunications, de l'aérospatial, l'industrie lourde, l'environnement... La politique du gouvernement américain est de ne pas donner d'informations confidentielles aux sociétés privées, mais de les « assister ». Il ne contacte pas les responsables pour leur expliquer qu'un rapport de la CIA, couplée aux informations interceptées par la National Security Agency (NSA, l'agence qui chapeaute le programme Echelon), attestent que leur concurrent allemand ou japonais propose 4,95 dollars l'unité d'électricité, et que s'ils proposaient 4,90 dollars, ils remporteraient le contrat ! Il ne permet même pas à la société de savoir qu'elle a bénéficié des bons conseils de la NSA. Il chuchote simplement à l'oreille des entreprises quelques menus conseils, comme de descendre le prix à 4,90 dollars, sans autre explication. Subtile nuance.

Est-ce légal ?

Jusqu'en 1993, il n'existait pas de politique définie en la matière. À cette époque est intervenu au Congrès un débat public autour de deux questions : « *Devons-nous utiliser ce que nous collectons en matière d'intelligence économique pour aider les sociétés privées ?* », et « *Qu'est-ce qu'une société américaine ?* » Ford fabrique ainsi une partie de ses voitures en Corée, et certaines firmes japonaises ont des usines aux USA. La réponse est aujourd'hui disponible sur le site du Département du Commerce américain : son Advocacy Center (centre de soutien) propose un questionnaire où l'on peut déclarer travailler pour une société américaine en butte à un compétiteur allemand qui, lui, bénéficie de l'aide de son propre gouvernement... Et voilà, le tour est joué. C'est une politique très claire mise en place par Clinton pour venir en aide aux industriels américains, et cela a d'ailleurs contribué à son élection.

Comment ça marche ?

Supposons qu'il s'agisse d'un contrat au Brésil. Vous remplissez les *Dictionnaires* (logiciels qui filtrent les communications par mots-clés) des stations d'écoute de la NSA qui couvrent l'Amérique du Sud et l'Europe avec le nom des sociétés en compétition, de leurs dirigeants, des officiels brésiliens chargés de veiller à la bonne tenue du contrat, leurs numéros de téléphone et de fax respectifs et tous autres mots-clés relatifs au marché en cours (nom du projet, des matières premières ou produits manufacturés en jeu, etc.). Quand Thomson CSF communique avec son correspondant au Brésil, vous interceptez la communication, ce qui ne devrait pas être trop compliqué, à moins qu'ils ne l'aient cryptée. En l'espèce, Thomson CSF tentait de corrompre un officiel brésilien, ce qui a permis au gouvernement américain d'intervenir et de remporter le contrat.

Existe-t-il des systèmes de surveillance privés ?

Bien sûr. Certaines multinationales embauchent d'anciens agents de la NSA pour ça. Le moyen le plus simple est d'intercepter les communications satellites. Si elles ne sont pas cryptées, ça peut être très précieux. Mais le problème est moins de savoir ce qu'il est possible d'apprendre que ce que l'on peut en faire. Une multinationale peut voler des secrets industriels et battre au poteau l'un de ses concurrents, mais c'est toujours inférieur à ce qu'un pays comme les États-Unis peut faire. En l'état actuel, je dirai qu'ils peuvent surveiller de 80 à 90% des communications internationales non cryptées. Ceci exclut donc celles qui restent à l'intérieur même de frontières nationales.

Vous venez d'être auditionné par la commission d'enquête du Parlement européen. Votre sentiment ?

Le mandat de la Commission n'est pas restrictif et laisse toute marge de manœuvre aux membres qui la composent. Elle pourrait même recommander de changer la loi de telle sorte que l'espionnage industriel, au sein même de l'espace européen, soit considéré comme contraire à la loi. Si la commission s'était contentée d'étudier les possibles violations du droit européen, liées à l'existence d'Echelon, elle n'aurait pas pu aller bien loin puisque le cadre légal qui cimente l'Europe est resté très vague en matière d'espionnage industriel. Les parlementaires verts et ceux qui les soutiennent voulaient se doter de pouvoirs

d'investigation leur permettant d'obliger les officiels à témoigner. La commission ne dispose finalement pas de ces pouvoirs-là. De toute façon, le gouvernement britannique, souvent mis en cause, aurait trouvé moult prétextes et recours légaux pour éviter à ses officiels d'avoir à venir à Bruxelles répondre à leurs questions.

Alors qu'est-ce que ça change ?

La forme actuelle de la commission est aussi bonne, sinon meilleure, que ce que les Verts demandaient

Et qu'en attendez-vous ?

Echelon est devenu une problématique mondiale grâce au Parlement européen. Je pense que la commission d'enquête prendra des mesures importantes et révélera encore plus de failles, défauts et accords secrets. On peut espérer qu'elle change alors les lois nationales et internationales : les gens doivent comprendre que cette situation n'est pas normale et qu'il faut y remédier. Mais c'est aussi un processus qui prend du temps. Combien d'années a-t-il fallu attendre avant que des magistrats anglais et espagnols décident qu'il n'était pas normal que des dictateurs, ayant tué ou fait tuer, puissent voyager en toute impunité à l'étranger, comme ce fut le cas pour Pinochet ? Ce dernier a beau avoir été autorisé à rentrer dans son propre pays, les choses ne sont désormais plus comme avant.

Cette perspective est nouvelle et il s'agit bel et bien d'une campagne internationale en faveur des droits de l'homme. La mondialisation entraîne un certain nombre de dérives, comme McDonald's ou encore l'espionnage américain, mais aussi de bonnes choses. Ainsi, cette culture de la démocratie, des droits de l'homme qui, depuis 20 ans, traverse l'Amérique Latine ou encore l'Asie, où il était impensable, il y a quelques années encore, d'imaginer que des dictateurs puissent être inquiétés. Nous avons mis du temps à nous apercevoir de cette violation de la vie privée au niveau des communications internationales, mais l'Europe se trouve à la pointe de la protection de la vie privée.

Le processus dans lequel est aujourd'hui engagé le Parlement européen se répand dans le monde entier.

Et quid de Frenchelon, le système français de surveillance électronique ?

Je n'ai pas inventé le terme Frenchelon. Je pense que ce sont les services de renseignements anglais qui l'ont créé en vue de faire de la propagande anti-française. Le mot Echelon étant devenu si populaire, et les Français n'arrêtant pas de s'en servir pour leur taper dessus, ils ont dû ressentir une forme d'injustice dans la mesure où les Français font pareil, même si leurs capacités en la matière sont limitées.

Depuis leur reconstitution après la Deuxième Guerre mondiale, les services de renseignement français ont toujours été très forts en matière de d'intelligence des signaux. Avant même l'invasion de la France, ils écoutaient déjà les nazis. Le principal organisme en la matière fut le GCR (Groupement de Contrôle Radioélectrique) qui mit en place des stations d'écoute en France et dans ses colonies. Aujourd'hui, c'est la DGSE (Direction générale de la sécurité extérieure) qui s'en charge et entretient un certain nombre de stations réparties dans le monde entier. Selon Jean Guisnel, journaliste au Point et spécialiste du sujet, il y en aurait ainsi en Nouvelle-Calédonie, à Kourou, en Guyane, à Domme, près de Sarlat en Dordogne (en collaboration avec le BND, l'équivalent allemand de la DGSE). Une trentaine de pays au moins ont ainsi développé leur propre programme de surveillance des télécommunications. Une dizaine d'entre eux collaborent d'ailleurs avec le réseau anglo-saxon, au nombre desquels on compte le Japon, la Corée du Sud, la Turquie, la Norvège, le Danemark, l'Allemagne, les Pays-Bas...

N.B.: Entretien réalisé en juillet 2000 à Bruxelles dans le cadre de *World Information 2000*.

Source : *Transfert* (31/01/2001)

« Echelon *n'est pas invincible* » : rencontre avec Duncan Campbell.

Il est en quelque sorte le « gourou » d'Echelon. L'écossais Duncan Campbell, 46 ans, est l'un des spécialistes les plus aguerris de ce système d'écoute international, capable d'intercepter les conversations

téléphoniques, fax, emails partout sur la planète pour le compte des États-Unis et de quelques autres pays. Il planche sur le sujet depuis 1988, date à laquelle il a publié son premier article sur le sujet en Angleterre. Depuis, il a été le principal auteur des rapports au Parlement européen sur la question, en 1998 et en 1999. Aujourd'hui, sort en librairie *Surveillance électronique planétaire* (éditions Allia), la première publication de ses travaux sous forme de livre.

Interview de quelqu'un qui se dit « surtout pas paranoïaque ».

Dans votre livre, vous citez un ex-agent secret américain disant que « la technologie est devenue ces dernières années l'ennemie de l'interception des communications ». Echelon *serait-il mis en échec par le développement du Net ?*

Il n'y a pas de système d'écoute invincible. Ce qu'Echelon faisait facilement en écoutant les satellites de communication avec de grandes antennes est maintenant plus difficile et plus coûteux. La plupart des données passent aujourd'hui par des câbles en fibre optique, souvent posés au fond des mers. Il est donc difficile d'aller écouter ce qui transite sur un territoire national. Mais pour les liaisons internationales, les États-Unis utilisent des sous-marins pour collecter l'information depuis les années 70. Ils posent des nacelles sur les fonds marins, branchées sur les câbles. On a appris cela en 1982 quand les Russes ont découvert un tel système dans la mer d'Okhotsk. Ces activités ont continué, et d'autres sous-marins font ce travail aujourd'hui. Et il ne faut pas oublier que, sur l'Internet, les données circulent là où il y a de la capacité. Si vous envoyez un email de Paris à Hambourg et que les liaisons européennes sont encombrées, il peut transiter par la Californie. Et donc, la NSA (National Security Agency, service secret américain) peut y avoir accès — ce qui ne veut pas dire qu'elle le fait — grâce à des connexions sur les principaux nœuds du réseau sur le territoire américain.

Serions-nous écoutés en permanence ? Comment se protéger ?

Il faut garder à l'esprit que l'information collectée est traitée par des « ordinateurs-*Dictionnaires* » travaillant avec des mots-clefs, et dont la tâche principale est de jeter la plupart des données recueillies. Si vous envoyez des emails à votre mère qui habite au Canada, Echelon ne traite pas ces messages, même s'il peut potentiellement le faire. La meilleure protection vient de la cryptographie. Mais les outils pour crypter ses emails ne sont pas simples d'emploi... Si les choses sont bien faites, c'est invisible. Quand je me promène sur le Web avec un navigateur, mes activités peuvent être espionnées. Mais si je regarde mon compte en banque, par exemple, je passe sans même m'en rendre compte d'une communication ouverte à un canal sécurisé, crypté. Il est vrai que l'utilisation de PGP (logiciel pour crypter ses emails) est encore complexe : je m'en rends compte lorsque je communique avec certains journalistes. Je dois toujours leur expliquer comment faire. Si j'envoie un email pour dire « allons boire un verre », il devrait être crypté. Non parce qu'il s'agit d'une information confidentielle, mais parce que vous et moi ne devrions pas avoir à nous dire qu'il est compliqué de préserver sa vie privée.

Régulièrement, des militants organisent le Jam Echelon Day (Journée du brouillage) et incitent à envoyer des emails bourrés de mots-clefs comme « Irak », « terrorisme », « drogue » pour saturer Echelon. *C'est utile ?*

C'est naïf. D'abord, les initiateurs de cette action ne peuvent connaître la véritable liste de mots-clefs. C'est le produit de leur imagination. Ensuite, Echelon est justement destiné à filtrer le « bruit », sélectionner ce qui fait sens et jeter le reste. Si toute la planète s'expédie des emails avec les mêmes 70 mots-clefs, on est certain d'une seule chose : Echelon ne les traitera pas.

Quelle est la meilleure solution pour « brouiller » Echelon, *dans ce cas ?*

C'est l'action politique, bien sûr.

Une évaluation des techniques de contrôle politique

1. Introduction

La présente étude est un résumé d'une étude intérimaire intitulée « *Une évaluation des techniques de contrôle politique* » (PE 166.499) (ci-après désignée par « *étude intérimaire* »), rédigée par la Fondation Omega de Manchester et présentée au groupe du STOA lors de sa réunion du 18 décembre 1997 et à la commission des libertés publiques et des affaires intérieures le 27 janvier 1998.

Lorsqu'il est apparu que la question de la surveillance électronique figurerait à l'ordre du jour de la séance de session du mois de septembre 1998 du Parlement européen, il a été demandé à la fondation Omega de préparer un résumé analytique à jour de l'étude intérimaire, qui serait utilisé comme document de base. Ce résumé analytique couvre les divers domaines de la question des techniques de contrôle politique abordés par l'étude intérimaire. Le document dans sa forme actuelle ne porte toutefois que sur la question spécifique de la surveillance électronique. Seul le texte exhaustif reprend les notes et la bibliographie.

L'étude intérimaire a éveillé un grand intérêt et les commentaires suscités dans la presse dans toute l'Union européenne et au-delà témoignent de l'intérêt du public pour nombre d'innovations présentées par cette étude. Ce résumé est conçu pour répondre aux mêmes objectifs-clés que l'étude intérimaire, à savoir :

— fournir aux membres du Parlement européen un guide de référence concis sur les récents progrès réalisés en matière de techniques de contrôle politique ;

— identifier et décrire l'état actuel des développements les plus importants, en précisant davantage et en mettant à jour les éléments de l'étude intérimaire qui ont suscité l'intérêt et les commentaires les plus importants du public ;

— présenter aux eurodéputés un résumé des tendances actuelles en Europe et dans le monde ;

— proposer des options politiques couvrant des stratégies réglementaires pour le contrôle et la gestion futurs de ces techniques ;

— offrir des éléments de base succincts pour étayer la réponse du Parlement à la proposition de déclaration de la Commission sur les écoutes électroniques, déclaration inscrite à l'ordre du jour de la séance de session du Parlement européen du mercredi 16 septembre 1998.

2. Évolution des techniques de surveillance

Les techniques de surveillance peuvent être définies comme des dispositifs ou des systèmes capables de surveiller, de suivre et d'évaluer les mouvements des personnes, de leurs biens ou autres avoirs.

Ces techniques sont essentiellement utilisées pour suivre les activités de dissidents, de militants des droits de l'homme, de journalistes, de responsables étudiants, de minorités, de responsables syndicaux et d'opposants politiques. Il s'est développé une très vaste gamme de techniques de surveillance, en passant par les lunettes pour vision nocturne, les microphones paraboliques permettant de détecter des conversations à plus d'un kilomètre de distance, les versions laser, capables de surprendre n'importe quelle conversation derrière une fenêtre fermée dans la ligne de mire, la caméra stroboscopique danoise *Jai*, capable de prendre des centaines de photographies en quelques secondes et de photographier individuellement tous les participants d'une manifestation ou d'un défilé et les systèmes de reconnaissance automatique de véhicules capables de suivre des automobiles à travers les rues d'une ville via un système informatique géographique fonctionnant à base de cartes.

De nouvelles technologies, conçues à l'origine pour la défense et les renseignements, se sont, après la guerre, rapidement étendues dans les services chargés du maintien de l'ordre et le secteur privé. Il s'agit d'un des domaines du progrès technique dans lequel des réglementations d'un autre âge sont dépassées par un tableau d'infractions en constante augmentation.

Jusque dans les années soixante, la surveillance, pour l'essentiel, était peu technique et onéreuse, car il s'agissait de suivre de place en place des suspects, ce qui nécessitait jusqu'à 6 personnes travaillant en équipes de 2 et faisant les 3 huit. Toutes les informations et les contacts récoltés devaient être dactylographiés et classés avec peu d'espoir de vérifications rapides par recoupement. Même la surveillance électronique employait un grand nombre de personnes. La police est-allemande, par exemple, recourait aux services de 500 000 informateurs secrets, dont 10 000 étaient employées uniquement à écouter et transcrire les communications téléphoniques des citoyens.

Dans les années quatre-vingt, de nouvelles formes de surveillance électronique sont apparues et nombre d'entre elles ont consisté à automatiser l'interception des communications. Cette tendance a été renforcée dans les années quatre-vingt-dix aux États-Unis par une accélération des financements gouvernementaux à la fin de la guerre froide, accompagnée d'une réorientation des agences de défense et de renseignement vers de nouvelles missions qui, pour justifier leurs budgets, ont effectué des transferts de technologies vers certaines applications à visée répressive, comme des opérations de lutte contre la drogue ou le terrorisme.

En 1993, les Départements américains de la défense et de la justice ont signé des protocoles d'accord relatifs à « des opérations autres que la guerre et le respect de la loi » afin de faciliter le développement conjoint des technologies et leur partage. Selon David Banistar de Privacy International, « *Pour contrebalancer les réductions de contrats militaires, qui ont commencé dans les années quatre-vingt, les entreprises de matériel informatique et électronique ont développé de nouveaux marchés — aux États-Unis et à l'étranger — avec des équipements conçus à l'origine pour les militaires. Des sociétés, telles que E Systems, Electronic Data Systems et Texas Instruments vendent des systèmes informatiques avancés et des équipements de surveillance à des gouvernements nationaux et locaux qui les utilisent pour maintenir l'ordre, pour contrôler les frontières et dans l'administration sociale. Les rêves les plus fous de la police secrète est-allemande sont rapidement en train de devenir réalité dans le monde libre* ».

2.1 Réseaux de surveillance avec télévision en circuit fermé (CCTV)

En fait, le mode de surveillance visuelle a terriblement changé ces dernières années. Certes, les officiers de police et de renseignement continuent à photographier les manifestations et les individus qui les intéressent, mais ces images peuvent de plus en plus être mémorisées et exploitées. L'ultra miniaturisation qui ne cesse d'enregistrer des progrès signifie que ces dispositifs peuvent être rendus quasiment indétectables et peuvent faire l'objet d'un usage abusif par des personnes physiques, des entreprises et des agences publiques.

L'attitude face aux réseaux de caméra CCTV varie énormément dans l'Union européenne, de la position du Danemark, qui interdit par la loi l'usage de ce type de caméras, à la position du Royaume-Uni où il existe plusieurs centaines de réseaux CCTV. Il devrait y avoir cependant une position commune générale sur le statut de ces systèmes lorsqu'ils existent, par rapport aux principes de protection des données. Un aspect spécifique est l'admissibilité juridique des preuves fournies par les informations numériques recueillies par les systèmes les plus avancés de CCTV.

Ces informations relèvent pour l'essentiel de la législation relative à la protection des données si les informations recueillies peuvent être exploitées par plaque minéralogique ou en fonction de l'heure, par exemple.

Compte tenu du fait que les informations obtenues avec de tels systèmes peuvent être publiées, la directive européenne sur la protection des données doit être mise en œuvre par l'intermédiaire d'une législation primaire qui précise le droit lorsqu'il s'applique aux CCTV afin d'éviter toute confusion parmi les contrôleurs des informations CCTV et les citoyens, en tant que sujets de ces données. La législation primaire permettra d'étendre les effets de la directive à des domaines d'activité qui ne relèvent pas de la compétence communautaire. Les articles 3 et 13 de la directive ne doivent pas servir de couverture à l'utilisation des CCTV en toute circonstance dans un contexte national.

Il conviendrait d'étendre un code de pratique approprié, tel que celui mis en place par l'Unité d'information des collectivités locales (Local Government Information Unit — LGIU, 1996) basée au Royaume-Uni, de façon à prendre connaissance des meilleures pratiques recensées dans l'ensemble des États membres de l'Union européenne pour couvrir l'utilisation de tous les systèmes de surveillance CCTV fonctionnant dans les lieux publics et, notamment, les zones résidentielles. Une première démarche consisterait, pour la commission des libertés publiques, à envisager formellement d'étudier l'utilisation et le contrôle des CCTV dans l'ensemble des États membres en vue d'établir quels éléments des divers codes pourraient être repris dans un code unifié et un cadre juridique relatif à l'application de la loi ainsi qu'à la protection et à la restauration des libertés publiques.

2.2 Systèmes de surveillance algorithmiques

La révolution en matière de surveillance urbaine donnera naissance à une nouvelle génération de contrôles lorsque les systèmes fiables de reconnaissance des visages feront leur apparition. Ils seront installés dans un premier temps dans des lieux fixes, comme les tourniquets, les douanes, les portiques de sécurité, etc. pour permettre une reconnaissance standard de tout le visage.

L'étude intérimaire estime qu'au début du 21e siècle, la reconnaissance des visages sur CCTV sera effective et que les pays disposant d'infrastructures CCTV considéreront cette technique comme une option allant de soi. En fait, la compagnie américaine *Software and Systems* a mis à l'essai un système à Londres, capable de scruter les foules et de comparer les visages aux images mémorisées dans une base de données contenue dans un ordinateur délocalisé. Nous sommes à l'aube d'une révolution en matière de « surveillance algorithmique », d'analyse réelle de données par l'intermédiaire d'algorithmes complexes permettant la reconnaissance et la poursuite automatiques. Cette automatisation non seulement étend le filet que constitue la surveillance, elle en réduit également la taille des mailles.

De même, des systèmes de reconnaissance des véhicules ont été développés, qui sont capables d'identifier une plaque minéralogique et de suivre le véhicule à travers une ville en utilisant un système informatisé d'informations géographiques. Des systèmes de ce type sont désormais commercialisés, comme le système Talon, mis sur le marché en 1994 par la société britannique Racal, au prix de £2000 pièce. Ce système est capable de reconnaître les plaques minéralogiques à partir d'une technologie de réseau neurale développée par *Cambridge Neurodynamics* et peut fonctionner de jour comme de nuit.

À l'origine, il a été utilisé pour surveiller la circulation, mais ses fonctions ont été récemment adaptées pour être utilisées dans la surveillance de sécurité et il a été incorporé à la « ceinture d'acier » autour de Londres. Ce système peut enregistrer tous les véhicules qui entrent ou quittent le périphérique un jour donné.

Il est important de fixer des directives et des codes de pratiques précis pour ces innovations technologiques avant que la révolution numérique n'offre des possibilités nouvelles et inenvisagées pour la collecte, l'analyse, la reconnaissance et l'archivage de ces images. D'ores et déjà, des systèmes multifonctions de gestion du trafic, tels que « *Traffic Master* » (qui utilise des systèmes de reconnaissance des véhicules pour localiser et quantifier les bouchons), permettent la mise en place d'une architecture de surveillance.

Une réglementation de ce type devra se baser sur de solides principes de protection des données et tenir compte de l'article 15 de la Directive européenne de 1995 relative à la protection des personnes physiques et au traitement des données à caractère personnel.

Cet article dit en substance que « *les États membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données…* ».

Le Parlement a beaucoup à faire après les conseils contenus dans un récent rapport de la Chambre des Lords britannique (rapport de la commission d'enquête sur la valeur de preuve des images numériques, 1998), à savoir :

— le Parlement européen établit des directives à l'intention des secteurs publics et privés sur l'utilisation des recoupements de données et, notamment, sur le raccordement des systèmes de surveillance à d'autres bases de données ; et

— il est conféré au service responsable de la protection des données le pouvoir de contrôler le fonctionnement des systèmes de croisement des données.

Ces systèmes de surveillance soulèvent d'importantes questions de responsabilité, notamment lorsqu'ils sont délivrés à des régimes autoritaires. Les caméras utilisées sur la place Tiananmen avaient été vendues par *Siemens Plessey* comme systèmes avancés de contrôle de la circulation. Or, après le massacre des étudiants en 1989, une chasse aux sorcières a été organisée par les autorités qui ont torturé et interrogé des milliers de personnes afin d'identifier les éléments subversifs. Le système de surveillance *Scoot* équipé de caméras américaines *Pelco* a été utilisé pour enregistrer très fidèlement les manifestations.

Manifestation étudiante place Tiananmem

Les images ont été diffusées à de multiples reprises par la télévision chinoise, assorties d'une récompense pour toute information ce qui a abouti à l'identification de la quasi-totalité des opposants.

Une fois encore, le contrôle démocratique est le seul critère qui distingue un système moderne de contrôle du trafic d'une technologie avancée d'arrestation des dissidents.

Des sociétés étrangères exportent des systèmes de contrôle de la circulation à Lhassa, au Tibet, alors que Lhassa ne connaît aucun problème de contrôle du trafic. Le seul problème pourrait être ici un manque coupable d'imagination.

2.3 Dispositifs d'écoute et d'interception

Tout un arsenal de dispositifs d'écoute et d'interception a été développé pour enregistrer les conversations et intercepter les télécommunications. Au cours de ces dernières années, il a beaucoup été question, dans de nombreux États européens, de la pratique très répandue des écoutes légales ou illégales et de l'installation de microphones miniatures. L'installation de ces derniers est toutefois une technologie dépassée. Les espions modernes peuvent acheter des ordinateurs portables adaptés à cet effet et se régler simplement sur tous les téléphones mobiles branchés dans le secteur en déplaçant le curseur sur le numéro de ces appareils. La machine pourra même rechercher les numéros « intéressants » pour voir s'ils sont en communication.

Ces types d'écoute font toutefois piètre figure face aux réseaux d'interception gouvernementaux opérant à l'échelon national et international.

2.4 Réseaux nationaux et internationaux d'interception des communications

L'étude intérimaire présente de façon détaillée les systèmes de surveillance globale qui facilitent la surveillance de masse de toutes les télécommunications, y compris le téléphone, les transmissions par fax et par courrier électronique, qu'il s'agisse de celles des citoyens privés, des hommes politiques, des

syndicalistes ou des entreprises. On a assisté récemment, en matière d'écoutes téléphoniques, à une réorientation politique. Au lieu d'enquêter sur la criminalité (une démarche réactive), les services répressifs font de plus en plus porter leur travail sur la surveillance de certaines classes sociales et de certaines races vivant dans des zones « sensibles » — avant que ne surviennent les infractions — une forme de veille informatique à caractère préventif, basée sur des modèles militaires visant à recueillir d'énormes quantités de renseignements peu importants.

Sans encodage, les systèmes modernes de communication sont pratiquement transparents face aux équipements de pointe en matière d'interception qui peuvent être utilisés pour les écoutes. L'étude intérimaire explique également que les téléphones mobiles comportent, par conception, des systèmes de surveillance et de poursuite auxquels peuvent avoir accès la police et les services de renseignement. Ainsi, la technique numérique requise pour localiser les utilisateurs de téléphones mobiles à la réception d'appels fait des téléphones mobiles de tous les utilisateurs d'un pays, lorsqu'ils sont branchés, de mini dispositifs de poursuite permettant de localiser leurs propriétaires à tout moment, informations enregistrées dans l'ordinateur de la société. Ainsi, la police suisse a secrètement pris connaissance des allers et venues des utilisateurs de téléphones mobiles à partir de l'ordinateur du prestataire de service Swisscom qui, selon le *Sonntagszeitung*, avait enregistré les mouvements, à quelques mètres près, de plus d'un million d'abonnés, et ce, pendant au moins six mois.

Toutefois, de tous les développements couverts par l'étude intérimaire, c'est la partie portant sur certains aspects constitutionnels et juridiques liés à l'accès de la National Security Agency américaine à toutes les télécommunications européennes, et sa capacité à intercepter ces dernières qui a suscité le plus d'inquiétude.

Certes, personne ne nie le rôle de ces réseaux dans les opérations de lutte contre le terrorisme, le narcotrafic, le blanchiment de l'argent et le commerce illicite des armes, mais l'ampleur du réseau d'interception des communications étrangères, décrit dans l'étude, a suscité bien des craintes, notamment quant à la capacité de la législation existante, des systèmes de protection des données et de la vie privée, en vigueur dans les États membres, à protéger la confidentialité entre les citoyens et les entreprises de l'Union et des pays tiers.

Dans la mesure où une certaine confusion a régné dans les articles parus par la suite dans la presse, il semble utile de préciser certaines des questions liées à la surveillance électronique transatlantique et de dresser un bref historique et une mise à jour des événements survenus depuis la publication de l'étude intérimaire en janvier 1998. Il existe globalement deux systèmes distincts :

— le système anglo-américain couvrant les activités de services de renseignement militaires tels que NSA-CIA aux États-Unis englobant le GCHQ et MI6 britannique qui opèrent un système connu sous le nom d'Echelon ;

— le système UE-FBI qui assure la liaison entre divers services répressifs, tels que le FBI, la police, les douanes, les services de l'immigration et ceux de la sécurité intérieure.

Compte tenu du risque de confusion que peut engendrer le titre du point 44 de l'ordre du jour de la séance de session du Parlement européen du 16 septembre 1998 — il s'agit, en termes de renseignements, de deux « communautés » distinctes — il est bon de passer brièvement en revue les activités de ces deux systèmes, soit Echelon, le codage, la surveillance UE-FBI et les nouvelles interfaces permettant, par exemple, d'accéder aux fournisseurs d'accès Internet et aux bases de données d'autres services.

2.4.1 Interception NSA de toutes les télécommunications de l'UE

Selon l'étude intérimaire, toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la National Security Agency des États-Unis, qui transfère toutes les informations provenant du continent européen via le centre stratégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York Moors au Royaume-Uni.

Le système a été mis à jour pour la première fois dans les années soixante-dix par un groupe de chercheurs au Royaume-Uni (Campbell, 1981). Des travaux menés récemment par Nicky Hager (*Secret Power*, Hager, 1996) fournissent des détails extrêmement précis sur un projet nommé Echelon. Hager a interrogé plus de 50 personnes travaillant dans le renseignement pour découvrir un système de surveillance qui s'étend au monde entier pour former un système pointé sur tous les satellites clés Intelsat utilisés pour transmettre l'essentiel des communications téléphoniques, Internet, le courrier électronique, les télécopies et télex transmis par satellite dans le monde entier.

Les sites de ce système sont basés à Sugar Grove et Yakima aux États-Unis, à Waihopai en Nouvelle-Zélande, à Geraldton en Australie, à Hong Kong et à Morwenstow au Royaume-Uni.

Le système Echelon fait partie du système anglo-américain, mais, à l'inverse de nombreux systèmes d'espionnage électronique développés au cours de la guerre froide, Echelon vise essentiellement des cibles non militaires : des gouvernements, des organisations et des entreprises dans pratiquement tous les pays. Le système Echelon fonctionne en interceptant sans distinction de très grandes quantités d'informations puis en en triant les éléments intéressants à l'aide de systèmes d'intelligence artificielle comme *Memex*, à la recherche de mots-clés.

Cinq nations se partagent les résultats, les États-Unis faisant figure de partenaire principal en vertu de l'accord UK-USA de 1948 et la Grande-Bretagne, le Canada, la Nouvelle-Zélande et l'Australie ayant un rôle subalterne de fournisseurs d'informations.

Chacun des cinq centres fournit aux quatre autres des « *Dictionnaires* » de mots-clés, de phrases, de personnes et de lieux pour « l'identification » et le message intercepté ainsi identifié est transmis directement au pays demandeur. Parallèlement à la somme d'informations recueillies sur d'éventuels terroristes, il existe une grande part de renseignements à caractère économique, notamment une surveillance renforcée de tous les pays participants aux négociations du GATT. Hager a cependant noté que les principales priorités du système, et de loin, continuent à être le renseignement militaire et politique correspondant aux principaux centres d'intérêt des partenaires du système.

Hager cite des agents de renseignements très haut placés qui se sont exprimés dans l'*Observer* de Londres. « Nous estimons ne pas pouvoir nous taire plus longtemps sur ce que nous considérons comme une incurie et une négligence grossière de la part des institutions pour lesquelles nous travaillons ». Ils ont cité pour exemple l'interception par GCHQ des communications de trois organisations bénévoles, y compris *Amnesty International* et *Christian Aid*. Selon cette source du GHCQ : « *à tout moment GCHQ est en mesure d'écouter leurs communications pour répondre à une demande ciblée de routine* ». Dans le cas d'écoutes téléphoniques, la procédure est connue sous le nom de *Mantis*. Pour les télex, elle a pour nom *Mayfly*. Lorsque l'on tape un code relatif à l'aide au tiers monde, la source est en mesure de se positionner sur les télex des trois organisations. En l'absence de système de contrôle, il est difficile de découvrir les critères qui déterminent qui échappe à ce criblage.

Depuis la publication de l'étude intérimaire, il est vrai que des journalistes ont affirmé qu'Echelon avait été utilisé pour avantager des entreprises américaines impliquées dans des contrats d'armement, pour renforcer la position de Washington dans d'importantes négociations relatives à l'organisation mondiale du commerce avec l'Europe lors du différend avec le Japon sur les exportations de pièces détachées automobiles. Selon le *Financial Mail on Sunday*, « *les mots-clés identifiés par les experts américains incluent les noms d'organisations intergouvernementales et de consortiums d'affaires en concurrence avec des entreprises américaines. Le mot «bloc» est sur la liste pour identifier les communications sur les ressources pétrolières offshores dans des régions où le fond de la mer doit encore être divisé en blocs d'exploration* »... « *Il a été suggéré également qu'en 1990, les États-Unis ont entamé des négociations secrètes pour persuader l'Indonésie d'inclure le géant américain AT&T dans un contrat de télécommunications d'une valeur de plusieurs millions de dollars qui, à un moment donné, revenait entièrement à la firme japonaise NEC* ».

Le *Sunday Times* (11 mai 1998) a relaté que par le passé les radômes de Menwith Hill (station NSA F83) dans le Nord du Yorkshire au Royaume-Uni, avaient eu pour tâche d'intercepter l'ensemble du trafic ILC — essentiellement des communications commerciales ordinaires. Le personnel est passé de 400 personnes dans les années quatre-vingt à plus de 1400 aujourd'hui auxquelles s'ajoutent 370 personnes venues du ministère de la Défense. Le *Sunday Times* fait part également d'allégations selon lesquelles les conversations entre la société allemande Volkswagen et General Motors ont été interceptées et que les Français se sont plaints que Thomson-CSF, l'entreprise électronique française, avait perdu un contrat d'un montant de 1,4 million de dollars destiné à la fourniture d'un système radar au Brésil parce que les Américains avaient intercepté des détails des négociations et les avaient transmis à la compagnie américaine Raytheon qui avait par la suite remporté le contrat. Selon une autre plainte, Airbus industrie aurait perdu un contrat d'une valeur d'un milliard de dollars au profit de Boeing et McDonnel Douglas car des informations avaient été interceptées par l'espionnage américain.

D'autres journaux comme *Libération*, dans son édition du 21 avril 1998, et *Il Mondo*, daté du 20 mars 1998, qualifient le réseau de réseau d'espionnage anglo-saxon en raison de son axe UK-USA. *Privacy International* va plus loin. Tout en reconnaissant qu'au sens strict du terme, ni la Commission ni le Parlement européen ne disposent d'un mandat pour légiférer ou intervenir dans le domaine de la sécurité... Ils sont néanmoins responsables de l'harmonisation dans l'ensemble de l'Union.

Selon *Privacy International*, le Royaume-Uni pourrait réaliser que ses « relations particulières » contreviennent aux obligations auxquelles il a souscrit en vertu du traité de Maastricht dans la mesure où le titre V du traité de Maastricht fait obligation aux États membres de s'informer mutuellement et de se concerter au sein du Conseil sur toute question de politique étrangère et de sécurité présentant un intérêt général, en vue d'assurer que leur influence combinée s'exerce de la manière la plus efficace par la convergence de leurs actions. Or, en vertu de sa relation particulière, la Grande-Bretagne ne peut s'engager à consulter librement ses autres partenaires européens.

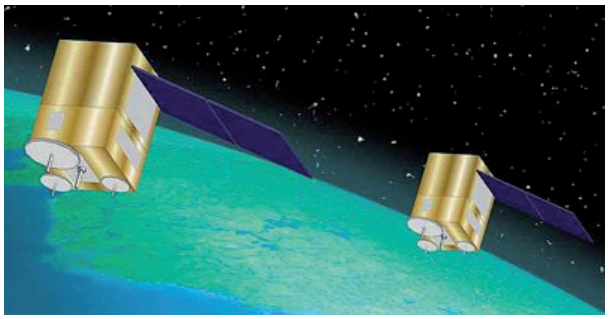
La situation devient plus complexe encore après les affirmations du magazine français *Le Point*, en vertu desquelles, les Français espionnent systématiquement les communications téléphoniques et par câble des Américains et de leurs autres alliés via le satellite-espion Helios 1A[144] (*Times* daté du 17 juin 1998).

Si la moitié seulement de ces informations est exacte, le Parlement européen doit agir pour s'assurer que ces puissants systèmes de surveillance opèrent de façon plus démocratique dès lors qu'il a été mis fin à la guerre froide. Certes, les politiques transatlantiques des États membres de l'Union européenne ne coïncident pas toujours avec celles des États-Unis et, en termes de commerce, l'espionnage reste ce qu'il est. Aucune autorité digne de ce nom aux États-Unis n'autoriserait qu'un tel système d'espionnage européen opère à partir du sol américain sans strictes limitations, si tant est qu'elle le fasse. Après un large débat sur les incidences du fonctionnement de ce type de réseaux, le Parlement européen est invité à procéder à un audit indépendant approprié et à contrôler les procédures. Toute tentative visant à proscrire l'encodage par les citoyens de l'Union doit être rejetée jusqu'à la mise en place de systèmes démocratiques et responsables.

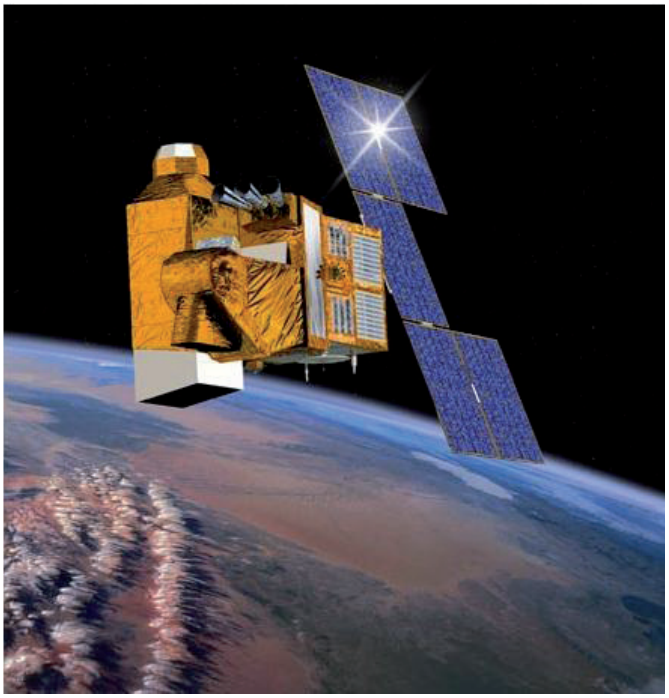
[144] Hélios 1A est un engin de 2,5 tonnes, d'une durée de vie de cinq ans, dont le coût est estimé à 10 milliards de francs. Il fait entrer la France dans le club restreint des nations possédant des moyens indépendants de reconnaissance optique spatiale. Jusqu'ici, seuls les États-Unis, la Russie, la Chine, l'Inde et Israël disposaient, en effet, de satellites espions. La décision de la France de mettre au point Hélios, un projet auquel l'Italie et l'Espagne sont associées — à hauteur respectivement de 14 % et 7 % — a été hâtée par la guerre du Golfe, en 1991. L'armée française s'était en effet retrouvée totalement dépendante de celle des États-Unis pour certains types de renseignements. Hélios 1A, dont le maître d'œuvre est la compagnie française Matra Marconi Space, sera capable de prendre des photos uniquement de jour et par beau temps. Plus tard, Hélios 2, en cours de mise au point et qui devrait être en orbite en 2001, sera opérationnel de jour comme de nuit mais toujours uniquement par temps favorable. (Note : le satellite Hélios 2a a été lancé le 18 décembre 2004 par Ariane 5-G+, masse au lancement : 4200 kg.)

Satellite Hélios 1A

À l'occasion du lancement par la France du Satellite d'observation Hélios 2A, ont été également placés sur orbite 4 micro-satellites « Essaim ». Essaim est le nom donné au programme de la DGA chargé d'analyser le spectre d'origine électromagnétique pour déterminer la densité de communications stratégiquement intéressantes dans les différentes parties du monde. Essaim est basé sur la plateforme Myriade développée par le CNES et Astrium. Chaque satellite pèse 120Kg et a une durée de vie de trois ans, avant de faire place à la seconde génération prévue pour 2008. Le contrôle de ces satellites s'effectuera par deux stations : une station de contrôle (sous la responsabilité du CNES) et une station de traitement des informations qui se situe au Celar à Bruz près de Rennes.



Satellites Essaim



Satellite Hélios 2A (lancé en 2004)

Installation des satellites Essaim sur Ariane 5-G+

2.4.2 Système global de surveillance des télécommunications UE-FBI

L'essentiel des informations et de la recherche nécessaire pour faire connaître au public l'histoire, la structure, le rôle et la fonction de la convention passée entre l'UE et le FBI visant à légitimer la surveillance électronique globale, est l'œuvre de *Statewatch*, une organisation de surveillance et de recherche sur les libertés publiques, basée au Royaume-Uni et qui fait autorité en la matière.

Statewatch a longuement décrit la signature du calendrier transatlantique à Madrid lors du sommet UE-US du 3 décembre 1995 — dont faisait partie le « *Plan d'action conjoint UE-US* » — et a analysé par la suite ces efforts comme une tentative de redéfinition de l'Alliance transatlantique dans l'après guerre froide, un thème de plus en plus utilisé pour justifier les efforts déployés par les services de sécurité interne pour conforter leur rôle de maintien de l'ordre en Europe. Statewatch note que le premier plan de surveillance « hors zone » de l'action conjointe n'a pas été inscrit à l'ordre du jour de la réunion des ministres de la justice et des Affaires intérieures, mais a été adopté sans discussion, sous forme de point A (sans débat) par, oh combien surprenant, le ***Conseil de la pêche*** du 20 décembre 1996.

En février 1997, Statewatch indiquait que l'UE avait secrètement accepté la création d'un réseau international d'écoutes téléphoniques via un réseau secret de commissions créées dans le cadre du « troisième pilier » du traité de Maastricht couvrant la coopération dans les domaines juridiques et du maintien de l'ordre. Les principaux points de ce plan sont soulignés dans un protocole d'accord, signé par les États de l'Union européenne en 1995 (ENFOPOL 112 10037/95, 25.10.95), qui est toujours classé secret. Selon le *Guardian* du 25-2-97, il reflète la crainte exprimée par les services de renseignements européens que les technologies modernes les empêchent d'écouter les communications privées. Les pays de l'UE, selon ce journal, devraient convenir de normes internationales en matière d'interception, fixées à un niveau permettant le décodage ou l'interprétation des mots brouillés par les services gouvernementaux. Des rapports officiels indiquent que les gouvernements de l'UE ont convenu de coopérer étroitement avec le FBI à Washington. Or, des procès-verbaux antérieurs de ces réunions semblent indiquer que l'initiative est venue à l'origine de Washington.

Selon Statewatch, les fournisseurs de réseaux et de services au sein de l'UE seront tenus d'installer des systèmes « écoutables » et de placer sous surveillance toute personne ou groupe lorsqu'ils se verront présenter une demande d'interception. Ces projets n'ont jamais été soumis au contrôle d'un gouvernement européen, quel qu'il soit, ni à la commission des libertés publiques du Parlement européen, en dépit des aspects évidents de libertés publiques soulevés par ce type de système non contrôlé. Le feu vert a simplement été donné secrètement par « écrit » sous forme d'un échange de télex entre les gouvernements des 15 États membres de l'UE.

Statewatch précise que le plan global de surveillance UE-FBI se développe désormais « en dehors du troisième pilier ». En clair, cela signifie que ce plan est développé par un groupe de vingt pays — les 15 États membres de l'UE plus les États-Unis, l'Australie, le Canada, la Norvège et la Nouvelle-Zélande. Ce groupe de vingt pays ne rend aucun compte de ses travaux au Conseil des ministres de la justice et des affaires intérieures, ni au Parlement européen ou aux parlements nationaux. Rien n'est dit sur le financement du système, mais un rapport émanant du gouvernement allemand estime que la partie du projet concernant les téléphones portables s'élève, à elle seule, à 4 milliards de DM.

Statewatch en conclut que c'est l'interface entre le système Echelon et son évolution potentielle sur les communications téléphoniques, combinée à la normalisation de centres et d'équipements permettant l'écoute des communications, bénéficiant du soutien de l'Union européenne et des États-Unis qui présente une véritable menace globale sur laquelle ne s'exerce aucun contrôle juridique ou démocratique (Communiqué de presse du 25-2-1997).

À maints égards, nous assistons à des réunions d'agents d'une nouvelle puissance mondiale militaire et du renseignement. Il est très difficile pour quiconque d'avoir un tableau d'ensemble de ce qui se décide lors de ces réunions au sommet qui élaborent cet « Agenda transatlantique ». Bien que Statewatch ait

obtenu une décision favorable de la part du médiateur concernant l'accès aux documents, au motif que le Conseil des ministres n'appliquait pas correctement le code d'accès, pour l'heure, elle n'a pas obtenu l'accès à ces agendas. Sans un accès à ces documents, nous nous trouvons face à un processus décisionnel occulte. L'éloquence de la déclaration sans précédent de la Commission sur Echelon et les relations transatlantiques, programmée pour le 16 septembre, pourrait en dire long, autant sur ce que l'on tait que sur ce l'on veut bien dire au public.

Les membres du Parlement européen pourraient souhaiter examiner les options énumérées ci-après.

2.5 Options

Commande d'une série d'études plus détaillées sur les incidences sociales, politiques, commerciales et constitutionnelles des réseaux globaux de surveillance électronique, cités dans la présente étude, en vue d'organiser une série d'auditions d'experts afin d'étayer la future politique de l'Union européenne en matière de libertés publiques. Ces études pourraient porter sur :

— les questions d'ordre constitutionnel soulevées par la capacité de la National Security Agency (NSA) américaine à intercepter toutes les télécommunications européennes, notamment les engagements juridiques pris par les États membres dans le cadre du traité de Maastricht et l'ensemble de la question relative à l'utilisation de ce réseau à des fins d'espionnage commercial et politique automatique ;

— les incidences sociales et politiques du système global de surveillance FBI-UE, son accès croissant à de nouveaux moyens de télécommunications, y compris le courrier électronique et son extension dans de nouveaux pays ainsi que toutes les questions financières et constitutionnelles connexes ;

— la structure, le rôle et le mandat d'un organe de contrôle opérant dans l'ensemble de l'UE, indépendant du Parlement européen, susceptible d'être créé pour surveiller et contrôler les activités de tous les organes chargés d'intercepter les télécommunications à l'intérieur de l'Europe ;

Le Parlement européen a pour option de demander le rejet de toutes les propositions émanant des États-Unis et visant à autoriser l'accès des messages privés transmis dans le cadre du réseau global de communications (Internet) aux agences de renseignement américaines. De même, le Parlement ne devrait pas accepter de nouveaux contrôles onéreux de transformation cryptographique sans un large débat au sein de l'UE sur la portée de telles mesures. Celles-ci devraient englober les droits de l'homme et les libertés publiques des citoyens européens et les droits commerciaux des entreprises d'exercer une activité légale sans surveillance abusive de la part d'agences de renseignements opérant de concert avec des multinationales concurrentes. Le Parlement devrait organiser une série d'auditions d'experts couvrant toutes les activités techniques, politiques et commerciales des organes chargés de surveillance électronique et étudier les options possibles afin de ramener ces activités dans le cadre d'un contrôle démocratique et de la transparence.

Ces auditions pourraient également étudier la question de codes de pratique appropriés pour garantir un redressement en cas d'abus ou d'incurie. Il conviendra de définir des critères explicites en fonction desquels il sera décidé qui fera ou non l'objet d'une surveillance, de quelle manière seront stockées, traitées et partagées les informations ainsi collectées et si ces critères et autres codes de pratique pourront être mis à disposition du public.

Modification du mandat de la commission des libertés publiques et des affaires intérieures de façon à y inclure des pouvoirs et compétences dans tous les domaines portant sur les problèmes des libertés publiques soulevés par les dispositifs et réseaux de surveillance électronique et rédaction d'une série de rapports au cours de son prochain programme de travail, portant notamment sur :

— la manière dont les codes de pratique obligatoires peuvent garantir la couverture des nouvelles techniques de surveillance par une législation appropriée en matière de protection des données ;

— la production de lignes directrices à l'intention des secteurs public et privé sur l'utilisation des recoupements d'information, notamment sur les liaisons entre les systèmes de surveillance et d'autres bases de données ; la question consistant à doter les services chargés de la protection des données dans les États

membres de pouvoirs leur permettant de contrôler le fonctionnement de ces systèmes de recoupement des données ;

— la manière dont la fourniture de dispositifs électroniques d'écoute à des citoyens privés et à des entreprises peut être davantage réglementée de sorte que leur vente soit régie par une autorisation juridique plutôt que par une sorte d'autoréglementation ;

— la manière dont l'utilisation des interceptions téléphoniques par les États membres peut être soumise à des procédures de contrôle public mentionnées au point (a) ci-dessus. (Par exemple, toute interception de communication téléphonique devrait faire l'objet d'une autorisation préalable, conformément aux prescriptions du parlement concerné. Dans la plupart des cas, les services répressifs ne devraient pas pouvoir se délivrer d'auto-autorisation d'interception sauf dans des cas très particuliers qui devraient faire l'objet d'une communication à l'autorité délivrant l'autorisation dès que possible) ;

— la manière dont les techniques facilitant la reproduction automatique et l'analyse spectrographique des communications téléphoniques en vue de créer des réseaux d'amitié ou de contacts devraient être soumises aux mêmes conditions juridiques que les technologies relatives aux interceptions téléphoniques et devraient être communiquées au parlement de l'État membre concerné ;

— la commande d'une étude ayant pour but d'analyser ce qui constitue la meilleure pratique et le contrôle optimum des CCTV dans l'ensemble des États membres en vue d'établir quels éléments des divers codes pratiques pourraient être repris dans un code unifié et un cadre juridique couvrant la répression et la protection des libertés publiques ainsi que leur restauration.

Établir des procédures en vertu desquelles toute commission du Parlement européen examinant des propositions relatives à des technologies ayant des implications dans le domaine des libertés publiques (travaux de la commission des télécommunications sur les questions de surveillance, par exemple) devrait être tenue de transmettre toutes les propositions et rapports sur le sujet à la commission des libertés publiques afin que celle-ci puisse faire par avance des remarques sur les décisions politiques ou financières relatives aux mesures à prendre ;

Définir des accords entre les États membres en vertu desquels des statistiques annuelles devraient être communiquées aux parlements des États membres sous une forme standard et cohérente. Ces statistiques devraient fournir des détails exhaustifs sur le nombre réel des communications interceptées et les données ne devraient pas être présentées sous forme d'agrégats (pour éviter que les statistiques n'identifient que le nombre d'autorisations délivrées alors que les organisations sous surveillance peuvent compter des centaines de membres dont tous les téléphones sont sur écoute).

Ce document portait comme indication « *Le contrat électronique* » (sic). Il semble dater de 1998.

United-Kingdom - USA Security agreement en matière de renseignement électronique SIGINT

Il faut se féliciter que cette affaire fasse enfin quelque bruit et, en même temps, déplorer que le citoyen s'intéresse trop souvent à des querelles de clocher, alors que, dans le même temps, ses libertés fondamentales — politiques ou individuelles — sont bafouées.

A cet égard, il n'est pas indifférent de signaler que *Le Figaro* était en mesure de publier les éléments de recherche réunis par son journaliste, Christophe DORE, plusieurs semaines avant le quotidien *Il Mondo* qui révéla au grand public cette affaire en Europe.

Les « révélations » publiées par *Il Mondo* sur la NSA et le pacte UKUSA étaient, pour l'essentiel, des données accessibles au public depuis assez longtemps.

I/ Un secret fort mal gardé par le Commonwealth

A/ Des fuites dans la presse

Dès le 28 mai 1986, le *Globe and Mail* de Toronto levait le voile — sans les nommer — sur les activités des groupes P et R de la NSA : « *La NSA est un bras indépendant du Ministère de la Justice américain*

qui gère toutes les communications et les activités électroniques du gouvernement américain » (...) ; « *Pour espionner électroniquement les communications des pays étrangers et des individus* » ; c'est le rôle dévolu au National SIGINT Operations Center au sein du groupe P (Office of signals intelligence operations) ; « *L'agence doit casser leurs codes* » ; il s'agit de la mission confiée au groupe R (Office of Research and Engineering) .

B/ Des conflits de vassalités

Des conflits de vassalité au sein du pacte UKUSA ont permis la divulgation progressive des états inféodés à la NSA et au GCHQ britannique. Le pacte United-Kingdom — Usa security Treaty désigné « secret treaty » est signé en 1947, puis étendu, à partir de 1948, à d'autres services de renseignement du Commonwealth, au rang desquels le CSE canadien, le DSD australien et le GCSB néo-zélandais.

Or, l'allégeance à la NSA induit, dans la pratique, la mise sous tutelle américaine des politiques étrangères des États vassaux du pacte. United-Kingdom — USA Security agreement en matière de renseignement. La Grande-Bretagne, le Canada, l'Australie, la Nouvelle-Zélande et l'Afrique du Sud consentent des abandons de souveraineté en contrepartie desquels ils se croient à l'abri de l'espionnage industriel et diplomatique américain. Or, il n'en est rien.

Aux termes du mémorandum d'Eisenhower de 1953 « *les informations secrètes ne sont communiquées aux alliés que si elles profitent à Washington* ». Cette disposition est respectée à la lettre au détriment immédiat des membres du pacte : les USA, partisans de la préférence supranationale, communiquent avec parcimonie et au gré de leurs intérêts les informations collectées par des nations vassales et déchiffrées sur leur sol et n'hésitent pas à déclarer l'embargo aux nations récalcitrantes.

Quelques exemples de dissensions :

— pendant la crise de Suez en 1956 les Australiens, qui accueillent sans résistance la NSA sur leur sol, font eux-mêmes les frais des bases d'interception qu'ils hébergent : Fort Meade est immédiatement avisé des initiatives diplomatiques de ses hébergeants.

3 les Américains eux-mêmes sont choqués d'apprendre qu'à la faveur d'une opération baptisée « *Shamrock* », l'ensemble de leurs communications à destination de l'étranger étaient interceptées par le centre de Sugar Grove au profit de la NSA,

— en 1985, la NSA, qui n'admet pas l'interdiction d'accostage de navires nucléaires américains, interrompt le transfert d'informations électroniques au profit du Government Communications Security Bureau néo-Zélandais jusqu'à la guerre du Golfe. Ainsi, la parution de l'ouvrage *Secret Power* de Nicky Hager est à mettre sur le compte de l'exaspération d'une nation félonne à l'impérialisme américain au sein même du pacte UKUSA. Cet ouvrage révèle que :

— des stations implantées par la NSA dans les pays membres du pacte peuvent intercepter, sans discrimination, tous les appels téléphoniques, fax, télex, email, SMS, d'où qu'ils viennent où qu'ils aillent, que tout cela peut être collecté, sélectionné, déchiffré s'il y a lieu, puis traité à Fort Meade sur le sol amérindien.

— les membres du pacte se sont dotés d'objectifs dits « civils » (espionnage industriel, diplomatique, parajudiciaire) depuis près de quinze ans,

— les dispositifs britanniques de Morwenstow et Menmith Hill se sont tournés vers l'Europe occidentale depuis la fin de la guerre froide.

— les deux principaux acteurs et bénéficiaires de cet espionnage planétaire sont les États-Unis et la Grande-Bretagne.

II/ S'agissant du fondement moral de la duplicité britannique.

Le degré d'interaction et de collaboration entre les États-Unis et la Grande-Bretagne est une insulte à la décence : la Grande-Bretagne, membre de l'Union Européenne, espionne en permanence, pour le compte des États-Unis et avec leur concours, ses partenaires européens, et, à en croire Sir John Ayde, directeur du *Government Communications Headquarters* depuis 1989, nos amis anglais se flattent d'exé-

cuter leur tâche avec un zèle exemplaire, car ils retirent un bénéfice considérable d'un système qui leur permet d'espionner ses partenaires tout en se plaçant à l'abri d'une telle menace.

Chaque jour, les deux pays se concertent, tout fonctionne comme un unique et vaste système cogéré, des échanges entre officiers de renseignement ont lieu (SUKLO, special UK liaison officer ; SUSLO, special US liaison officer)

Les partenaires européens de la Grande-Bretagne, en particulier, auraient matière à s'indigner : c'est en Cornouailles que convergent les interceptions pratiquées sur l'espace européen. Peut-on encore s'étonner de ce procédé, qui peut apparaître comme un comble de déloyauté, alors qu'il n'est que l'expression naturelle du génie anglais ? Il serait naïf d'oublier certaines choses essentielles :

Le système Echelon est un système anglo-saxon. Tocqueville aurait dit « *anglo-américain* » pour nommer ce qui vient de cette grande famille indéfectiblement unie. (« *Le lien du langage est peut-être le plus fort et le plus durable qui puisse unir les hommes* ») La communauté de langage semble l'emporter — dans l'esprit saxon — sur les autres critères constitutifs de l'État-Nation.

Or, à défaut de langue européenne, les critères avancés jadis par Herder et Ernest Renan — au rang desquels la volonté de vivre en commun, l'identité culturelle, le respect d'une organisation politique et juridique commune — doivent nécessairement présider au raisonnement juridique qui doit conduire une assemblée de peuples européens à se doter de règles communes.

Mais l'Anglais sera toujours, pour reprendre une formule de G B Shaw, une « *race à part* » (« *the English are a race apart* »), qui pensera sincèrement obéir à un principe d'ordre moral et religieux lorsqu'il s'agira de servir son intérêt national.

III/ Quelles sont les incriminations et voies de recours existantes ?

A/ En droit interne

L'adhésion de la Grande-Bretagne au système Echelon dans le cadre du pacte UKUSA compromet les libertés fondamentales du citoyen français. Tout citoyen a droit au respect de sa vie privée personnelle[145] professionnelle et à la garantie du secret de ses correspondances. La participation britannique au programme Echelon doit-elle être qualifiée pénalement d'espionnage ou de trahison ?

Or, le mode opératoire du système Echelon repose sur la violation systématique et permanente de la vie privée. Par conséquent tout citoyen, toute entreprise, victime de tels agissements est fondé à porter plainte entre les mains du procureur de la République de son domicile, de son siège social.

a/ *Commises par des particuliers ou une entreprise*

L'article 226-15, al 2 du Code pénal punit d'un an d'emprisonnement et de 300 000 francs d'amende le fait, pour un particulier ou une entreprise d'intercepter, de détourner d'utiliser, de divulguer, de prendre connaissance de correspondances émises transmises ou reçues par voie de télécommunication (SMS, fax, email, télex) ou de procéder à l'installation d'appareils destinés à les intercepter, quelles que soient les qualités du mandataire chargé de les remettre au destinataire (British Telecom, AT, Compuserve, AOL (...) par exemple). Il s'ensuit nécessairement dans le cas particulier qui nous occupe :

— qu'une entreprise, un individu, bénéficiaire d'une confidence émanant du pacte UKUSA peut être poursuivi du chef de recel du délit d'atteinte au secret des correspondances émises par voie de télécommunication,

— qu'un opérateur de télécommunication, complice du pacte UKUSA pourrait être poursuivi du chef de complicité de ce délit.

b/ *Commises par des représentants de l'autorité publique*

L'article 432-9, al 2 du nouveau code pénal punit de trois ans d'emprisonnement et de 300 000 francs d'amende les interceptions pratiquées par des autorités publiques hors les cas des interceptions judiciaires et des interceptions de sécurité pratiquées par CNCIS

[145] Répression du délit d'atteinte au secret des correspondances par la voie des télécommunications

2/ Trahison ou espionnage

Depuis une loi du 26 juillet 1968, la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique est punie d'un an d'emprisonnement et d'une amende de 120 000 francs. Par ailleurs, le Code pénal a enchâssé en son livre quatrième des incriminations consécutives aux faits d'espionnage ou de trahison : Le fait de communiquer à une entreprise étrangère, une puissance étrangère, un agent étranger des informations intéressant le patrimoine industriel, technique français est qualifié de trahison si l'infraction est commise par un Français, d'espionnage s'il s'agit d'un ressortissant étranger.

Traîtres ou espions ? Qu'en est-il du fonctionnaire de Menmith Hill ? L'abstention britannique de signer la plupart des traités européens autoriserait « une normande hésitation »... si les articles 411-6 et suivants de notre code pénal étaient transposés en droit européen.

B/ En Droit européen

1/ En droit européen des personnes

Il convient de rappeler que le respect de la vie privée est un droit fondamental reconnu et garanti par la Commission européenne des droits de l'homme (article 8), dont le Grande-Bretagne est signataire, et que la seule possibilité d'y déroger — rappelée à l'article 9 de la Convention du Conseil de l'Europe pour la protection des personnes physiques (24 octobre 1995) — autrement dit de surveiller en secret les citoyens se limite à la mesure « *strictement nécessaire à la sauvegarde des institutions démocratiques* », c'est-à-dire que l'on doit être en présence d'infractions d'une certaine gravité et bien délimitées.

La jurisprudence est bien établie d'après les arrêts Klass (1978) contre la RFA et Malone (1984) contre la Grande-Bretagne. Elle proscrit toute surveillance « exploratoire ou générale ». Les États membres, dont la Grande-Bretagne, du Conseil de l'Europe ont rappelé, expressément (octobre 1985), à propos des technologies nouvelles, qu'il était souhaitable d'étendre la protection du droit au respect de la vie privée, « *eu égard à l'intensification de la circulation des données à caractère personnel faisant l'objet de traitement automatisé (...) sur le territoire de chaque partie* ». On ne saurait être plus clair et plus vertueux en bonnes intentions.

L'article 19 de la directive du parlement européen du 24 octobre 1995 permet de saisir le comité consultatif du Conseil de l'Europe et provoquer une réunion de celui-ci, avec, à l'ordre du jour, une question écrite relative à l'application ou à la violation des dispositions de la convention.

2/ S'agissant des acteurs économiques

A la faveur des interceptions pratiquées, des groupes français sont contrés par des groupes anglo-saxons, dès l'émission, pourtant confidentielle, mais hélas formulée par courrier électronique — des réponses aux appels d'offres émanant de l'Union Européenne. Le détournement du secret des correspondances perturbe le libre jeu de l'offre et de la demande sur le marché européen. La Commission de la concurrence et la Commission des droits de l'homme sont compétentes et peuvent être saisies.

3/ Déclencher le repentir britannique et saxon

En droit communautaire, chaque état membre est tenu à une obligation de coopération loyale (traité de Rome, traité de Maastricht, acte Unique, Accord sur l'espace économique européen) à l'égard des autres membres et à faire respecter la parité des conditions commerciales. Or, celle-ci est délibérément et *ipso facto* violée par tout processus d'espionnage économique au profit de nations tierces.

À l'échelon européen, est-il envisageable d'adresser une remontrance solennelle à la Grande-Bretagne en la sommant, face à ce conflit d'intérêt évident, né de son rôle pivot au sein du pacte UKUSA, de faire un choix ? Le veut-on vraiment ?

Il n'est pas sûr qu'on le veuille : les états membres s'accommodent depuis longtemps d'un partenaire qui fait du double jeu une seconde nature, de sorte qu'il est illusoire d'attendre des instances de Bruxel-

les la moindre initiative coercitive. Il ne faut pas renoncer, pour autant, à titre individuel ou à l'échelle gouvernementale, à saisir la Commission des libertés civiques du Parlement européen.

La plupart des commentateurs consultés jugent irréversible la participation (renforcée en 1988 par une intégration indéfectible) de la Grande-Bretagne au pacte UKUSA et font le constat d'évidence que le maintien de cette situation est radicalement incompatible avec le processus maastrichien.

Certaines voix s'élèvent bien, en Grande-Bretagne, contre l'attitude peu honorable de la couronne dans cette affaire d'espionnage planétaire, mais elles sont très minoritaires. D'autres voix se prononcent expressément pour la poursuite de la politique générale actuelle, dont elles vantent les bienfaits tangibles.

Quant à l'opinion britannique, aurait-elle changé depuis 1833 ? Tocqueville prétendait avoir remarqué en Angleterre « *un symptôme alarmant qui distingue le peuple anglais de tous les autres, c'est une parfaite satisfaction de lui-même* : *tout est bien à ses yeux, dans ses lois comme dans ses mœurs.* »

Tout porte à croire que la Grande-Bretagne, confortée par un succès économique et qui jouit d'un crédit appréciable et mérité dans de nombreux domaines, ne se convertira pas d'elle-même à la vertu en abandonnant sa participation au sein du pacte UKUSA. Il est tout aussi illusoire de penser que les USA, si prompts à organiser des missions de contrôle chez les autres, acceptent qu'un organisme supranational, une sorte de conseil de sécurité de l'Europe, pratiquant le « devoir d'ingérence », ait un droit de regard au sein de la NSA. (A cet égard, il est permis de voir dans l'aplomb et la détermination du ministère français des affaires étrangères lors du règlement pacifique de la dernière crise du Golf les prémices d'une autonomie de l'Europe Occidentale en matière d'observation spatiale digne de dénoncer les contrevérités avancées par les observateurs du pacte UKUSA s'agissant de la dissimulation d'un prétendu arsenal chimique en Irak.)

En l'état, la situation est bloquée. Elle est intolérable. Une réaction s'impose à l'échelle européenne, à l'heure où l'essentiel de l'espionnage, qu'il soit politique, diplomatique, économique, technologique, se fait par satellite et grâce à l'interception des télécommunications, tant il est vrai que chaque état membre a le devoir de garantir l'inviolabilité des télécommunications sur son territoire et pour chaque citoyen.

C/ La saisine du législateur européen

Le député européen a reçu compétence en matière de télécommunications par satellite.

Possibilité de faire déposer une question écrite par un député européen.

En effet, le parlement européen a reçu de l'Acte unique compétence en matière de recherche et de développement technologique. Le parlement européen et la Commission ont élaboré déjà plusieurs communications et plusieurs rapports.

Ainsi, le rapport Toksvig, établi en 1985 au sein de la Commission sur l'Énergie, la Recherche et la Technologie, reproche a l'ASE (domaine de l'espace) de mettre l'Europe dans une position de dépendance trop marquée vis-à-vis des États-Unis.

Le second rapport Toksvig, du 25 mars 1987 rappelle le besoin d'indépendance européenne. L'Europe occidentale s'y est employée :

En effet, jusqu'à la mise au point des satellites français Hélios 1/A en 1994 puis Hélios 1/B en 1997 (résultat d'un investissement franco-italo-hispanique), seuls les USA avaient une compétence de reconnaissance au sein de l'OTAN et ne fournissent volontiers de renseignements avérés qu'aux membres du pacte UKUSA

Les images d'Hélios, d'une précision de 1 à 3 mètres seraient exploitées dans le Centre d'Interprétation des données satellites à Torrejon (Espagne) dans le cadre de l'Union de l'Europe occidentale. Les Britanniques semblent exclus de ce dispositif. Est-ce à juste titre ?

La Communication du 26 juillet 1986, ratifiée par les Britanniques, ébauchait les grandes lignes de l'action commune future portant sur :

a/ le renforcement du secteur des télécommunications,

b/ la promotion des techniques satellites dans les réseaux et services européens,

c/ l'implantation de systèmes de communication par satellite dans les politiques communautaires.

Dans le même temps, la Grande-Bretagne — signataire de ce qui précède — concluait un arrimage définitif au programme Echelon et s'engageait a intensifier son activité au sein d'UKUSA ...

Ce document provient du site de *La Tribune.*

Il date du 11 février 2003.

Un antagonisme persistant, Eric Chalmet et Olivier Provost

L'histoire court dans les services de renseignement et les grandes entreprises françaises.

Voilà une dizaine d'années (on parle de 1992-93), les services américains spécialisés dans la sécurité et le renseignement économique nouveau cheval de bataille de la CIA, mais aussi de la puissante NSA, National Security Agency ont voulu faire le point sur les secteurs clés pour l'économie des États-Unis, en particulier pour ses exportations. Sont arrivés en tête l'aéronautique et le spatial (avec Boeing), l'armement, l'agroalimentaire et l'énergie. À partir de là, les Américains ont voulu identifier qui étaient leurs principaux concurrents. Et là, surprise :

Aéronautique ? Les Européens avec Airbus dont le siège est à Toulouse, France. Même chose dans le spatial avec Arianespace. Armement ? Les Français là encore. Idem dans l'énergie, du pétrole au nucléaire en passant par les centrales électriques. Agroalimentaire ? Il fallait une nouvelle fois chercher du côté de l'Hexagone. Selon des industriels français, sur 23 technologies clés identifiées par les Américains, les Français étaient leurs principaux rivaux dans 17 cas.

Dès lors, Washington est fortement suspecté par Paris d'avoir nettement intensifié la pression sur les entreprises françaises. Les plus paranoïaques (ou réalistes ?) parleront d'espionnage. Mais les États-Unis ont aussi et surtout porté au maximum la pression politique exercée sur les pays candidats à l'achat de matériel sensible et leurs efforts dans le cadre des négociations multilatérales, de type de celle du GATT devenu l'OMC (Organisation mondiale du commerce). L'antagonisme entre la France et les États-Unis est particulièrement tangible dans cette enceinte.

Politique agricole, subvention aux producteurs d'acier, règles antidumping, accès aux médicaments génériques des pays en voie de développement sont autant de dossiers qui gênent les relations transatlantiques et sur lesquels la France se trouve en première ligne au sein de l'Union européenne.

Ces dossiers figureront parmi les sujets de discussion de la réunion « miniministérielle » de l'OMC qui se tiendra du 14 au 16 février à Tokyo.

De ce côté de l'Atlantique, il se murmure que pour défendre leurs intérêts économiques, les États-Unis viennent de resserrer leurs priorités hors du cadre feutré de l'OMC, faisant de l'acquisition des technologies sensibles un de leurs nouveaux objectifs. Rumeur que les forts soupçons de déstabilisation de l'entreprise française *Gemplus*, spécialiste mondial de la carte à puce, au profit d'intérêts américains, ne font que renforcer.

La NSA avoue utiliser des cookies et Web bugs pour tracer les visiteurs de sites gouvernementaux.

Selon un certain nombre d'internautes, des sites gouvernementaux américains utiliseraient des « cookies » permanents et/ou des « Web Bugs[146] » afin de tracer l'activité des visiteurs. La NSA vient de confir-

[146] Techniquement, les Web Bugs n'exploitent aucune innovation. Ils se résument, en fait, à une ligne de code qui, embarquée dans une page Web d'un site A, affiche une « image-pixel » (un point de couleur donc, voire un point invisible s'il est de la couleur du fond de page), appelée depuis un site B. De cette manière, le site B peut récupérer des informations assez classiques (adresse IP, type de navigateur utilisé, date et heure de transfert de la page) ainsi que celles stockées dans des cookies partageant le même domaine Internet d'origine. Selon leurs détracteurs, les Web Bugs sont utilisés par les sociétés qui gèrent par exemple les bandeaux de publicités en ligne ou encore les programmes d'affiliation. De cette manière, ces sociétés essayent de consolider des statistiques sur les visiteurs communs à leurs sites affiliés. C'est peut-être le cas en effet. Mais ce n'est pas le seul procédé possible et ces sociétés n'ont d'ailleurs pas attendu les Web Bugs pour tenter d'élaborer des profils inter-sites...

mer l'information. Les « Web bugs » associés aux « Cookies » permanents se révèlent être de redoutables mouchards électroniques.

Cette rumeur persistante a été confirmée dans le courant de la semaine du 29 décembre 2005 par des officiels de la très célèbre « National Security Agency ». Ces officiels ont reconnu avoir recours aux « Cookies » et « Web bugs » afin de tracer l'activité des visiteurs d'une douzaine de sites Internet gouvernementaux. Tout comme les « Cookies », les « Web bugs » permettent de tracer le comportement d'un internaute sur un site Internet. A la différence des « Cookies » les « Web bugs » peuvent également permettre la surveillance des emails.

Les Web bugs sont généralement des images GIF transparentes, de la taille d'un pixel, placées dans une page Web ou un courrier électronique au format HTML, qui s'activent lors du téléchargement de la page et lancent une requête à un serveur distant qui collectera des informations sur l'internaute à son insu. Parmi les informations pouvant être ainsi récupérées, figurent l'adresse IP, le nom et la version du système d'exploitation et du navigateur utilisés, ou même encore la résolution de l'écran de l'internaute.

Les cookies sont de petits fichiers textes stockés par le navigateur Web sur le disque dur du visiteur d'un site Web et qui servent (entre autres) à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site. Le webmestre peut ainsi reconnaître les habitudes d'un visiteur. Les « Web bugs » associés aux « Cookies » permanents se révèlent être de redoutables mouchards électroniques.

Peter Swire professeur de droit à l'université de l'Ohio et rédacteur de la célèbre « *Web Tracking Policy* » rappelle qu'utiliser ce type de technologies est contraire à la réglementation américaine. Les internautes qui se retrouveront envahis de « cookies » permanents et de « Web bugs » peuvent être rassurés, la loi est de leur côté.

Microsoft et la NSA complices[147] ?

Microsoft et la N.S.A

Qui n'a jamais entendu parler de Microsoft et de son « célèbre » produit Windows ? C'est le système d'exploitation le plus répandu au monde : sur les nouveaux ordinateurs, dans les entreprises et même dans l'armée, enfin, partout ! En résumé : une opportunité rêvée pour espionner le Monde entier.

Depuis quelque temps, une rumeur court : le géant de l'informatique Microsoft et la NSA sont associés !

Imaginons que la NSA fournisse des informations sur ses concurrents à Microsoft et que, en échange, Microsoft fournisse à la NSA une porte dérobée sur Windows, en clair : tous les ordinateurs équipés de Windows et ayant une connexion à Internet sont concernés. La NSA a un droit d'accès illimité à vos fichiers lorsque vous vous connectez à Internet.

Mais cela n'est pas prouvé :

Contrairement à d'autres systèmes d'exploitation (comme Linux), Microsoft ne dévoile pas le code source de ses programmes, ce qui rend quasiment impossible les chances de prouver cette coopération pour le moment. Information basée sur un rapport de la Délégation aux affaires stratégiques (DAS) du ministère français de la Défense :

(certains extraits ont été rendus publics par « *Le Monde du Renseignement* » de janvier-février 2000) Ce rapport interne indique qu'il y a des liens entre Microsoft et la NSA. Il dénonce la présence de « backdoors » (porte dérobée) ; ce qui permettrait à la NSA de pénétrer dans vos ordinateurs (avec Windows) à votre insu et sans que vous vous en rendiez compte. Il va aussi jusqu'à suggérer que la NSA aurait

[147] Ce sujet sera développé plus longuement dans la section traitant de la sécurité informatique.

vivement aidé Microsoft à faire surface financièrement et qu'elle aurait contraint IBM à se servir de MS-DOS comme système d'exploitation.

Comment se protéger ?

Pour avoir un ordinateur fiable, il ne faut plus utiliser Windows, mais un autre système d'exploitation, comme Linux , par exemple qui dévoile le code source de ses programmes, ce qui permet de vérifier qu'il ne comporte pas de portes dérobées. Utilisez Netscape, ou un autre navigateur et non Internet Explorer.

Essayez aussi de faire attention aux cookies, ces petites « gâteries » qui vous espionnent en donnant des informations personnelles, comme votre nom, votre adresse email ou des informations sur votre système, ce que vous y faites, à quelle fréquence, etc.

Pourquoi ne pas utiliser les produits Microsoft :

Windows et Internet Explorer (Office) renferment un numéro d'identification de l'utilisateur, le GUID (Globally Unique Identifier). Ce numéro d'identification est ensuite inscrit dans tous les documents créés avec les applications de Microsoft Office. Il peut être consulté à distance par Internet grâce à des commandes spéciales prévues par Microsoft. Le système Windows et Internet Explorer intègrent d'autres commandes spéciales qui permettent de sonder le contenu du disque dur de l'utilisateur, durant ses connexions à Internet. Microsoft a reconnu l'existence de ces commandes spéciales et du GUID.

Extrait du rapport provisoire sur le Réseau Echelon par le Parlement Européen (p104-105) :

« *Excel, par exemple, a fait la une des journaux* : *il a été avancé que dans la version européenne, la moitié de la clé apparaissait en clair dans le header. Microsoft a également attiré l'attention de la presse, car un hacker a trouvé une clé NSA dans le programme, ce que Microsoft dément évidemment avec la dernière énergie. Étant donné que Microsoft n'a pas publié son code source, porter un jugement sur la question relève de la spéculation.* »

États-Unis : *les visiteurs de sites web fédéraux tracés illégalement*

La NSA, les ministères de la Défense, des Finances... De nombreux sites Web gouvernementaux ont recours aux cookies permanents, permettant de suivre la navigation de leurs visiteurs. Au mépris d'une réglementation l'interdisant depuis 2003. Selon une enquête réalisée par *CNET News.com*, des dizaines d'agences fédérales américaines pistent les visites sur leurs sites Web. De l'armée de l'air au ministère des Finances, ces agences gouvernementales américaines utilisent des mouchards ou des cookies permanents pour en savoir plus sur leurs visiteurs. Pourtant, la législation fédérale interdit cette pratique.

Pour repérer les agences qui s'adonnent au pistage électronique, *CNET News.com* a fait développer un programme informatique. Il s'est connecté aux sites Web de toutes les agences répertoriées dans le guide du gouvernement américain (*U.S. Government Manual*) afin d'examiner les techniques de surveillance utilisées. Résultat : beaucoup de cookies qui expirent entre 2006 et 2038 ; la plupart marqués comme valides pendant au moins 10 ou 20 ans.

Des cookies permanents par erreur

Après avoir été contactés par *CNET News.com*, certains ministères ont modifié dans la foulée leurs pratiques. Le Pentagone a affirmé ne pas être au courant que son portail *Defenselink.mil* pistait les visiteurs. « *Nous ne savions pas que les cookies étaient paramétrés pour expirer en 2016* », a déclaré un représentant du Pentagone mercredi. « *Tous les cookies que nous avions définis avec* WebTrends *devaient être strictement temporaires ; nous avons immédiatement pris des mesures.* »

WebTrends est un service commercial de surveillance du Web, utilisé également par la Maison Blanche.

La National Security Agency (NSA) vient elle aussi d'être vivement critiquée pour ses cookies permanents, qui permettent de surveiller les visiteurs de son site. Après une enquête et des révélations de l'*Associated Press*, elle a tout interrompu.

« *C'est la preuve même que le respect de la vie privée n'est pas pris au sérieux* », a déploré Peter Swire, professeur de droit à l'université de l'État d'Ohio.

Une directive du gouvernement américain de 2003 stipule pourtant que, d'une manière générale, « *il est interdit aux agences d'utiliser des mouchards ou des cookies pour pister les internautes* ». Ces deux techniques permettent d'identifier des visiteurs réguliers et, selon leur configuration/paramétrage, de suivre également des comportements de navigation sur des sites non gouvernementaux.

Un manque de clarté et des exceptions

Si la pratique consistant à définir des cookies permanents est donc globalement interdite, leur exploitation n'est en outre pas claire. Dans le pire des cas, ils peuvent être utilisés pour s'immiscer dans la vie privée d'une personne, en mettant en corrélation ses visites sur des milliers de sites Web. Mais ils peuvent aussi être totalement inoffensifs, en permettant à un internaute de définir la langue par défaut d'un site Web, par exemple.

La surveillance des internautes n'est pas totalement prohibée. La directive américaine de 2003 prévoit une exception pour les agences fédérales qui en ont un « besoin impérieux ». À condition cependant de le dire et de recevoir l'approbation de leur hiérarchie. La directive ne s'applique pas non plus aux sites Web des gouvernements des États américains, des tribunaux, ni à ceux créés par des membres du Congrès.

Le type de traçage le plus intrusif réside probablement dans les cookies d'éditeurs commerciaux, adoptés délibérément. Ils permettent de mettre en corrélation des visites sur des milliers de sites Web. Ainsi, un internaute se rendant sur le site du Pentagone pourrait être identifié comme étant la même personne qui a consulté les sites *Hilton.com* et *HRBlock.com*, car ces deux sociétés sont des clients *WebTrends*.

Les éditeurs de cookies se défendent

Pour sa part, WebTrends dément mettre en corrélation ces informations. « *Les éditeurs qui ont essayé de le faire par le passé ont eu très mauvaise presse* », souligne Brent Hieggelke, vice-président du marketing de l'éditeur. « *Nous ne traçons pas le trafic d'un site à un autre* », a-t-il assuré. « *Nous ne proposons pas de services permettant d'avoir une vision du trafic entre des sites n'ayant aucun rapport entre eux.* »

Les défenseurs des libertés individuelles se méfient de ces cookies. Ils redoutent notamment les éventuelles failles de sécurité, qui mettraient à nu les habitudes de navigation sur le web.

« *Si WebTrends a la possibilité de relier une visite sur le site de la Maison blanche à une visite sur un site commercial, cela ressemble fort à du pistage persistant* », estime Peter Swire, le professeur de droit de l'Ohio. « *Il serait utile de commander un audit indépendant de la situation.* »

Pas de revente, mais un simple sondage d'usage

Du côté des éditeurs, on se défend. Notamment *Statcounter.com*, dont le programme de statistiques sur le Web met en place des cookies tiers. Il est utilisé par les ministères américains du Commerce et de l'Énergie. La société irlandaise se défend de mettre en relation les informations de plusieurs sites internet. « *Nous ne vendons aucune information à des tiers* », affirme son représentant américain. « *Les seules informations qu'il nous intéresse de collecter sont celles indiquant (à un webmestre) d'où viennent les visiteurs, ce qu'ils ont consulté, les informations vers lesquelles ils sont retournés... des données qui indiquent la manière dont le site est utilisé.* »

Des règles claires ont pourtant été fournies en juin 1999, sous l'administration Clinton. L'Office of Management and Budget (OMB) de la Maison blanche a publié des premières recommandations à destination des agences fédérales. Ce document de dix pages leur donnait trois mois pour diffuser sur

leur site des règles de respect de la vie privée « *clairement énoncées et faciles d'accès* », et proposait des formulations.

Une situation explosive depuis 2000

Pourtant, en 2000, le système de suivi utilisé allègrement par le site de lutte antidrogue *Freevibe.com* de la Maison blanche, a suscité une controverse publique. Peu de temps après, la présidence américaine a publié une directive interdisant aux agences d'utiliser sur leur site toute forme de cookies ou autres « *mécanismes automatiques de collecte d'informations* », sauf circonstances particulières. La toute dernière directive de 2003 a étendu l'interdiction aux cookies permanents, autorisant en revanche les temporaires, valides uniquement le temps d'ouverture de la fenêtre du navigateur.

Le non-respect avéré des règles a plongé dans la tourmente les agences gouvernementales concernées. En 2001, l'inspecteur général du ministère de la Défense américain a passé au crible ses 400 sites, et a trouvé des cookies permanents sur 128 d'entre eux. En 2002, la CIA a reconnu avoir utilisé les cookies proscrits sans autorisation appropriée, et les a retirés de ses sites.

Aujourd'hui, le niveau de conformité aux règles semble avoir peu évolué depuis l'étude réalisée en 2000 par le General Accounting Office. Elle révélait qu'au moins une dizaine d'agences continuaient d'utiliser des cookies en apparente violation des règles.

Les développeurs de sites montrés du doigt

Bon nombre des cookies sur les différents sites ont été générés par l'outil de création Web *ColdFusion*, très populaire. Lorsqu'il crée certains types de cookies, il les définit par défaut comme des cookies permanents qui doivent expirer environ 30 ans plus tard, a expliqué Tim Buntel, chef de projets senior.

Les créateurs de *ColdFusion* encouragent les développeurs Web, lorsqu'ils montent un site, à faire en sorte de pouvoir gérer et modifier les paramètres des cookies à loisir, recommande Tim Buntel. « *N'importe quelle application créée avec ColdFusion peut être entièrement développée sans l'utilisation du moindre cookie* », précise-t-il.

Des représentants de plusieurs agences se sont dits surpris de trouver des cookies sur leur site web. Ils ont mis en cause son concepteur, qui aurait dû s'informer des paramétrages par défaut avec *ColdFusion*.

Un paramétrage par défaut mis en cause

Même cas de figure pour la Defense Threat Reduction Agency, qui dépend du Pentagone. « *Lorsque l'agence a installé ColdFusion (logiciel de développement Web d'Adobe Systems, Ndlr) sur notre serveur Web, nous avons configuré le logiciel en appliquant ses paramètres par défaut* », a expliqué William Alberque, porte-parole de la Defense Threat Reduction Agency. « *Or il s'avère que la configuration par défaut génère des cookies de session qui peuvent rester sur votre ordinateur pendant 30 ans ou jusqu'à ce qu'ils soient supprimés* ». Mais « *nous n'avons jamais conservé de base de données contenant ce type d'informations* », tient-il à préciser. « *Honnêtement, je ne pense pas que quiconque ait même été au courant de leur existence, mais c'est maintenant le cas et nous allons agir en conséquence* », a assuré Daniel Horowitz, porte-parole de l'U.S. Chemical Safety and Hazard Investigation Board, agence fédérale de prévention des risques sanitaires industriels.

L'un des administrateurs du site du National Air and Space Museum, dédié à l'aéronautique et l'aérospatiale, a initialement contesté l'existence des cookies persistants détectés par *CENT News.com*. Avant de reconnaître que les paramètres *ColdFusion* étaient probablement en cause. « *Quoi qu'il en soit, je peux vous assurer que nous n'utilisons et ne diffusons pas d'informations récoltées par des cookies* », a certifié le représentant.

Quelques agences, dont le Federal Reserve Bank System et l'U.S. Institute of Peace, ont ainsi fait savoir qu'elles étaient indépendantes, et donc non soumises à la directive 2003 de l'OMB. « *Nous ne*

sommes pas une agence gouvernementale », a soutenu Calvin Mitchell, vice-président de la Federal Reserve Bank (banque de réserve fédérale) de New York. « *Nous essayons de respecter l'esprit de certaines réglementations gouvernementales, mais nous ne sommes pas tenus de nous y conformer* ».

Les sites .mil *ou* .gov *doivent être conformes*

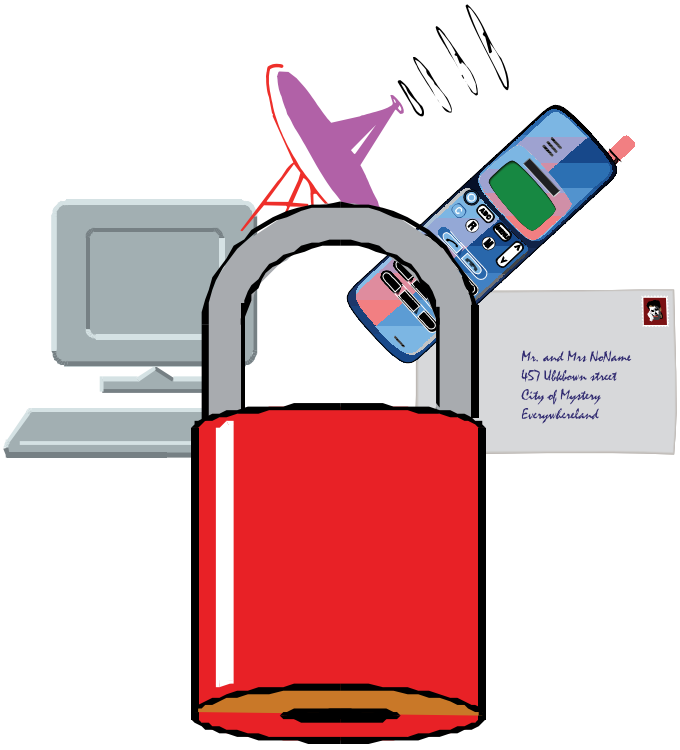
Un officiel de la Maison blanche a proposé une interprétation différente. « *Concernant les sites Web du gouvernement fédéral, la politique est claire. Tout site se terminant par .mil ou .gov est soumis à la politique fédérale telle qu'elle est définie dans les recommandations de l'OMB* », a déclaré David Almacy, responsable Internet de la Maison blanche.

Seule une agence fédérale contactée cette semaine semble en parfaite conformité avec la directive. Le National Institute of Dental and Craniofacial Research indique avoir reçu en janvier 2005 l'autorisation d'activer des cookies sur son site Web pour une étude. Les cookies, d'une validité d'un mois, permettent d'éviter de demander aux mêmes personnes de participer à l'enquête.

La Maison blanche assure pour sa part respecter la directive, puisqu'elle utilise une image de 1x1 pixel qui se charge à partir du site de WebTrends. « *Aucun cookie n'est placé sur le site Web, que ce soit à partir de la Maison blanche ou de WebTrends* », a précisé David Almacy. « *Aucune information personnelle n'a été recueillie. Le site de la Maison blanche respecte et a toujours respecté les recommandations de l'OMB.* »

Les hommes politiques eux-mêmes semblent ne pas donner l'exemple. Soixante-six parlementaires du Sénat américain et de la Chambre des représentants utilisent les cookies permanents sur leurs sites. Sur ce nombre, 23 (18 républicains, et 5 démocrates) s'étaient pourtant engagés à ne jamais s'en servir, dénonçant le principe, a appris *CNET News.com*. Mis en cause, certains ont assuré ne pas être au courant de la présence de cookies sur leurs pages.

Les moyens de garder le secret des télécommunications



Préface

Depuis que l'homme communique à distance et quel que soit l'objet de ses communications, il a cherché le moyen de garder secret le contenu de ses messages, en laissant à son seul destinataire la compréhension.

Du général à l'amoureux transi, du financier au truand, tous ont recours à des méthodes de *brouillage* de leurs messages. Nous disons *brouillage* dans un premier temps, car les méthodes utilisées par les uns et les autres ne s'apparentent pas forcément à du « chiffrage » pur et dur comme nous l'étudierons plus loin, mais parfois à des procédés originaux, fruits de l'imagination d'autant plus exubérante que le message a d'importance aux yeux de l'expéditeur.

Nous rappellerons dans un premier temps des faits historiques bien connus ou découverts à l'occasion de nos recherches. Nous verrons les méthodes originales utilisées pour masquer le vrai contenu d'un message écrit. L'utilisation de pictogrammes n'étant pas utilisables par la plupart des procédés de communication actuels sera tout de même évoquée. Mais la plupart des autres moyens, y compris la stéganographie, qui permettent de crypter un texte avant émission feront l'objet de cette étude.

On peut dire que dès le début de l'utilisation des moyens de communication à distance, quelle qu'en soit la méthode, sonore ou optique, des codes furent en usage. Les messages écrits, évidemment, dès qu'ils devaient être transmis par un intermédiaire, furent codés ; et ce sont souvent les mêmes méthodes de codage ou des méthodes dérivées qui furent utilisées pour la télécommunication à ses débuts.
L'avènement des moyens « modernes », télégraphe puis radio, empruntèrent souvent à l'Histoire des procédés de codage réputés inviolables. Le combat entre cryptographes et cryptanalystes, qui continue de nos jours, nous a apporté quels hauts faits . Les mathématiques, nerf de la cryptographie moderne, ont vu de grands cerveaux développer, grâce notamment à l'outil informatique, des algorithmes de plus en plus complexes et sûrs. Mais gageons que les mêmes moyens, entre les mains des « *casseurs de codes* » de tous poils n'assureront que provisoirement la sécurité des télécommunications.

En réalité, nous pensons que seule la masse vertigineuse d'informations circulant avec les moyens modernes est le rempart, fragile malgré tout, qui protège les communications « sensibles ». C'est en effet le tri, dans ces milliards d'octets, qui pose le plus de problèmes actuellement.
Reste que la sécurité de tout système repose sur le maillon le plus faible, et que souvent ce maillon est en amont du système de cryptage. À quoi bon crypter avec un algorithme ultra performant si n'importe qui peut capturer à quelques mètres de distance ce que l'on frappe sur son clavier ? Pourquoi chercher à casser une clé de codage bancaire alors qu'il suffit de regarder par-dessus votre épaule quand vous saisissez votre code ?

Et puis il y a le problème de la sécurité intérieure des nations. Les législations en la matière sont diverses et variées selon les régimes en place. L'encadrement de l'utilisation de moyens de cryptage a pour objectif de permettre un contrôle par les autorités. Mais cela reste bien illusoire, car les terroristes, pour ne citer qu'eux, ne vont pas s'embarrasser avec la législation ! De plus, la mise en lumière dans des affaires récentes, soit de criminalité, soit de trafics en tout genre ou de terrorisme, des possibilités d'identification

ou de localisation des auteurs de messages, ainsi que du contenu de ceux-ci, incite vraisemblablement les malfrats à s'éloigner des nouvelles technologies. On doit cependant admettre de sacrifier un peu de sa liberté si l'on souhaite continuer à vivre sous nos régimes démocratiques. « Big brother » devient un mal nécessaire et l'impression d'être « fliqués » est à mettre en balance avec la sécurité des personnes. Et au fond, même si tout le monde a son jardin secret, qui peut croire sérieusement que des services secrets s'intéressent à vous ? À moins que...

La vigilance s'impose tout de même, et il ne semble pas raisonnable de laisser un pays ou une nation s'arroger le droit au contrôle de la correspondance privée, quelque en soit le procédé.
C'est dans la troisième partie de cet ouvrage que nous traiterons des attaques de la correspondance et des télécommunications et moyens de protection à mettre en œuvre dans la vie courante ainsi que des précautions à prendre, en particulier avec Internet.

Nous ne résistons pas à citer Blaise de Vigenère[150] dans son *Traicté des Chiffres ou Secrètes manières d'écrire* :

Entre les autres dons de grace qu'il a pleu à Dieu impartir à l'homme, pour aucunement le recompenser des miseres et pauvretez où la transgression des premiers parens le fait naistre ; et de tant de travaux, mesaises[151], dangers, inconveniens, et malheurs à quoy sa fragilité l'abandonne, est l'usage de la raison, et de la parole, que les Grecs, non sans grand mystere, comprennent sous le seul mot de λόγοσ ; ce dont principalement il differe des bestes brutes, avec lesquelles il participe d'un costé des facultez sensitives de l'ame ; et de l'autre, des naturelles avec les arbres et les plantes. Or ceste parolle assistee de la raison est en nous, ce qu'en la divinité la premiere emanation eternelle, assavoir le verbe, ou la sapience, *Quae ex ore altissimi prodiuit primogenita ante omnem creaturam*, en l'Ecclesiastique 24. Double au reste ; l'une animee de vive voix, procedant de l'estomac par la langue, en mots articulez et distincts ; Et l'autre, assavoir l'escriture, qui fait l'office de la parolle, comme muette et taisible[152], separee à part hors de nous, dont la main en est l'instrument : Toutes deux servans d'exprimer les interieures conceptions de nostre ame, d'où depend le noeud et lien principal de la societé humaine ; qui ne se sçaurait conserver sans une police bien ordonnee ; ne la police s'establir sinon par le moien de la raison : laquelle, nonobstant que dame et maistresse de toutes choses, sans le benefice de la parolle qui la jecte de puissance en action, ne pourroit sortir ses effects, ains demeurroit comme inutilement ensevelie à par soy dans l'estomac des personnes. Mais encore l'une et l'autre que seroient elles sans le secours de l'escriture, leur commune coadjutrice, qui ne se peult restreindre d'aucunes bornes qu'elle ne s'extende par tout ? Peu de chose certes, selon qu'on peult voir és sauvages des terres neufves, si barbares, incivils, bestiaux, estans privez de son usage. Cela nous est aucunement representé par la loy donnee de bouche au Prophete Moyse, et la loy escrite, qui est comme une ame de l'autre tenant lieu du corps : car la loy donnee de bouche, ce dient les sages Hebrieux en leu secrete theologie, n'a aucun fondement ny authorité sinon de la loy escrite ; nomplus que la Lune n'a point de lumiere fors ce qu'elle en reçoit du Soleil ; que Platon appelle la clarté transmise et infuse de la divinité en nos ames, pour les conduire et eslever à la cognoissance du monde intelligible : et celle de la Lune, l'instinct et discours naturel de raison, moiennant lequel, selon qu'il est exercé, nou-nous acquerons la science des choses celestes, et elementaires, au monde sensible. Mais les Cabalistes de leur costé, suivant ce verset du pseaume 19. *Dies diei eructat verbum ; et nox nocti indicat scientiam*, nomment ceste lumiere là, le jour, d'autant que c'est le Soleil qui le constitue ; le fils, et le laict ; le miroüer luisant aussi, et le sacrifice matutinal,

[150] Blaise de Vigenère dont nous reparlerons a écrit ce traité en 1586. Son système de code a résisté trois siècles environ à la cryptanalyse.
[151] Malaise, embarras, chagrin.
[152] Qui es-tu ?

qu'on offroit à Dieu pour l'avoir favorable et propice : et l'autre, la nuict à laquelle la Lune preside, la fille, et le vin ; comme l'interprete Elchana fort celebre docteur Hebrieu ; le miroüer non luisant tenebreux; et le sacrifice du soir, pour radoulcir la rigueur et severité de sa justice: ou, comme met plus particulierement le Zohar, le sacrifice du matin s'addressoit à Dieu, qui est appellé feu mangeant, et reunissant ; et celuy du soir pour mitiguer les puissances nuisibles, aux adversaires qui accusent les creatures devant le tribunal de sa majesté, à la main gauche et partie du Septentrion ; là où se faisoit division de la viande, à ce qu'à chacune desdites puissances ennemies, s'en distribuast sa part et portion. A ces deux encore se raportent l'Intellect agent, plein de formelles intelligences, qui tient lieu de masle et de Pere ; et l'intellect materiel ou passible, de femelle, et d'une generale tres-feconde mere du monde : Dequoy ne s'esloigne guere Platon, quand il discourt au mesme endroit, de la formation de l'homme, qui est la mesure de toutes choses ; *Qu'il estoit double*, (l'un interieur fault entendre, car il descrit cela d'une autre façon, et l'autre externe) *chacun avec ses propres et particuliers sentiments* ; l'ayant emprunté de Genese, là où au commencement il est dit, *Que Dieu crea l'homme à son image et ressemblance ; masle et femelle il les crea* ; neaumoins la femme n'estoit pas encore produitte : si qu'il presuppose l'homme interieur spirituel par le masle, qui est le meilleur et plus excellent ; et par la femelle l'exterieur, corporel et sensible, qui est le pire ; comme le marque aussi l'Apostre en tout-plein d'endroits. L'escriture ausurplus est double ; la commune dont on use ordinairement ; et l'occulte secrete, qu'on desguise d'infinies sortes, chacun selon sa fantasie, pour ne la rendre intelligible qu'entre soy et ses consçachans : Ce sont les chiffres, comme on les appelle d'un mot corrompu, aujourd'huy non appropriez à autres effects que pour les affaires du monde, et les negociations et practiques, aussi bien des particuliers que des Princes ; là où anciennement les Hebrieux, Chaldees, Egyptiens, Ethiopiens, Indiens, ne s'en servoient, que pour voiler les sacresecrets de leur Theologie, et Philosophie ; *Nam aliud Cabalista profert et scribit, aliud subintelligit et legit* ; Afin de les garentir et substraire du prophanement de la multitude, et en laisser la cognoissance aux gens dignes ; par ordonnance expresse du Talmud, qui porte ; *Non dabunt arcana legis, nisi consiliario sapienti* : Pourautant qu'ainsi que parle le Philosophe Melisse dedans le dialogue du Sophiste ; *Les yeux de l'ame du commun peuple, ne sçauroient bonnement supporter les lumineux estincellemens de la divinité* : A quoy se conformant Sainct Denys ; *Nous ne pouvons voir ne contempler Dieu* (dit-il) *sinon entant que ses luisans rayons viennent à s'introduire en nostre ame, pour y esclairer, tout ainsi que quelque chandelle ou flambeau dans un fanal*. Le Soleil mesme, à l'exemple de celuy dont il est l'image visible; et duquel il est dit au pseaume 36. *In lumine tuo videbimus lumen* ; ne se peult voir que par sa propre lumiere.

Ce traicté donques sera de semblables usages de chiffres, diversifiez en plusieurs manieres ; tant pour incidemment parcourir ce qui se presentera à propos de ces beaux et cachez mysteres, adombrez sous l'escorce de l'escriture ; que pour à l'imitation de cela en trasser beaucoup de rares, et à peu de gens divulguez artifices ; partie de nous apris et receuz des autres, voyageant ça et là en divers endroits de l'Europe ; et la plus grand'part provenans de nostre forge et meditation ; non encore, que nous sçachions, touchez jusques icy d'aucun.

Maintenant, ouvrons le livre de l'histoire de la cryptographie.

Écriture et codes

L'aventure des écritures

Chronologie sommaire

- 3300

Tablettes sumériennes en écriture pictographique à Uruk (basse Mésopotamie) : le plus ancien témoignage d'écriture connu.

- 3200

Hiéroglyphes égyptiens.

- 2800

L'écriture pictographique sumérienne devient cunéiforme.

- 2000

Le cunéiforme est utilisé pour noter l'akkadien (assyrien et babylonien) ;
Le sumérien subsiste comme langue savante.
Traces d'écriture chez les Olmèques (Amérique centrale).

- 1800

En Crète, écriture dite « linéaire A » (Cnossos), indéchiffrée.
Code d'Hammourabi (Babylone).

- 1600

Les Hittites utilisent un système hiéroglyphique.

1500

Au Proche-Orient, écriture protosinaïtique : 30 signes à allure hiéroglyphique ;
Écritures protocananéennes.

- 400

Chine : textes divinatoires gravés sur os ou plastrons de tortue.
Alphabet ougaritique (Syrie du Nord) : 30 signes cunéiformes.

- 300

Alphabet phénicien de 22 lettres-consonnes.

- 1200

Sarcophage d'Ahiram à Byblos, en alphabet phénicien de 22 lettres.

- 1000

L'alphabet phénicien se répand en Méditerranée et vers l'Asie.
Alphabet paléohébraïque.
Alphabet araméen.
Écritures sud-arabiques.

- 800

Alphabet grec ;

Invention des voyelles.

- 700

Alphabet étrusque adapté de l'alphabet grec.

En Égypte, écriture démotique.

- 600

Écriture hébraïque, dite « hébreu carré ».

- 400

Alphabet latin adapté de l'alphabet étrusque.

L'écriture grecque se répand grâce aux conquêtes d'Alexandre le Grand.

- 300

Deux écritures syllabiques en Inde : la kharosthi (d'origine araméenne) qui essaime vers l'Asie centrale et la brahmi qui donne naissance par la suite à de nombreuses écritures syllabiques en Asie du Sud-Est et en Indonésie.

Dans l'empire romain, floraison d'inscriptions lapidaires en quadrata (capitales).

- 200

« Pierre de Rosette » : copie d'un décret de Ptolémée V sur une stèle en hiéroglyphes égyptiens, en démotique et en grec.

Écritures punique et libyco-berbères attestées en Afrique du Nord.

- 100

Écriture nabatéenne (Petra).

Écriture copte en Égypte.

« 0 »

Invention du papier en Chine.

100

Écriture syriaque.

Apparition d'écritures cursives communes latines

200

L'onciale (majuscule avec emprunts aux cursives romaines) se répand en Europe.

Stèles mayas en Amérique centrale.

300

Écriture runique.

400

Alphabet sogdien dérivé de l'araméen, en Asie centrale.

Alphabet arménien.

Alphabet géorgien.

Syllabaire éthiopien

500

Premières inscriptions arabes.

Écritures gaélique.

600

La révélation coranique entraîne la codification de l'écriture arabe ; elle essaime vers l'Orient et vers l'Afrique du Nord.

700

Le Japon adapte l'écriture chinoise.

800

En France, la « minuscule caroline » remplace les graphies latines antérieures, devenues presque illisibles, et devient un modèle pour l'avenir.

Le persan emprunte l'alphabet arabe et le pehlevi tombe en désuétude.

En Asie, écriture ouïgoure dérivée de l'araméen.

Apparition de l'écriture cyrillique.

1000

La caroline se transforme en gothique et évolue par la suite vers la textura et la rotunda.

Les Turcs empruntent l'alphabet arabe.

1200

Écriture nahuatl adoptée par les Aztèques (Amérique centrale).

1300

En Italie, les humanistes redécouvrent la caroline et la transforment en écriture humanistique, modèle des écritures modernes utilisant les caractères « latins ».

Généalogie du signe et mémoire du graphe

Nos signes d'aujourd'hui ont connu leur époque mythique et légendaire avant de servir d'introduction à l'Histoire : nos lettres sont intimement liées, le plus souvent à notre insu, aux graphies les plus anciennes. Comme nos visages ont un air de famille avec ceux de nos aïeux, les lettres sont aussi modelées à la ressemblance de leurs aînées ; leurs traits, leur physionomie résultent d'une longue transmission.

Avons-nous souvenance, lorsque nous traçons la lettre *a*, d'évoquer par ce signe une tête de bœuf ? Lovée au sein de la petite « arrobe » (@) de notre courrier électronique, elle fête allégrement ses cinq mille ans d'âge ? Savons-nous que notre *n* fut jadis un petit serpent, tracé par des milliers de scribes attentifs et que nous ne faisons que repasser dans le même sillon ? Acharnés à déchiffrer d'antiques graffitis que nous croyons étrangers à nous-mêmes, à en chercher inlassablement le sens (écritures « indéchiffrées », langues « inconnues »), nous ne songeons pas à interroger ce qui vient simplement sous notre plume.

Ces lettres que nous traçons quotidiennement sont le plus récent état d'une perpétuelle métamorphose. Nées depuis l'aube des temps, elles ont eu aussi au fil des siècles des compagnons d'essai maintenant disparus et elles ont accueilli en leur groupe des membres nouveaux. Au cours des temps, mais aussi au gré des hommes qui, après avoir ébauché et façonné ce bel outil, ont continué de génération en génération de le pétrir et de le perfectionner sans répit pour faire coïncider le mieux possible formes et fonctions, habillant ou déshabillant consonnes et voyelles, les compactant dans des abréviations au risque de les rendre illisibles, les unissant par des ligatures, les affublant d'atours divers, leur faisant perdre ou gagner ces petites moustaches pendantes que sont les cédilles, les ornant de points, d'accents plus ou moins compliqués, les entourant enfin, pour leur venir en aide, de ces compagnons silencieux que sont les signes de renfort de l'écriture, virgules, traits d'union, parenthèses... Et, ce faisant, un étrange corps à

corps se livrait dès l'origine entre l'utilité de la lettre et sa beauté, entre lisibilité et esthétique, entre effort vers le visible et désir du secret.

L'écriture et les écritures secrètes

La diversité des systèmes d'écriture et des langues constitue déjà en elle-même une forme de codage. Souvenons-nous des hiéroglyphes dont la compréhension fut perdue pendant plusieurs dizaines de siècles.

L'écriture cunéiforme

L'écriture cunéiforme originaire de Mésopotamie, berceau de l'écriture, a été employée du III^e^ au I^er^ millénaire av. J.-C. Elle servira à transcrire successivement le sumérien, l'akkadien, le hittite et le perse.

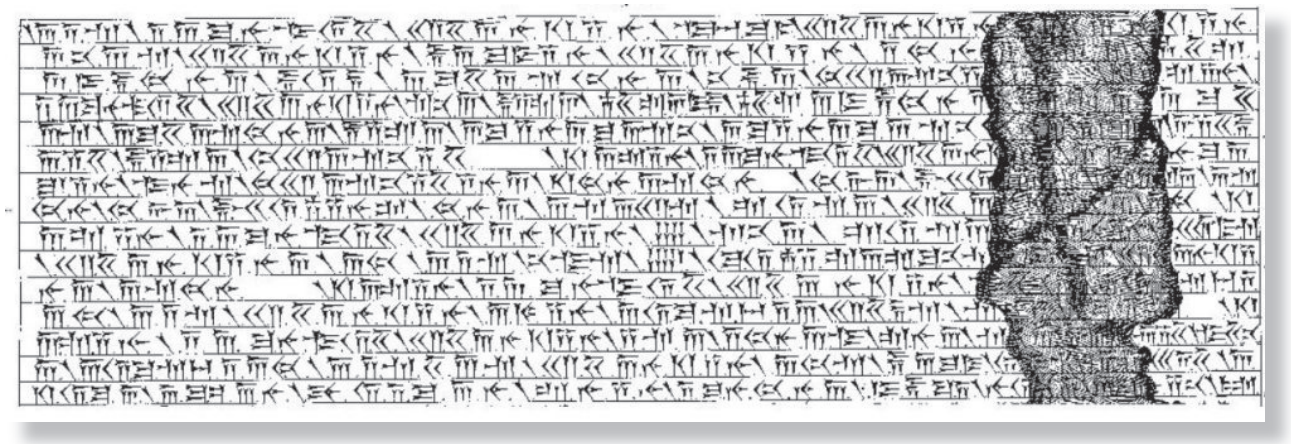
Elle se compose d'un grand nombre (au moins 300 à la basse époque) de signes, constitués par des traits en forme de « coins » et de « clous » plus ou moins diversement enchevêtrés, et qui représentent la stylisation sur argile de dessins linéaires primitifs traduisant des objets concrets. Les chiffres sont notés par des encoches, les marchandises par des pictogrammes.

Les plus anciens signes d'écriture ont été retrouvés essentiellement à Uruk (actuelle Warka, en Irak), ancienne capitale du pays de Sumer ; on les a datés d'environ 3300 av. J.-C. L'apparition de l'écriture coïncide avec l'essor des villes, dans des sociétés en mutation, où viennent de pénétrer l'invention de la roue et la technique du cuivre moulé et qui possèdent déjà tout un répertoire de signes et de symboles dans leurs arts plastiques.

L'écriture est née surtout de la nécessité ressentie par ces hommes de conserver la trace de leurs échanges. Ce sont les Sumériens qui finalisent le système, les Élamites n'allant pas au-delà de leurs propres pictogrammes et empruntant plus tard le modèle sumérien pour noter leur langue.

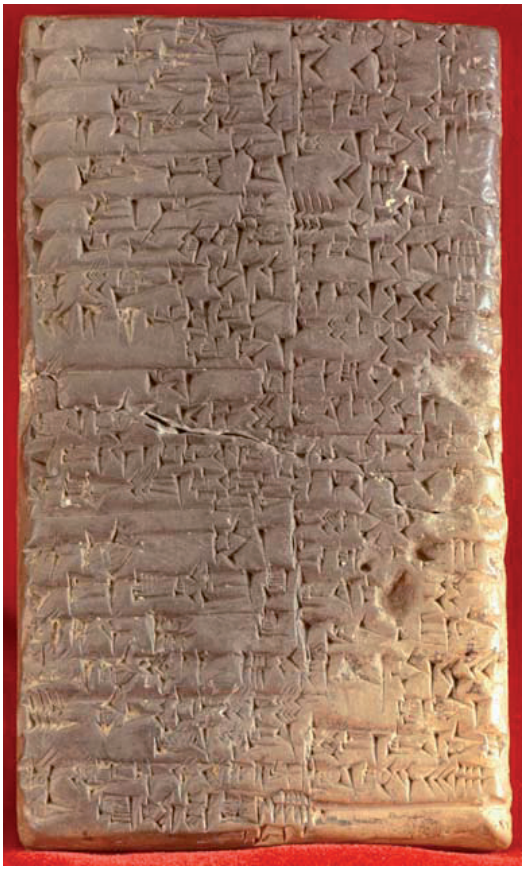
Premières tentatives de traduction

Les caractères cunéiformes découverts par les premiers voyageurs sur certaines ruines et, en particulier, sur celles de Persépolis, en Iran, sont longtemps restés non déchiffrés. En 1621, Pietro Della Valle, un voyageur italien, remarqua les 413 lignes inscrites sur la paroi rocheuse de Béhistun (ci-dessous), dans l'ouest de l'Iran, et en recopia certains signes. En 1674, Jean Chardin, un négociant français, publia



des groupes complets d'écriture cunéiforme et observa que les inscriptions se présentaient toujours par séries de trois formules parallèles. Les premiers progrès réellement enregistrés dans le déchiffrage de l'inscription de Béhistun sont le fait de Carsten Niebuhr, un membre allemand de l'expédition scientifique

danoise au Proche-Orient de 1761 à 1767. Il fut le premier à penser, à juste titre, que ces inscriptions en trois parties pourraient être des transcriptions d'un même texte dans trois types d'écriture inconnus, et il publia, en 1777, les premières copies complètes et précises de l'inscription de Béhistun. Ces grandes inscriptions trilingues de Darius Ier, roi de Perse, étaient rédigées en cunéiformes perses, élamites et babyloniens. Les rois perses de la dynastie des Achéménides utilisaient ces trois systèmes d'écriture afin que leurs décrets soient connus de leurs sujets de ces trois nations.



L'écriture cunéiforme perse fut la première des inscriptions déchiffrées. Les chercheurs allemands Oluf Gerhard Tychsen et Georg Friedrich Grotefend ainsi que le philologue danois Érasme Christian Rask identifièrent chacun plusieurs signes. L'orientaliste français Eugène Burnouf déchiffra ensuite la majorité des signes du système d'écriture cunéiforme perse, tandis que l'assyriologue britannique Henry Creswicke Rawlinson interprétait indépendamment le texte qu'il avait recopié lui-même à partir de la paroi de Béhistun, et publia les résultats de ses recherches en 1846. Le déchiffrement du système cunéiforme perse fut facilité par la connaissance du pahlevi, langue descendant du vieux perse. Le système perse est le plus simple et le plus tardif de tous les systèmes cunéiformes. Il se compose de trente-six caractères, qui sont presque tous alphabétiques bien que certains soient aussi employés pour certaines syllabes simples. En outre, le système cunéiforme du vieux perse utilise un signe comme séparateur entre les mots contigus. Il fut employé de 550 à 330 av. J.-C. Le plus ancien échantillon qui nous soit parvenu est sans doute une inscription de Cyrus le Grand à Pasargades[153], et le plus récent, celle d'Artaxerxès III (qui régna aux environs de 358-338 av. J.-C.) à Persépolis.

Le cunéiforme élamite est souvent appelé « la langue de la deuxième formule » parce qu'elle occupe la deuxième position sur l'inscription trilingue des rois achéménides. Son déchiffrement fut entrepris tout d'abord par l'orientaliste danois Neils Ludvig Westergaard en 1844. Le fait que le texte de l'inscription trilingue soit repris mot pour mot dans chacune des écritures cunéiformes fut d'une grande importance dans la traduction de l'élamite, pour laquelle aucune langue connue à l'époque ne pouvait fournir d'aide. Ce système contient quatre-vingt-seize signes syllabiques, seize logogrammes et cinq déterminants. Le sens des textes élamites est généralement clair, même si la signification de certains mots demeure encore incertaine. La version babylonienne de l'inscription de Béhistun fut déchiffrée grâce aux efforts conjoints de l'orientaliste français Jules Oppert, de l'orientaliste irlandais Edward Hincks, de l'archéologue français Caignart de Saulcy, et de Rawlinson. La similitude

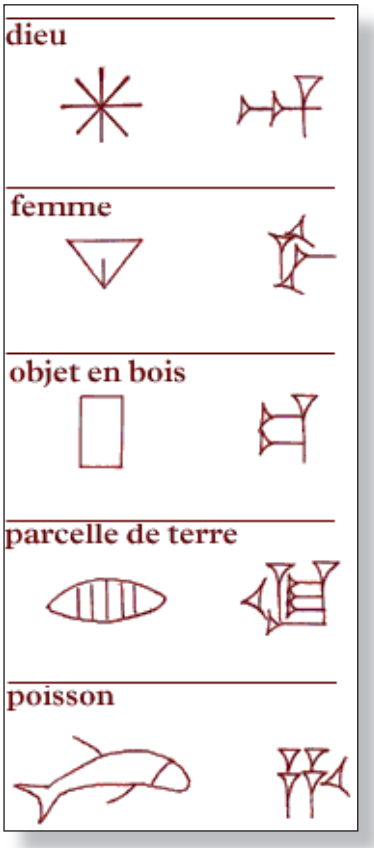
[153] Pasargades fut la première capitale dynastique de l'Empire achéménide fondée au VIe siècle avant J.-C. par Cyrus II le Grand, au cœur du Fars, la patrie des Perses. Ses palais, jardins, et le mausolée de Cyrus constituent de remarquables exemples de la première période de l'art et de l'architecture achéménide, et des témoignages exceptionnels de la civilisation perse. Les vestiges les plus dignes d'intérêt sur ce site de 160 ha sont notamment : le mausolée de Cyrus II , le Tall-e Takht, une terrasse fortifiée, et un ensemble royal composé de vestiges d'une porte, d'une salle d'audience, du palais résidentiel et du jardin. Pasargades fut la capitale du premier grand empire pluriculturel en Asie occidentale. S'étendant de la Méditerranée orientale et de l'Égypte à l'Indus, il est considéré comme le premier empire à avoir respecté la diversité culturelle des différents peuples qui le constituaient. En témoigne l'architecture achéménide, représentation synthétique de cultures diverses. (Site classé au patrimoine mondial de l'Unesco)

entre la langue écrite de cette troisième formule et certains dialectes sémitiques bien connus simplifia le déchiffrement.

Les inscriptions de Béhistun donnèrent la clef de l'énigme du cunéiforme babylonien, mais l'on sait à présent qu'il était déjà en usage plus de deux mille ans avant que ne fussent gravées ces inscriptions. De nombreux documents cunéiformes extrêmement anciens ont été découverts à Babylone, à Ninive et sur d'autres sites bordant l'Euphrate et le Tigre. Le cunéiforme babylonien est gravé sur des sceaux, sur des cylindres, sur des obélisques de pierre, sur des statues et sur les murs des palais. On le trouve écrit sur un grand nombre de tablettes d'argile de tailles variées : certaines ont un format de 22,8 cm par 15,2 cm, d'autres une surface dépassant à peine 2 cm^2. L'écriture est souvent minuscule. Certaines des plus petites tablettes ne comportent pas moins de six lignes et ne peuvent être lues qu'à la loupe.

Connaissance moderne de l'écriture cunéiforme

Il manquait une preuve indiscutable que l'écriture cunéiforme fût à l'origine constituée de pictogrammes, jusqu'à la découverte d'inscriptions primitives entièrement pictographiques. L'universitaire allemand Friedrich Delitzch, en 1897, fit valoir que l'écriture cunéiforme ne pouvait se composer à l'origine uniquement de pictogrammes, et soutint au contraire le fait que les pictogrammes s'étaient développés à partir d'un nombre relativement restreint de signes de base. Les combinaisons de ces signes de base, affirmait-il, avaient, au fil du temps, donné naissance à des centaines de signes cunéiformes. Sa théorie reçut un accueil mitigé, mais la majorité des chercheurs se rangèrent à cette théorie de l'origine pictographique. Le principe en fut définitivement établi en 1913 par l'orientaliste américain George Aaron Barton dans son livre *The Origin and Development of Babylonian Writing*, (*Origine et développement de l'écriture babylonienne*) qui présentait un ensemble de 288 pictogrammes trouvés dans les inscriptions cunéiformes les plus anciennes dont il reconstituait l'évolution. Selon Barton, les signes d'origine furent élaborés d'après le corps humain et ses différentes parties ainsi que d'après les mammifères, les oiseaux, les insectes, les poissons, les arbres, les étoiles et les nuages, la terre et l'eau, les bâtiments, les bateaux, le mobilier et les divers ustensiles domestiques, le feu, les armes, les vêtements, les objets de culte, les filets, les pièges, la poterie et les instruments de musique. Des fouilles conduites de 1928 à 1931 à Uruk, sur le site de l'actuelle Warka, en Irak, par des archéologues allemands, permirent de découvrir les plus anciens exemples connus de pictogrammes gravés sur des tablettes d'argile.



Exemples de déterminatifs cunéiformes

L'on doit, pour une grande part, à la traduction de l'écriture cunéiforme nos connaissances actuelles sur l'ancienne Assyrie et sur l'ancienne Babylone ainsi que sur le Moyen-Orient en général. Le code cunéiforme d'Hammourabi est l'un des documents les plus importants issus de toute l'Antiquité. D'autres tablettes cunéiformes ont permis d'éclairer l'histoire de l'Égypte ancienne. Un texte cunéiforme découvert en 1929 pendant les fouilles françaises de Ras Shamra, dans le nord de la Syrie, s'est révélé être un alphabet de consonnes ; on estime qu'il fut en usage à partir de 1400 à 1200 av. J.-C. Les textes mythologiques écrits dans ce qu'on a appelé l'alphabet cunéiforme de Ras Shamra nous renseignent sur de nombreux aspects de la vie religieuse du Moyen-Orient antique et ont pesé sur plusieurs réinterprétations de certains des aspects de la Bible.

Les hiéroglyphes

Les hiéroglyphes sont des caractères utilisés dans n'importe lequel des systèmes d'écriture comportant des caractères pictographiques, c'est-à-dire qui représentent des objets reconnaissables.

Les inscriptions hiéroglyphiques égyptiennes sont composées de deux types de signes de base : les idéogrammes (images représentant le sens du mot) et les phonogrammes (images représentant le ou les sons d'un mot).

Les Égyptiens utilisèrent les hiéroglyphes depuis l'époque du développement du système, vers 3200 av. J.-C., jusqu'à l'époque de l'Empire romain. La dernière inscription hiéroglyphique date de 394 apr. J.-C. La forme et le nombre des signes restèrent à peu près constants jusqu'à la période gréco-romaine (après 332 av. J.-C.), pendant laquelle le nombre de signes, en particulier celui des phonogrammes, augmenta beaucoup.

L'écriture pictographique hittite

Les Hittites[154], peuple indo-européen, utilisaient également un système pictographique, baptisé hiéroglyphique par analogie avec l'écriture égyptienne. Écrite en boustrophédon, c'est-à-dire que l'écriture se lisait de droite à gauche puis de gauche à droite comme un bœuf labourant son champ (du grec βοῦς, bœuf et στροφή, tourner), l'écriture pictographique cohabitait dans le royaume hittite avec le cunéiforme.

La collection de tablettes d'argile à écriture cunéiforme de Boghazköy (l'antique Hattousas) contient les seuls documents connus concernant la civilisation des Hittites, qui fondèrent au II^e^ millénaire avant notre ère l'une des plus puissantes organisations politiques du Moyen-Orient. La plupart de nos connaissances relatives à l'histoire de l'Asie Mineure et d'une partie du Moyen-Orient durant cette période nous viennent des tablettes à écriture cunéiforme découvertes à Boghazköy. Cette collection de presque 25.000 tablettes nous renseigne sur la vie sociale, politique et religieuse, sur l'activité commerciale, militaire, législative et artistique au II^e^ millénaire avant notre ère.

La collection comprend des tablettes où est inscrit le texte du traité de Qadesh, conclu entre les Hittites et les Égyptiens. Ce traité bien connu, dit de la « paix éternelle », garantissait la paix et la sécurité dans toute la région.

La collection comprend aussi de nombreuses œuvres littéraires, généralement de caractère épique et mythologique ; les principales racontent les exploits et les querelles des dieux, qui présentent en gros les mêmes traits essentiels que les dieux des autres peuples du Moyen-Orient.

Tout en étant liée à celle d'Akkad et de Sumer, la civilisation des Hittites a subi des influences égyptiennes et hourrites ; il semble, d'autre part, qu'elle ait elle-même influencé l'art égéen.

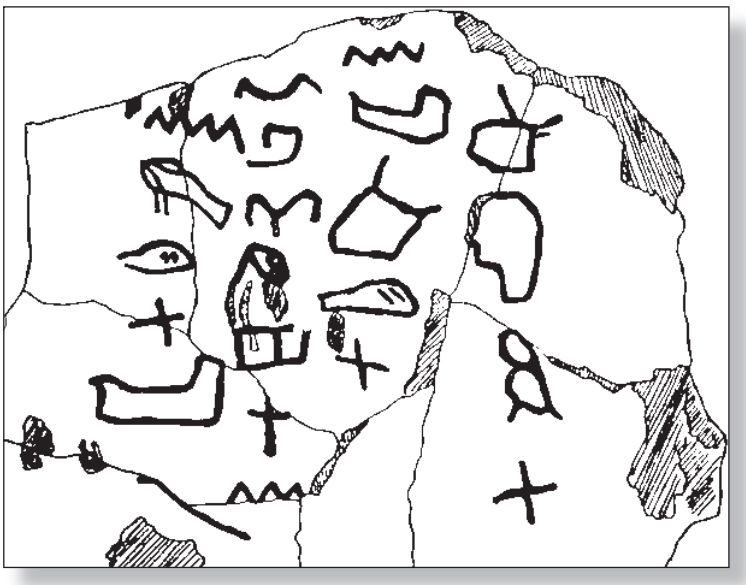
[154] Les Hittites ont été identifiés, au cours du XIX^e^ siècle par les archéologues, comme une confédération de peuples de langue indo-européenne – les Nésites, les Louvites, les Palaïtes, etc. – ayant établi un royaume en Anatolie centrale, vers 1750 avant J.-C. Dépourvu de frontières naturelles, ce royaume a dû batailler sans cesse pour conserver son cœur historique et s'emparer des riches et chaudes terres du Sud, avant d'être anéanti par les « Peuples de la Mer » vers 1180 avant J.-C. Dans sa plus grande extension, la civilisation hittite atteignit l'Euphrate moyen, à l'est, la côte méditerranéenne face à Chypre au sud, mais resta coupée de la mer Noire et de la mer Egée.

Les écritures crétoises

En Crète, existait une écriture essentiellement phonétique dans laquelle les signes isolés avaient une valeur syllabique. Constitué d'une centaine de signes, aujourd'hui non encore tous déchiffrés, le *linéaire A*[155] (XVII[e] siècle av. J-C.) et le *linéaire B*[156] ci-contre (XIV[e] siècle av. J-C.) étaient utilisés dans les îles de la mer Égée.

Les proto-alphabets cananéens

Vers 1800 av. J-C. apparurent dans le Sinaï central et à Byblos des signes pseudo-hiéroglyphiques, transcrivant un dialecte cananéen, mais sous une forme non spécifiquement alphabétique. Des tablettes retrouvées à Byblos, suggère l'existence d'une écriture essentiellement syllabique, car ne comportant guère plus de 120 signes, baptisés « pseudo-hiéroglyphes » représentant des animaux, des végétaux, des bâtiments et des dessins géométriques. S'inspirant davantage de l'écriture crétoise que de l'écriture égyptienne, ce système scriptural fut en usage jusqu'à la fin du XIII[e] siècle av. J-C., c'est à dire jusqu'à l'affirmation de l'alphabet phénicien.



En Canaan, occupée par les Égyptiens, naquit vers le XV[e] siècle avant notre ère, une écriture qui prit le nom de proto-sinaïtique[157], car on découvrit ses plus beaux spécimens dans des mines de turquoise égyptienne du désert du Sinaï. Son origine est à rechercher du côté de l'Égypte. L'écriture hiéroglyphique comprenait en effet vingt-cinq signes mono-consonnantiques différents qui associés constituaient un alphabet complet. Mais les Égyptiens, trop conservateurs, ne l'utilisèrent jamais comme tel. L'écriture inventée par les scribes cananéens, isolait ces signes et leur attribuait une valeur phonétique représentée plus ou moins schématiquement par ces signes. Elle constitue la première expérience probante de simplification alphabétique de l'écriture. Toutefois, son destin nous est encore aujourd'hui inconnu.

Les idéogrammes chinois

Comme d'autres écritures anciennes, le chinois écrit provient d'une symbolisation picturale. Il n'a évolué vers une représentation mot à mot de la langue que lorsque ses utilisateurs comprirent que certains termes trop abstraits pouvaient être indiqués par leur son, plutôt que par leur sens.

[155] Le linéaire A est une écriture qui fut utilisée dans la Crète ancienne. On suppose qu'il transcrit le langage des Minoens. C'est Arthur Evans qui découvrit en Crète les vestiges de cette écriture, ainsi que d'autre écritures anciennes.

[156] Le linéaire B apparaît en Crète à Cnossos aux environs de 1375 avant J.-C. Il y a été découvert, avec le linéaire A, en 1900 par Sir Arthur Evans sur des tablettes d'argile cuites accidentellement par un incendie. Des tablettes ont également été retrouvées à Pylos, Mycènes, Thèbes et Tirynthe. Le linéaire B se trouve également sur des vases trouvés à Éleusis, Kreusis, Orchomène, Chania et au Ménélaion, à Thérapné. Les styles d'écriture permettent d'identifier une centaine de scribes différents à Cnossos, et une cinquantaine à Pylos.

[157] Moïse aurait-il connu le proto-sinaïtique ou un développement de celui-ci ? Aurait-il employé cette écriture alphabétique pour la Torah comme l'affirme la tradition ?

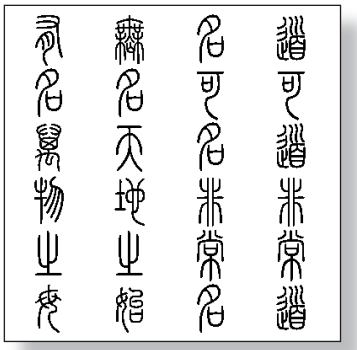
Toutefois, à l'inverse des autres systèmes d'écriture, qui ont tous évolué vers une représentation alphabétique – c'est-à-dire essentiellement phonétique – des mots, le chinois fonctionne encore autant de manière pictographique que phonétique.

En outre, la représentation des sons n'a pas suivi l'évolution de la langue parlée, et reflète toujours la prononciation d'il y a trois mille ans.

La langue chinoise écrite attribue un symbole ou un caractère distinctif unique pour chaque mot de vocabulaire. La connaissance de deux mille ou trois mille caractères est nécessaire à sa lecture.

Les écrits les plus anciens que l'on connaisse sont des oracles gravés sur des carapaces de tortue et des omoplates de bœuf, dus à des devins de cour de la dynastie des Shang, à partir du XIVe siècle av. J.-C.

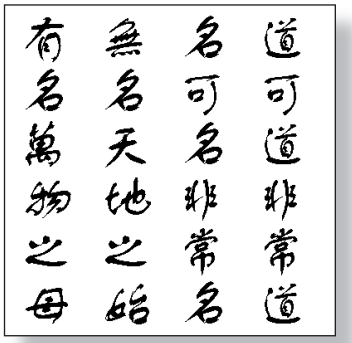
On trouve également en chinois des pictogrammes à valeur phonétique, c'est-à-dire l'emprunt du pictogramme d'un mot concret pour indiquer un mot abstrait ayant une prononciation identique ou très proche.



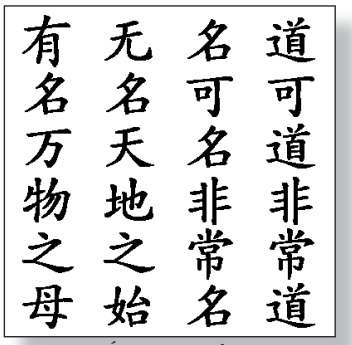
Petit Sceau

Qin Shi Huangdi, premier souverain d'un empire chinois unifié, supprima de nombreuses transcriptions régionales pour imposer une écriture simplifiée et standardisée, appelée le « Petit Sceau ». Sous la dynastie Han (206 av. J.-C.-220 apr. J.-C.), le système se ramifia en divers styles : lishu, écriture des fonctionnaires, xingshu, écriture cursive, caoshu, écriture de brouillon, et kaishu, écriture régulière. Le chinois imprimé se conforme à l'écriture régulière. Les styles cursif et régulier ont introduit de nombreux caractères abrégés, employés aussi bien dans la calligraphie artistique que dans la correspondance commerciale ou privée, mais furent longtemps bannis des documents officiels. Devenue la norme en République populaire de Chine, l'impression des caractères abrégés reste proscrite à Taïwan.

Écriture des fonctionnaires



Écriture cursive



Écriture régulière

L'écriture hiéroglyphique des Mayas

Les Mayas écrivaient sur du papier fabriqué à partir de fibres végétales et utilisaient des pigments naturels pour l'encre ; ils gravaient également sur des stèles en pierre. Des codes de lois et des calendriers nous sont ainsi parvenus. L'écriture maya utilise à la fois des idéogrammes et des phonogrammes.

Les peuples mayas créèrent un système d'écriture hiéroglyphique pour consigner leur mythologie, leur histoire et leurs rites sous forme d'inscriptions sculptées et peintes sur des stèles, des linteaux et des escaliers, ou peintes dans des livres formés de feuilles de papier en fibres végétales recouvertes d'une pellicule de chaux. Quatre de ces manuscrits nous sont parvenus : le codex[158] Dresdensis, conservé à Dresde,

[158] Ensemble de feuilles de parchemin reliées pour former un livre. Par extension : manuscrit ancien se présentant sous cette forme. Le codex est l'ancêtre du livre.

le Peresianus, à Paris, le Tro et le Cortesianus, à Madrid. Ces livres, utilisés comme calendriers divinatoires, traitaient de thèmes comme l'agriculture, le temps, la maladie, la chasse et l'astronomie.

Le maya (également appelé yucatèque), la langue propre des Mayas, est parlé par environ 350 000 personnes dans le Yucatán, le nord du Guatemala et au Belize. Les autres langues de la famille linguistique maya sont au nombre de vingt-trois. Malgré cette persistance linguistique, moins de la moitié des 400 signes hiéroglyphiques répertoriés ont été déchiffrés : nombres et noms des jours, des mois, des dieux.

Le Codex de Dresde

Le plus vieux document chiffré

Le premier document chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, retrouvée en Irak, et datant du XVI[e] siècle av. J.-C. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots. Le texte qui y est gravé est codé. Il a été inscrit sur cette tablette par ce potier babylonien qui voulait dissimuler la recette de son succès. Après avoir rajouté quelques consonnes et reconnu les mots à l'orthographe fantaisiste, les archéologues ont réussi à déchif-

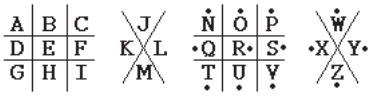
frer la formule de fabrication d'un vernis dont le potier gardait jalousement l'exclusivité. L'histoire ne dit pas si la ruse fut efficace.

Les écritures codées

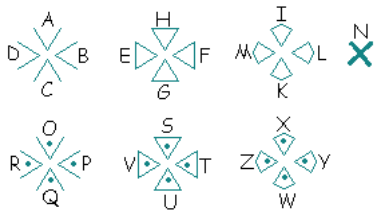
L'Histoire et la littérature regorgent de systèmes de codages d'écriture utilisant des signes convenus entre les correspondants et étant sensés déjouer la curiosité de ceux qui n'ont pas à connaître le contenu des messages échangés. Nous allons en citer quelques exemples.

Le chiffre des Templiers

Plutôt que de remplacer chaque lettre par une autre, certains (essentiellement des membres de société plus ou moins secrète) ont préféré remplacer les lettres par des symboles pour diffuser leurs messages codés. C'est ainsi qu'ont procédé les francs-maçons au XIX[e] siècle avec le chiffre de PigPen.



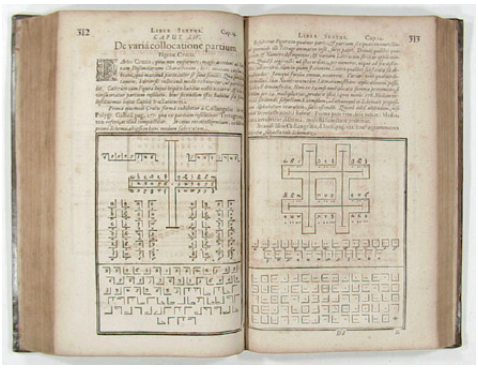
Le Temple était un ordre de moines fondé au XII[e] siècle, dont la mission première était d'assurer la sécurité des pèlerins en Terre sainte. Rapidement, les Templiers se détournèrent de cet objet, et s'enrichirent considérablement au point de devenir les trésoriers du roi et du Pape. Pour coder les lettres de crédit qu'ils s'échangeaient, ils remplaçaient chaque lettre par un symbole, suivant la substitution suivante :



Par exemple, si nous souhaitons coder : CODE DES TEMPLIERS, on obtient :

À part la difficulté liée au fait qu'on manipule des symboles peu courants, facilement surmontée par un petit temps d'adaptation, le chiffre des Templiers ne peut être considéré comme plus sûr que n'importe quel code par substitution.

On trouve aussi des descriptions de chiffres du type Pig Pen dans le traité de Gustavus Selenus *Cryptomenytices et Cryptographiae, Libri IX*, 1624

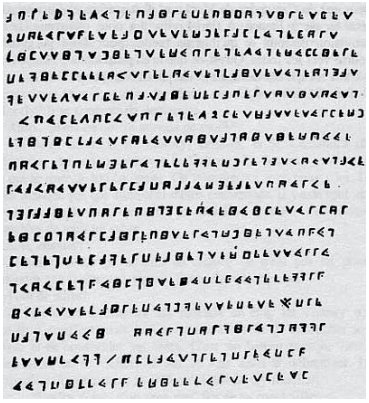


Cryptogramme du Forban.

Avant d'être pendu à St-Paul, le pirate La Buse[159] lança ce message chiffré dans la foule en criant : « mes trésors à qui saura comprendre ! »

Même traduit, ce texte reste hermétique et le trésor n'a toujours pas été retrouvé..

[159] Olivier Levasseur, dit la Buse , est né à CALAIS vers 1680. Fils de flibustier, son père le prit à bord de la Reine des Indes et lui enseigna les bases de la navigation. À cette époque, maîtriser les océans c'est maîtriser le monde. Maîtriser les bateaux

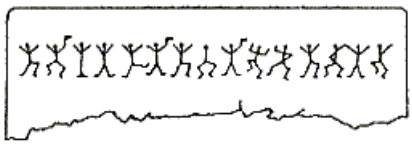


La Buse, pirate célèbre écuma l'océan Indien au début du 18ème siècle. Il aurait caché un trésor estimé à 4,5 milliards d'euros quelque part à La Réunion. Aujourd'hui encore, des chercheurs et des scientifiques se lancent à la recherche de ce trésor précieusement conservé depuis plus de 280 ans.

Littéralement, on peut lire :
«aprè jmez une paire de pijon tiresket
2 doeurs sqeseaj tête cheral funekort
filttinshientecu prenez une cullière
de mielle ef ovtre fous en faites une ongat
mettez sur ke patai de la pertotitousn
vpulezolvs prenez 2 let cassé sur le che
min il faut qoe ut toit a noitie couue
povr en pecger une femme dhrengt vous n ave
eua vous serer la dobaucfea et pour ve
ngraai et por epingle oueiuileturlor
eiljn our la ire piter un chien tupqun
lenen de la mer de bien tecjeet sur ru
nvovl en quilnise iudf kuue femm rq
i veut se faire dun hmetsedete s/u dre
dans duui ooun dormir un homm r
esscfvmm / pl faut n rendre udlq
u un diffur qecieefurtetlesl

Si l'on essaye de déchiffrer ce texte, on peut lire :
«Prenez une paire de pijon, virez
les 2 coeurs...tête de cheval... une kort
fil winshient écu prenez une cuillière
de mielle... outre vous en faites une ongat
mettez sur le passage de la...
...Prenez 2 liv cassé sur le chemin
Il faut... toit à moitié couvé
pour empêcher une femme... vous n'avez
qu'à vous serrer la... pour veni
... épingle ...juillet...
.. faire piter un chien turc un
... de la mer... bien sécher et sur
... qu'une femme qui
veut se faire d'un...
dans... dormir un homme
... faut en rendre...
qu'un diffur...»

Dans *les Hommes dansants*, nouvelle de Sir Arthur Conan Doyle, Mr Hilton Cubitt rapporte à Sherlock Holmes des feuilles de papier sur lesquelles sont dessinés des petits hommes qui miment des pas de danse. Ceci pourrait passer pour de petits dessins d'enfant (comme le pense Watson), mais Mr Hilton Cubitt est inquiet, car sa femme semble très préoccupée depuis que ces dessins apparaissent sur les appuis de fenêtre ou sur des feuilles de papier abandonnées dans le jardin.



Le manuscrit de Voynich

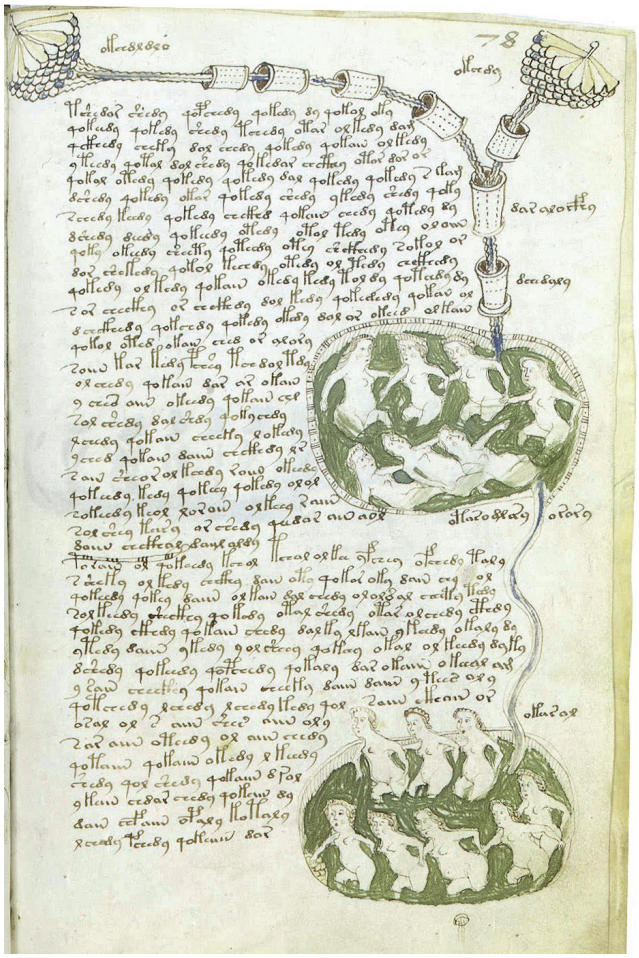
Le texte comprend plus de 170 000 glyphes, normalement séparés les uns des autres par de fins interstices. La plupart de ces glyphes sont écrits avec un ou deux traits. Les experts restent divisés concernant l'alphabet utilisé, car certains des glyphes sont similaires. On pense toutefois que l'alphabet du manuscrit

espagnols, portugais et anglais c'est maîtriser les routes et les flibustiers en profitaient pour arraisonner le maximum de navires pour se renflouer en biens, tout en s'imposant comme autorité.

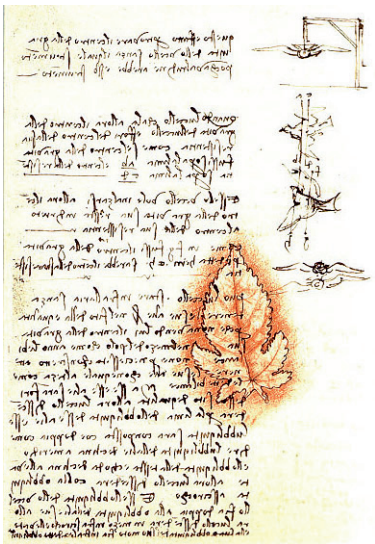
de Voynich comprend entre 20 et 30 signes. Certains caractères inhabituels apparaissent ici et là, on en dénombre une douzaine de ce type.

Des espacements plus larges divisent le texte en 35 000 mots environ, de taille variable. Il semble que le texte suit des règles phonétiques ou orthographiques : certains caractères doivent apparaître dans chaque mot (à l'instar des voyelles en français), certains caractères n'en suivent jamais d'autres ; d'autres peuvent apparaître en double.

Sur d'autres points, le langage du manuscrit de Voynich diffère sensiblement des langues européennes. Par exemple, il n'y a pratiquement aucun mot avec plus de 10 symboles, et presque aucun mot de moins de trois lettres. Les distributions des lettres à l'intérieur d'un mot sont étranges : certains caractères n'apparaissent qu'au début d'un mot, d'autres seulement à la fin et une partie n'apparaît qu'au centre du mot. Une telle disposition se retrouve dans l'alphabet arabe, mais pas dans l'alphabet cyrillique, grec ou encore latin.



Comme l'alphabet du manuscrit ne ressemble à aucun autre et que le texte est toujours indéchiffrable, les seuls signes reflétant son ancienneté et son origine sont les illustrations, spécialement les robes et les coiffures des personnages, ainsi que deux châteaux apparaissant dans les schémas. Ils sont caractéristiques du style européen et, se basant sur ce fait, les experts datent le livre sur une période comprise entre 1450 et 1520. Cette évaluation est confortée par des indices complémentaires.



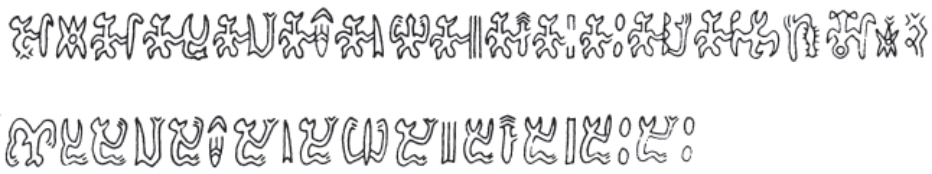
Pour tenir ses écrits à l'abri des regards indiscrets, Léonard de Vinci avait l'habitude d'écrire de droite à gauche, si bien qu'il fallait un miroir pour lire ses manuscrits. Évidemment, ce procédé n'offre qu'une très faible protection, mais à son époque c'était assez efficace, puisque peu de gens savaient lire.

Vous voyez ci-contre une illustration de Rudyard Kipling pour « *The first letter* », une des histoires de son célèbre livre pour enfants « *Just So Stories* ».

Cette image montre une défense en ivoire sur laquelle sont gravés des dessins racontant l'histoire d'une jeune fille nommée Taffimai. Kipling dit que les étranges symboles sur les côtés sont des lettres runiques magiques, mais il s'agit en fait d'un alphabet de substitution.

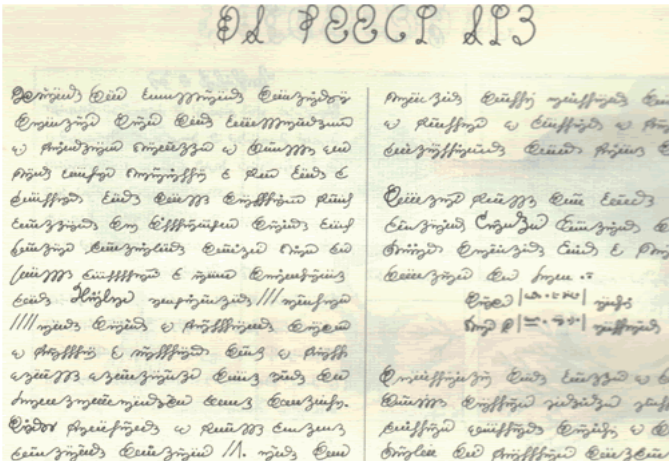
Autres écritures secrètes ou indéchiffrables, langues inconnues

Le Rongo-Rongo (« récitation, message ou grande étude » en langue Rapa Nui) est l'écriture sur tablettes de bois ou bâtons, découverte sur l'Île de Pâques en 1864 par le Frère Eugene Heyraud. Les objets rongo-rongo n'ont pas été déchiffrés à ce jour (2007). La séquence d'écriture se présente sous forme de lignes boustrophédon inversées ce qui nécessite une rotation de la tablette à chaque changement de ligne. Les Pascuans avaient perdu les neuf-dixièmes des données sur leur propre écriture et un chercheur français, Lorena Bettocchi, avec l'aide des Musées et d'institutions françaises et chiliennes, met tout en œuvre pour leur rendre ce qui leur est dû (Loi de protection des cultures indigènes ONU) et le retour de toutes les images, photographies et épigraphie aux propriétaires de cette écriture.



L'étude de ces 26 tablettes dispersées à travers le monde depuis la fin du XIX[e] siècle, connaît un développement récent, qui donnerait plusieurs sens possibles aux signes. Une autre théorie se base sur le type d'écriture. Certains peuples qui ont créé leur écriture ont inventé un alpha-syllabaire (Cherokee, Vai, Afaka...) : un symbole représente un son.

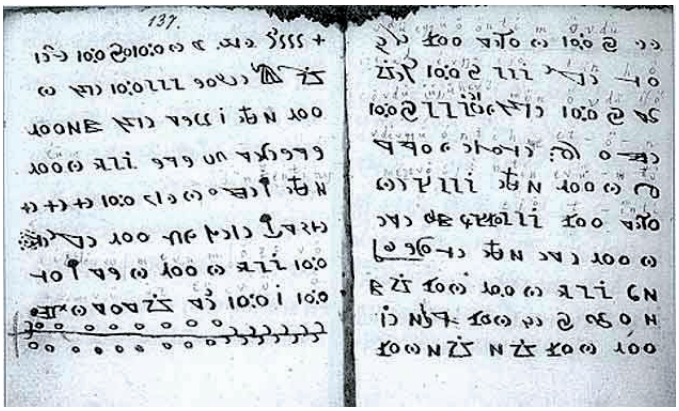
Codex Seraphismus



Luigi Serafini est né à Rome en 1949. C'est en 1970 qu'il commence d'une part un tour du monde, et d'autre part se lance dans l'architecture.

Entre 1976 et 1978, il écrit seul, dans un appartement romain, sans commande d'aucune sorte un livre, le Codex Seraphinianus, qu'il livre à l'éditeur d'art milanais Franco Maria Ricci en 1981. Le Codex en est à sa sixième édition. Il est écrit dans une langue inventée dont on ne sait si elle a un sens. Elle semble plus graphique que sémantique.

Codex Rohonczi

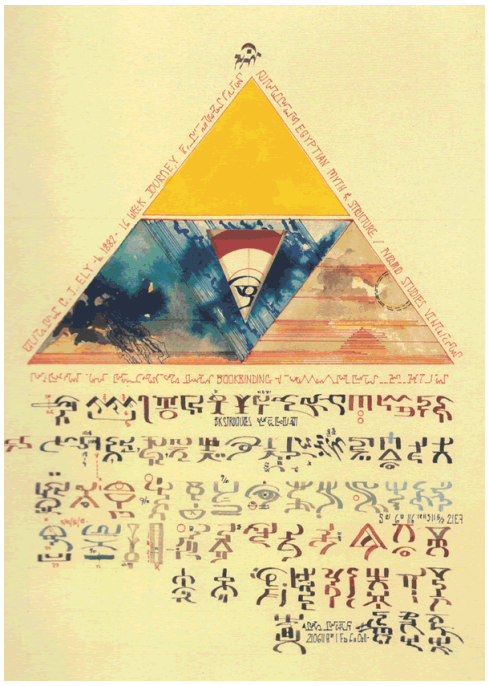


L'origine du codex est incertaine. Il a été donné à la « *Hungarian Science Academy* » par Batthyany Gutsztav, un noble hongrois, avec l'intégralité de sa bibliothèque. Il a été cité proche de la ville de Rohoncz, dans l'ouest de la Hongrie, où il a été gardé jusqu'en 1907, précédent son transfert à Budapest. Cette même année, il a été mentionné dans un travail de Bela Toth : « Rare Hungarian Writings ». Le codex a été envoyé à un chercheur autrichien, Bernhard Jülg, professeur à l'Université d'Innsbruck, mais il échoua et affirma que ce codex

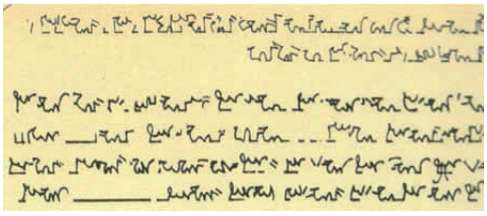
n'avait pas de sens. Le codex a 448 pages de papier (12x10cm), chacune ayant entre 9 et 14 rangées de lettres. À côté du texte, se trouvent 87 illustrations qui sont d'apparence religieuse, laïque et militaire. Les illustrations de la croix semblent indiquer un environnement où le christianisme, le paganisme et même la religion musulmane coexistaient, alors que les symboles de la croix, de la demi-lune et du soleil et de la croix svastika sont omniprésentes.

Les nombreux symboles du Codex sont environ 10 fois plus élevés que dans n'importe quel alphabet connu, alors que quelques lettres ne sont rarement qu'utilisées, et ils pourraient alors représenter des pictogrammes au lieu de lettres. L'étude du papier sur lequel il est écrit montre que le papier semble vénitien, fait dans les années 1540. Cependant, il a pu être simplement retranscrit d'une source plus ancienne. Le langage dans lequel il est écrit est inconnu bien qu'il ait été proposé comme hongrois, dacien, roumain ou cumain... mais rien n'indique de quelle langue il s'agit vraiment.

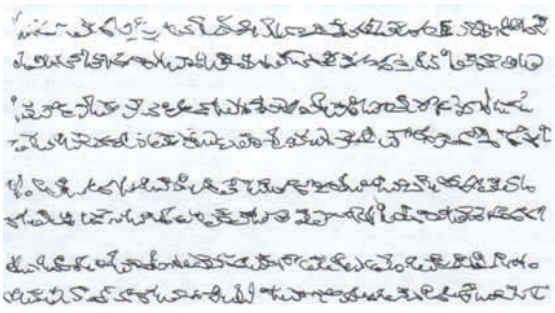
Écriture de Timothy C. Ely



Timothy C. Ely[150] avoue que pendant 25 ans il a fait des lettres telles qu'on peut les voir dans son livre, et qu'être gaucher l'a conduit à écrire de gauche à droite pour éviter les taches d'encre. En commençant à écrire dans le sens inverse, son écriture se révéla proche des alphabets asiatiques ou du Moyen-Orient, et ce qui lui plut fut que ça ressemblait à des écritures codées. Il continue « ça me semblait mystérieux, et j'aimais l'idée de remplir des pages avec une sorte de métapoésie ou de métaphysique. Les langages n'ont pas à être verbaux ou visuels. Ils peuvent être une sensation, ou dans la forme dont ils se représentent ». Il poursuit : « Les caractères parfois sont assignés à une couleur émotionnelle ou à une note musicale. Il y a beaucoup de bruit de fond (= entropie) dans ces caractères, et c'est crucial pour le livre ».



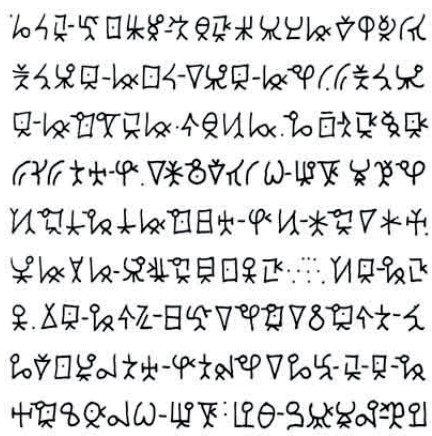
Ce qui au premier abord dans l'écriture nous semblait construit et organisé, est bien une suite de caractères calligraphiés avec spontanéité et limpidité, mais un ordre de formation quelconque ne révélant aucun sens si quelqu'un se prêtait à tenter le déchiffrement de l'écriture.



Andersch Martin, Allemagne. En 1988, après plus de 20 ans d'enseignement de la calligraphie, propose dans une méthode ludique et expérimentale une écriture rythmique, sans contenu sémantique, se transformant jusqu'à presque devenir des images abstraites. Ce qui est intéressant est le tracé et la constance des caractères : le tracé est régulier, mais saccadé, comme si l'écriture se cherchait au fur et à mesure qu'elle est couchée sur le papier. La constance dans l'écriture est ici absente : de très

[150] Peintre américain né en 1949.

nombreux caractères dont il nous serait pas ou peu possible d'en tirer un alphabet, quel que soit d'ailleurs le nombre de lettres de cet alphabet.



Le Linéaire « Z » a été ingénieusement créé de toutes pièces par Olivier Monné , en hommage au disque de Phaistos, aux Linéaires A et B des Crétois, et avec l'aide complice de... Corinne. Cette écriture, cohérente et rigoureuse, peut à la fois avoir été inventée dans un objectif de crypter des messages, et dans un souci de création graphique à part entière. Il est très probable que cette écriture ne puisse être déchiffrée qu'après de réels efforts, et peut être même de vains efforts pour celui qui n'aurait pas la clef d'entrée. En espérant que son travail détaillé d'abord dans un premier livret soit le début d'une œuvre littéraire complète, originale et artistique.

Le disque de Phaïtos

En1908, dans la plaine crétoise de la Messara, une équipe d'archéologues italiens exhume au milieu des ruines millénaires du palais de Phaïstos un disque d'argile recouvert sur ses deux faces de pictogrammes inconnus. Sa découverte attise rapidement l'intérêt du public et on parle déjà du nouveau Champollion qui déchiffrerait le contenu de ce que l'on considère alors comme un texte porteur de sens ; s'en suit naturellement un grand nombre d'études aboutissant pour la plupart à des traductions intégrales peu convaincantes. Voilà maintenant près d'un siècle que le Disque de Phaïstos résiste aux attaques d'une recherche presque essoufflée attendant avec impatience la relève d'une nouvelle génération.

L'art du message secret

La cryptographie est l'étude des messages secrets. Le terme *cryptographie* vient en effet des mots grecs anciens : *kruptos* (κρυπτος) qu'on peut traduire comme *secret* ou caché, et *graphein* (γραφην) pour écriture. Plus précisément, la cryptographie est l'étude des codes secrets, et non celle des messages simplement voilés (comme avec de l'encre invisible, par exemple). Les origines de la cryptographie semblent remonter à plus de 4000 ans. On a trouvé, sur une tombe égyptienne de cette époque, des inscriptions contenant des hiéroglyphes modifiés, et il semblerait qu'on ait cherché par ces modifications à obscurcir le sens des inscriptions. Quoi qu'il en soit, plusieurs indications archéologiques tendent à montrer que les écritures secrètes sont en fait aussi anciennes que l'invention de l'écriture elle-même comme nous l'avons vu précédemment.

Deux grandes tendances visent à protéger l'information :

– 1 ***la stéganographie*** qui cherche plutôt à dissimuler la présence d'informations pertinentes au sein de plusieurs autres sans intérêt pour le destinataire du message : le message secret est caché dans un support de manière à passer inaperçu lors de la communication.

– 2 ***le chiffrement***, dont l'objectif est de rendre l'information incompréhensible à une personne ne possédant pas les connaissances adéquates, par exemple une personne surveillant le canal de communication par lequel transite le message sait qu'un échange a lieu, mais est ainsi incapable d'en interpréter le contenu.

L'opération de chiffrement transforme un texte *clair* en un texte *chiffré*, appelé cryptogramme, au moyen d'une clé (qu'on dénomme la clé de chiffrement). Le déchiffrement est le traitement des données qui transforme le texte chiffré en texte en clair. La cryptographie est la science qui consiste à créer de tels systèmes de chiffrement. La *cryptanalyse* est la science complémentaire qui consiste à déterminer certaines propriétés de ces systèmes dans le but de reconstituer le texte en clair, souvent en l'absence des paramètres qui sont nécessaires pour le déchiffrement.

La *cryptologie* englobe la cryptographie et la cryptanalyse. Le chiffrement est généralement accompli avec un algorithme bien défini et une clé. Ceci s'applique aussi au déchiffrement bien que les algorithmes ne soient pas nécessairement les mêmes pour ces deux étapes.

La Stéganographie

Ce dessin contient un message codé en Morse. L'avez-vous découvert ?

La Stéganographie : un texte peut en cacher un autre...

On peut définir la stéganographie comme étant l'art de cacher des messages et de rendre leur présence insoupçonnable.

S'agissant des procédés de masquage tendant à rendre les messages invisibles, nous traiterons des méthodes par génération de support, méthode consistant à construire un support autour du message à dissimuler.

Nous nous intéresserons également à la stéganographie dans les textes, car nombre de ces astuces de masquage de texte dans le texte (les textes produits peuvent ensuite être cryptés ou chiffrées par tout autre procédé classique). Acrostiche, contrepèterie, jeux de césure, saut de mot ou de lettre, les procédés sont multiples et la littérature regorge de textes à double lecture.

La stéganographie apparaît dès l'Antiquité. Ainsi, Hérodote (484-445 av. J.-C.) raconte qu'Histiée envoya à Aristagoras de Millet un esclave porteur d'un message sans importance, puis, plus tard l'indication qu'il fallait lui raser la tête. Sur le crâne tatoué de l'esclave apparut alors le message indiquant que l'heure était venue de la révolte contre les Perses. Cette méthode ne s'applique pas aux cas d'urgence... puisqu'il faut attendre que les cheveux du porteur de message aient suffisamment repoussé avant de l'envoyer à travers les lignes ennemies !

Dans son *Enquête*, l'historien grec Hérodote rapporte ainsi une anecdote qui eut lieu au moment de la Seconde Guerre médique. En 484 avant l'ère chrétienne, Xerxès, fils de Darius, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce (Livre VII, 5-19). Quatre ans plus tard, lorsqu'il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décide de transmettre l'information à Sparte (Livre VII, 239) : « *Il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi, le porteur d'une tablette vierge ne risquait pas d'ennuis* ».

Un autre procédé, utilisé dès le VI[e] siècle av. J.-C. est la scytale, technique assyrienne révélée par Plutarque. Elle consistait à écrire le message sur une bandelette enroulée autour d'un bâton. La bande déroulée, le texte n'était plus qu'une suite de lettres ou de mots sans suite. Le destinataire possédait un bâton de même diamètre sur lequel il lui suffisait d'enrouler la bande pour lire le texte.

Dès le I[er] siècle av. J.-C., Pline l'Ancien décrit comment réaliser de l'encre invisible (ou « *encre sympathique* »). L'encre sympathique est la plus connue des méthodes de stéganographie. L'utilisation du jus de citron, ou du lait comme encre rend le message invisible, dissimulé sous un message écrit à l'encre ordinaire sur la même feuille. Les Allemands, pendant la dernière guerre mondiale, utilisèrent une variante de ce procédé : ils cochaient les lettres d'un journal avec une encre invisible spécifique qui ne réagissait qu'avec un produit chimique particulier.

L'historien de la Grèce Antique Enée le Tacticien imagina d'envoyer un message secret en piquant de minuscules trous sous certaines lettres d'un texte anodin. La succession de ces lettres fournit le texte secret. Deux mille ans plus tard, les épistoliers anglais employèrent la même méthode, non pour assurer le secret à leurs envois, mais pour éviter de payer des taxes excessives. En effet, avant la réforme du service postal, dans les années 1850, envoyer une lettre coûtait environ un shilling tous les cent miles, ce qui

était hors de portée de la plupart des gens, mais les journaux ne payaient pas de taxe. Grâce aux piqûres d'épingle, les Anglais malins pouvaient envoyer leurs messages gratuitement.

Au XVI[e] siècle, le scientifique italien Giovanni Porta découvrit comment cacher un message dans un œuf dur : il suffit d'écrire sur la coquille avec une encre contenant une once d'alun pour une pinte de vinaigre ; la solution pénètre la coquille et dépose sur la surface du blanc d'œuf le message que l'on lira aisément après avoir épluché l'œuf.

À la même époque, une nouvelle méthode de stéganographie fut introduite par les services secrets allemands : le micropoint de Zapp, qui, utilisé comme ponctuation banale dans un texte quelconque contient des informations que seul un fort grossissement peut révéler. Il ne fut repéré par le F.B.I. qu'en 1941, ce qui permit ensuite de démanteler plusieurs réseaux d'espionnage. Le microfilm caché sous le timbre d'une enveloppe est aussi une belle idée de stéganographie chère à l'espionnage moderne.

Plus récemment, des chercheurs américains ont réussi à utiliser l'ADN pour transmettre des messages secrets.

L'ADN pourrait bientôt faire partie de la panoplie du parfait espion. Des chercheurs de la *Mount Sinaï School of Medicine*, à New York, viennent de créer des micropoints dans lesquels a été caché un message à base d'ADN. Perdu au milieu d'un génome plus important, il serait alors particulièrement difficile à déceler.

Catherine Taylor Clelland, Viviana Risca et Carter Bancroft du département de *Physiologie et Biophysique de la MSSM* ont franchi un nouveau pas dans l'utilisation de cette technique. Ils ont imaginé un message codé par une séquence de nucléotides, chaque triplet de bases désignant une lettre de l'alphabet. Flanqué d'une amorce connue seulement du destinataire, ce morceau d'ADN pourrait ensuite être amplifié par PCR puis séquencé afin d'être décrypté. Pour corser le tout, les trois chercheurs ont proposé de mélanger le message codé à de l'ADN dénaturé. Contenant près de trois milliards de paires de nucléotides, le génome humain constitue le parfait camouflage. Car même si un ennemi quelconque repérait le micropoint, il lui serait virtuellement impossible de lire le message sans connaître l'amorce utilisée pour l'amplification. Si cette dernière comprenait vingt bases aléatoires, il lui faudrait en effet réaliser puis analyser quelque 1020 PCR différentes. Enfin, il serait également possible de créer des « diversions » à l'aide de génomes non humains.

Afin d'étudier la faisabilité de leur théorie, les trois chercheurs américains ont créé un message secret en synthétisant un brin d'ADN de 69 nucléotides flanqué de deux amorces de PCR de 20 nucléotides. Mélangée en quantités variables à de l'ADN humain dénaturé, la séquence a ensuite été placée sur un point imprimé sur du papier filtre.

« Les amorces ont été conçues pour amplifier le message secret directement sur le micropoint sans solubilisation préalable, indiquent les auteurs des travaux. Le produit peut alors être analysé par électrophorèse. » Les expériences réalisées sur le message de 69 nucléotides ont montré que l'amplification était nécessaire et qu'il existait une limite de détection d'une copie par génome haploïde. « Après avoir choisi puis séquencé la bande amplifiée la plus claire, nous avons utilisé la clé de décryptage, ajoutent les trois chercheurs. Nous avons alors obtenu le texte initialement codé – *June 6 invasion : Normandy.* » Selon leurs premiers tests, les micropoints contenant 100 copies par génome haploïde du message collé sur des lettres puis envoyé par courrier dans tous les États-Unis ont pu être décodés facilement. Preuve que l'ADN pourrait maintenant servir aux James Bond de la planète.

La crainte que des espions infiltrés ne communiquent par stéganographie des informations stratégiques importantes a amené des situations cocasses. Peu après Pearl Harbor, les États-Unis mirent sur pied un service de censure de plus de 10 000 personnes chargé de repérer et d'intercepter tous les messages suspects. Les parties d'échec internationales étaient interdites, car on craignait que la liste des coups d'une partie ne masque une information utile à l'ennemi. Les timbres pour réponse contenus dans les

enveloppes étaient échangés contre d'autres de même valeur, de peur qu'ils ne signifient quelque chose de convenu. Les dessins d'enfants joints aux lettres pour grands parents attendris étaient confisqués, car la censure pensait qu'une carte ou une information militaire importante pouvait s'y dissimuler. Seuls les textes clairs en anglais, français, espagnol ou portugais étaient autorisés.

L'office de censure décida aussi que les demandes de diffusion de disques formulées par lettre ou appels téléphoniques aux stations de radio locales ne seraient satisfaites qu'avec un délai variable, ainsi que les annonces concernant les chiens perdus. Cette consigne devait empêcher la diffusion de messages codés destinés aux U-boats allemands.

On connaît les « messages personnels » diffusés par la B.B.C. pendant la dernière guerre et le fameux « *les sanglots longs des violons...* » signal du débarquement.

Cette stéganographie où le message est présent dans les symboles du message anodin est la plus intéressante. Elle s'apparente à la stéganographie pure, car le message anodin, même recopié, contient toujours le message secret.

Le langage convenu est la plus élémentaire des stéganographies pures. Au XIV^e^ siècle, la papauté utilisait un tel code où, par exemple, *Égyptien* signifiait *Gibelin* et où les *enfants d'Israël* désignaient les *Guelfes*[160]. Ce genre de convention est utilisé dans les argots professionnels, où des doubles sens ne sont compris que des initiés. Les démonstrations de « télépathie spectacle » font un usage intensif d'un langage convenu, les partenaires de ce type de numéro se transmettant toutes les informations nécessaires à la réussite de leur tour.

Un langage convenu permet un codage quasi indétectable. Un exemple célèbre est le code de Jean Trithème[161] qui transforme un texte en une litanie, certes obscure, mais tout à fait crédible (pour peu qu'on y ajoute ici et là quelques mots de liaison et qu'on place l'ensemble dans un contexte mystico-religieux). Ce simple texte : « Ces Dieux qui dans Pharsale ont mal servi Pompée... » signé Corneille, en utilisant le code suivant :

A = dans les cieux
B = à tout jamais
C = un monde sans fin
D = en une infinité
E = à perpétuité
F = sempiternel
G = durable
H = sans cesse
IJ = irrévocablement
K = éternellement
L = dans la gloire

[160] Les Guelfes et les Gibelins qualifient les factions qui soutiennent la papauté ou le Saint Empire romain germanique et qui s'affrontent en Italie.

[161] L'abbé Jean Trithème est né à Trittenheim, dans le diocèse de Trèves, le 1^er^ février 1462, et il mourut le 26 décembre 1516. Il est considéré comme un des pères de la cryptographie. Il fut un moine célèbre de l'ordre Bénédictin, et fut successivement abbé de Spanheim et abbé de Saint-Jacques le Majeur, Herbipolis, (i.e. Wurtzburg, en Bavière, le siège d'une université). Un très intéressant exposé de sa vie, avec des observations au sujet de son œuvre, se trouve dans la *Biographie Universelle*. Ses écrits quelque peu volumineux sont d'ordre théologiques, biographiques et historiques, et dans sa vie en latin il est dit qu'il prétendit à la révélation. Une copie manuscrite de ses *Annales* se trouve à la Bibliothèque de l'Université de Cambridge. Son œuvre sur la vanité et les malheurs de l'existence fut imprimée à Mayence en 1495. Plusieurs ouvrages de cryptographie ou de stéganographie ont en effet été publiés sous le nom de l'abbé Tritheim sans qu'on puisse savoir exactement ce qui s'y trouve de lui. Une traduction de son livre « *Polygraphiae* » publié en 1499 en Germanie (à Spanheim plus précisément), a été faite par Gabriel de Collange : « *La Polygraphie et universelle escriture cabalistique de Jean Trithème* ; Paris 1561 ». Trithème fut soupçonné de diablerie, et il fut accusé de pratiques nécromantiques.

M = dans la lumière
N = en paradis
O = toujours
P = dans la divinité
Q = dans la déité
R = dans la félicité
S = dans son règne
T = dans son royaume
UVW = dans la béatitude
X = dans la magnificence
Y = au trône
Z = en toute éternité
deviendra :
Un monde sans fin à perpétuité
Dans son règne et en une infinité
Irrévocablement et à perpétuité
Dans la béatitude et dans la magnificence
Dans la déité et dans la béatitude
Irrévocablement et en une infinité
Dans les cieux et en paradis
Dans son règne et dans la divinité
Sans cesse car dans les cieux
Dans la félicité et dans son règne
Dans les cieux et dans la gloire
À perpétuité pour toujours
En paradis et dans son royaume
Dans la lumière et dans les cieux
Dans la gloire et dans son règne
À perpétuité et dans la félicité
Dans la béatitude et irrévocablement
Dans la divinité pour toujours
Dans la lumière et dans la divinité
À perpétuité, à perpétuité
Un monde sans fin pour toujours
Dans la félicité et en paradis
À perpétuité et irrévocablement
Dans la gloire, dans la gloire
À perpétuité

Le code Navaro en 1942

L'idée vient de Philipp Johnston, un enfant de missionnaire élevé dans une réserve Navajo dans la région de San Diego. Ce dernier réfléchissait, en temps qu'ingénieur, sur un nouveau système de chiffrage de message. Il proposa son idée au lieutenant-colonel James E. Jones, officier des transmissions dans le Camp Elliott. Autre point fort des Navajos : la langue Navajo est de la famille des langues Na-Dene, comprenez qui n'a aucun lien avec une langue européenne ou asiatique. Les esquimaux font partie de cette catégorie. Autre fait important, les Navajos étaient le seul peuple a ne pas avoir eu la visite d'étudiants allemands depuis 1922. Avec ces éléments en mains, quelques semaines plus tard, la mission « code Talkers » étaient lancées par l'État major US.

L'US Army va donc s'équiper de ce code de chiffrement révolutionnaire et cela grâce au langage des indiens Navaros. Un vocabulaire, des phrases, qui n'existaient que sous forme orale. Les Américains vont inventer l'alphabet et l'écriture Navaro, d'où un décryptage impossible à l'époque. Le film WindTalkers de John Woo, Nicolas Cage, retrace l'histoire de ces indiens Navaros qui font partie intégrante de la victoire des Alliés lors de ce conflit mondial. Les mathématiciens de l'US Army, basés à l'époque au Camp Pendleton, en Californie, vont transformer la langue Navaro en un code quasi indéchiffrable, car basé sur aucune formule mathématique. Le « Code Talkers » Navajo emploie des mots tirés de la nature pour ensuite décrire des termes militaires spécifiques. Par exemple, les Navaros parlaient des saumons sous le mot de « Besh-Lo ». Traduit, Besh-Lo donnait « poisson de fer » qui en langage militaire signifiait sous-marin. Même idée pour « Da-he-tih-hi » qui signifiait colibri, il identifiait pour les soldats américains l'aviation. Donc-la-ih, signifiait étoile. La traduction militaire décrivait un général, « Da-gha-hi », signifiait barbe, comme celle portait par les légionnaires français. En trois ans, de 1942 à 1945, prés de 450 indiens des réserves de l'Arizona et du Nouveau-Mexique vont être utilisés pour mettre en place ce code atypique. Vingt-neuf d'entre eux iront sur le terrain pour servir de codeur/décodeur. Près de deux cents vingt cinq mots seront ainsi inventés. L'Oncle Sam étant ce qu'il est, les indiens Navajos étaient surveillés comme un diamant sur le sable. Ces soldats pas comme les autres étaient perpétuellement escortés par d'autres soldats qui avaient pour mission de les protéger... mais aussi de les tuer en cas ou ils tomberaient entre les mains ennemies.

Les « code talkers » resteront dans l'anonymat jusqu'en 1968. Les services secrets US vont se servir de ce code durant la guerre froide avant de l'abandonner définitivement. En 1982, le gouvernement américain institua, en l'honneur des « code talkers », une fête nationale, le 14 août. Sur vingt-neuf Navajos, quatre sont encore vivant aujourd'hui. Ils ont reçu, en 2001, la médaille du Congrès, la plus haute récompense décernée à des civils. Les vingt-cinq autres l'ayant reçu à titre posthume. Comble du comble, la médaille du Congrès US est la plus haute distinction remise à un civil : les soldats Navajos n'ont même pas eu droit aux honneurs militaires !

La méthode des lettres repérées est aussi un moyen de stéganographie pure, l'acrostiche (la première lettre de chaque mot ou vers constitue le message connu) en est l'exemple le plus connu. Nous y reviendrons. Mais d'innombrables variantes moins évidentes ont été inventées. Ainsi, au milieu du XVII^{e} siècle, sir John Trevanion, partisan de Charles I^{er}, fut arrêté par les hommes de Cromwell et enfermé au château de Colchester. Alors qu'il attendait une condamnation à mort, on lui remit une lettre dont on peut penser qu'elle avait été soigneusement examinée par ses gardiens. Il remarqua toutefois que certaines virgules étaient étrangement placées et repéra alors qu'en prenant la troisième lettre après chaque

signe de ponctuation il obtenait le message : *Panel at east end of chapel slides* (le panneau à l'extrémité est de la chapelle peut glisser). Il demanda à être seul dans la chapelle pour y prier et s'évada.

Un autre système utilisant l'espacement entre les mots peut également être proposé. On change l'espacement entre les lettres ou entre les mots dans deux versions d'un même texte. La superposition des deux textes fait apparaître le message.

A l'envers, cette figure nuit à la compréhension.
A l'endroit, son exposition semble trop convenue.

et celle-ci

A l'envers, cette figure nuit à la compréhension.
A l'endroit, son exposition semble trop convenue.

La superposition des deux met en relief une phrase :

A l'envers, **cette** figure **nuit** à la compréhension.
A l'endroit, son exposition semble trop **convenu**e.

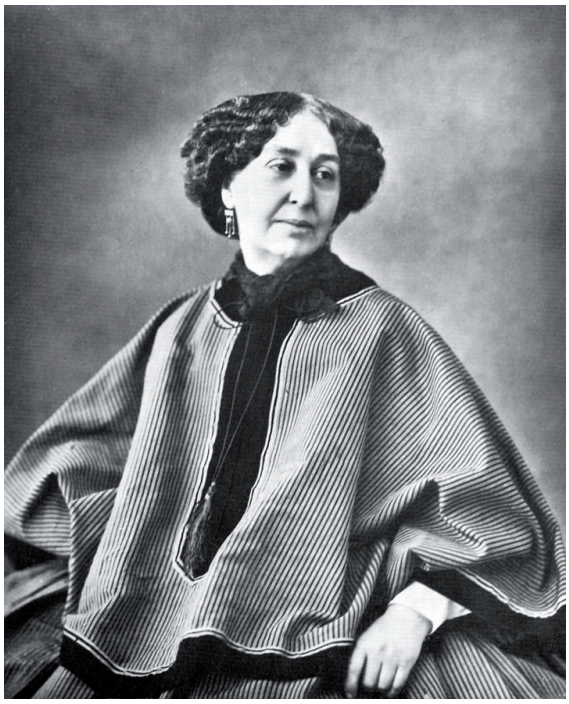
Bien des exemples de messages par lettres marquées pourraient être cités, comme celui du « nègre » qui laisse son nom caché dans le manuscrit qu'il rédige pour un autre. On trouve un bel exemple de signature avec l'utilisation de l'acrostiche dans *Fils du peuple*, hagiographie de Maurice Thorez publiée en 1937, signée par ce dernier, mais rédigée par Jean Fréville critique littéraire à *L'Humanité*. Un indice oriente les initiés : une description curieuse du paysage de l'adolescence de Thorez qui se révèle être un procédé pour signer le livre :

« *ferrailles rongées et verdies, informes lacis, larges entonnoirs aux escarpements crayeux, ravinés, immenses, tranchées creusées en labyrinthes, infranchissables vallonnements ravagés, embroussaillés* ».

En prenant la première lettre de chaque mot, on peut lire : « *Fréville a écrit ce livre* ».

Un autre exemple de stéganographie pure appartient à la littérature française avec la très célèbre lettre de George Sand envoyée à Alfred de Musset. L'apparent romantisme fait place à une déclaration pour le moins explicite... (lire une ligne sur deux)

Je suis très émue de vous dire que j'ai
bien compris, l'autre jour, que vous avez
toujours une envie folle de me faire
danser. Je garde un souvenir de votre
baiser et je voudrais que ce soit
là une preuve que je puisse être aimée
par vous. Je suis prête à vous montrer mon
affection toute désintéressée et sans cal-
cul. Si vous voulez me voir ainsi
dévoiler, sans aucun artifice mon âme
toute nue, daignez donc me faire une visite.
Et nous causerons en amis et en chemin.
Je vous prouverai que je suis la femme
sincère capable de vous offrir l'affection
la plus profonde et la plus étroite
amitié, en un mot, la meilleure amie
que vous puissiez rêver. Puisque votre
âme est libre, alors que l'abandon où je
vis est bien long, bien dur et bien souvent
pénible, ami très cher, j'ai le cœur
gros, accourez vite et venez me le
faire oublier. À l'amour, je veux me sou-
mettre entièrement.



Votre poupée.

La réponse d'Alfred de Musset, n'est pas moins ardente (lire le premier mot de chaque ligne) :

Quand je vous jure, hélas, un éternel hommage

Voulez-vous qu'un instant je change de langage
Vous avez su captiver les sentiments d'un cœur
Que ne puis-je, avec vous, goûter le vrai bonheur
Je vous aime, ô ma belle, et ma plume en délire
Couche sur le papier ce que je n'ose dire
Avec soin, de mes vers, lisez le premier mot
Vous saurez quel remède apporter à mes maux.
Et pour conclure...
Cette grande faveur que votre ardeur réclame
Nuit peut-être à l'honneur, mais répond à ma flamme.
...Fut la réponse !

Autres textes à double lecture utilisant des coupures dans la disposition du texte :

J'adjure maintenant	Rome avec sa croyance
Calvin entièrement	j'ai en grande révérence
J'ai en très grand mépris	la messe et tous les saints
Et en exécration	du Pape et la puissance
De Calvin la leçon	reçois en diligence
Et ceux qui le confessent	sont heureux à jamais
Tous damnés me paraissent	le pape et ses sujets
Oui Calvin et Luther	je veux aime sans cesse
Brûlerons en enfer	ceux qui suivent la messe

Plus près de nous, ce tract :

Aimons et admirons	Le chancelier Hitler
L'éternelle Angleterre	est indigne de vivre
Maudissons, écrasons	le peuple d'outre-mer
Le Nazi sur la terre	sera seul à survivre.
Soyons donc le soutien	du Führer allemand
De ces navigateurs	la race soit maudite.
A eux seuls appartient	ce juste châtiment
La palme du vainqueur	répond au vrai mérite

Enfin, revenons au romantisme avec cette lettre à double sens écrite dans un beau style :
Mademoiselle,
Je m'empresse de vous écrire pour vous déclarer
que vous vous trompez beaucoup si vous croyez
que vous êtes celle pour qui je soupire.
Il est vrai que pour vous éprouver,
je vous ai fait mille aveux. Après quoi
vous êtes devenue l'objet de ma raillerie.
Ainsi ne doutez plus de ce que vous dit ici celui
qui n'a eu que de l'aversion pour vous, et
qui aimerait mieux mourir que de

se voir obligé de vous épouser, et de
changer le dessein qu'il a formé de vous
haïr toute se vie, bien loin de vous
aimer, comme il vous l'a déclaré. Soyez donc
désabusée, croyez-moi ; et si vous êtes encore
constante et persuadée que vous êtes aimée,
sous serez encore plus exposée à la risée
de tout le monde et particulièrement de
celui qui n'a jamais été et ne sera jamais
Votre serviteur.

Autre procédé s'apparentant à la stéganographie : l'usage de la contrepèterie. Bien qu'il s'agisse ici de texte courts à usage souvent grivois, il n'en reste pas moins que le but est de cacher le vrai sens d'un texte. Exemples :

Consonnes simples placées au début des mots : *ce **p**ignon a royale **m**ine*
Consonnes simples à l'intérieur des mots : *À Beau**m**ont-le-Vi**c**omte* (Rabelais)
Consonnes simples au début ou à l'intérieur des mots : *la **b**erge du ra**v**in*
Consonnes doubles ou multiples au début des mots : *je suis arrivé à **p**ied par la **Ch**ine*
Consonnes doubles ou multiples à l'intérieur des mots : *Bran**ch**ez les co**l**onnes*
Consonnes doubles ou multiples au début ou à l'intérieur des mots :
*La **Ch**ine se dressait devant les Ni**pp**ons car la poule pon**d**ait quelque **p**art*

Un procédé de stéganographie de texte moderne : les pages HTML.

Deogol[162] est un projet qui modifie un fichier HTML pour y insérer un message texte. On peut se demander comment il s'y prend pour cacher ses données sans modifier ni l'aspect extérieur du fichier ni sa taille. La réponse se situe dans les attributs des balises HTML : il ne modifie pas les valeurs (ça modifierait l'aspect du document) mais leur ordre d'apparition dans la balise. Ainsi la balise :

Google.fr

peut aussi s'écrire :

Google.fr

On a donc deux états possibles : 0 ou 1. Ce qui nous permet de dissimuler... 1 bit ! Certes ce n'est pas vraiment le top. Mais dans le cas où une balise possède 8 tags, on a alors 8! (factorielle 8) possibilités ce qui nous permet de dissimuler d'après la documentation du logiciel, un peu moins de deux octets. Évidemment pour dissimuler de gros messages il faut de sacrées pages. Avec l'index d'un simple blog vous ne pouvez cacher que 47 octets. L'auteur conseille de prendre des pages de sites de news comme celle de News.Google.fr. Deogol s'utilise en ligne de commande et est assez simple d'utilisation, cependant une page qui semble alterner l'ordre des tags pour le plaisir ça choque au premier coup d'œil les spécialistes... Malgré tout, ça reste quand même un outil intéressant sur le sujet.

[162] Deogol est un programme en ligne de commande, qui permet la stéganographie simple pour les documents HTML, écrit en *Perl.* Le langage Perl (rétro-acronyme de « *Practical Extraction and Report Language* » ou Langage Pratique d'Extraction et de Rapport) est un langage de programmation créé par Larry Wall en 1987).

Le langage de description de ces pages, le HTML, interprète de la même façon un, deux, trois et même *n* espaces consécutifs : le navigateur n'affichera qu'un seul espace. Il suffit, entre les mots, d'insérer autant d'espaces que la lettre qu'on veut cacher (un espace pour A, deux espaces pour B, etc.).

Message à cacher : BIBMATHS
Description en espaces : 2-9-2-13-1-20-8-19

Affichage dans le navigateur	Code source
Avec l'avènement de l'informatique, la stéganographie est redevenu un...	Avec l'avènement de l'informatique, la stéga-nographie est redevenu un...

Bien sûr, il suffit de connaître le protocole utilisé pour retrouver le message original. En outre, ouvrir la page dans un éditeur comme *FrontPage*, puis la ré-enregistrer, suffit parfois à perdre l'information cachée.

Le code HTML permet d'insérer des commentaires qui ne sont visibles qu'en affichant le fichier source de la page (touche F5, ou clic droit « code source de la page »). Exemple de code HTML :

```
<HTML><HEAD>
<TITLE>Stéganographie</TITLE>
<link rel=«stylesheet» href=»../style.css»>

<!--
MESSAGE CACHE : ET VOILA, C'EST AUSSI SIMPLE QUE CELA !!!
-->

<SCRIPT LANGUAGE=«JavaScript»>
```

Le texte surligné n'apparaît évidemment pas sur l'écran, car il est encadré par des balises de commentaires (<!-- -->). Les commentaires sont des indications placées par le webmestre pour faciliter la correction d'erreurs et segmenter la construction de sa page web.

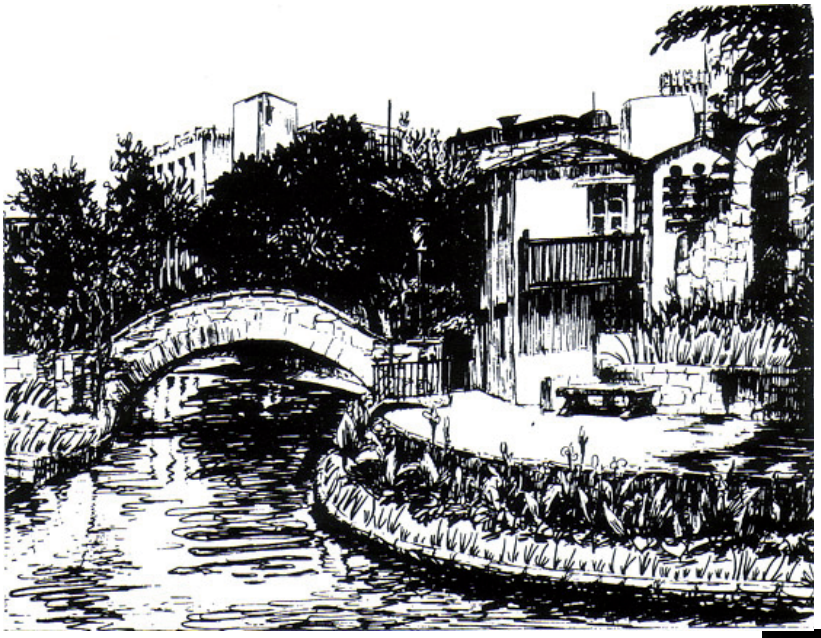
Les possibilités sont variées, car rien n'empêche de crypter le texte caché.

Pour ce qui est des mails, la sténographie du texte, selon les procédés décrits plus haut est applicable, mais l'utilisation d'images en pièces jointes est une techniques que nous détaillerons plus loin et qui met à l'abri de la plupart des systèmes de surveillance classiques.

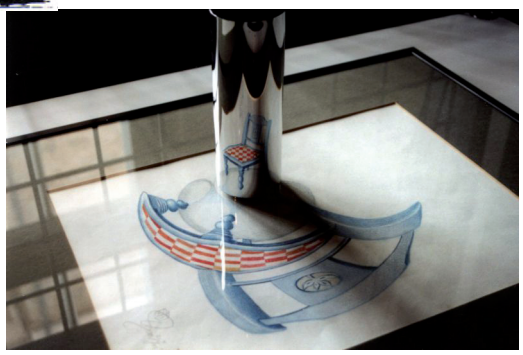
Aujourd'hui, des milliards de données parcourent le monde, et l'utilisation de la stéganographie assure parfaitement la discrétion des messages que l'on peut vouloir masquer. On a même prétendu que les auteurs de l'attentat du 11 septembre auraient utilisé simplement des passages du Coran ou des images pornographiques pour se transmettre les informations.

Les services de censure dont nous parlions plus haut n'auraient plus aucun sens à l'heure actuelle, car il faudrait tout interdire : l'envoi de cassettes audio, vidéo, disquettes informatiques, et toutes les communications Internet ! Les progrès techniques facilitent la vie des espions et autres terroristes ou trafiquants.

Un texte dans une image



Certains systèmes de stéganographie utilisent les images pour transmettre secrètement et rapidement de grandes quantités d'information. L'idée d'inclure un message secret dans une image n'est pas nouvelle, seule la technique a évolué. Nous voyons ci-contre une image dans laquelle est caché un message en code Morse. Ce sont les herbes au bord de la rivière qui abritent le message : une herbe longue = un trait, une herbe courte = un point.



L'utilisation de l'anamorphose permet même l'inclusion d'une image dans une autre, visible seulement par un œil averti. Les anamorphoses à miroir permettent grâce à l'interposition d'un miroir cylindrique ou conique de faire apparaître une image qui est la réflexion d'une image déformée conçue à cet effet. L'image déformée est peinte sur une surface plane autour d'un emplacement prévu du miroir ; ce n'est qu'en y installant le miroir que l'image apparaît non déformée sur la surface de celui-ci. Répandu au XVII^{e} siècle et XVIII^{e} siècle, ce procédé d'anamorphose a permis de diffuser caricatures, scènes érotiques et scatologiques, scènes de sorcellerie et grotesques qui se révélaient pour un public confidentiel lorsque le miroir était positionné sur la peinture.

Le développement de l'Internet et l'encadrement législatif des procédés de cryptographie que nous étudierons plus loin, ont provoqué la mise en place de systèmes permettant d'inclure un texte, codé ou non, et de façon invisible et indétectable par les « robots[163] » qui surveillent tout ce qui circule sur la toile, dans des images d'apparence anodines.

[163] Selon des sources du *Monde du Renseignement,* proches du Pentagone, dans des laboratoires de l'université de Syracuse, des chercheurs de l'US Air Force Rome Laboratory et de la NSA testent actuellement des prototypes de logiciels d'interception systématique des messages stéganographiés. La stéganographie appartient aux procédés de cryptographie les plus antiques, et consiste à dissimuler un message en le cachant dans le corps d'un autre texte ou d'une image. De nombreux services de renseignement, mais aussi des communautés de pirates, utilisent une version moderne de ce principe. Ils échangent sur Internet des textes secrets à travers des photographies à priori anodines. D'un point de vue schématique, des programmes spécialement développés permettent d'insérer des lettres dans des chaînes de pixels, sans altérer les qualités du cliché à l'œil nu. Des galeries d'art et des musées emploient déjà des versions simplifiées de cette technologie pour marquer les œuvres qui circulent sur Internet (principalement pour les photos d'art). Actuellement, l'entreprise allemande Demcom GmbH distribue sur le web *Steganos* le logiciel de Stéganographie le plus répandu. Récemment les scientifiques intervenant à Syracuse auraient réalisé plusieurs tests concluants d'identification et de déchiffrement de messages utilisant *Steganos*. Idéalement, leurs travaux tendent

La méthode de transmission par les images numériques est assez facile à mettre en œuvre. L'émetteur du message secret envoie une image à son correspondant, dans laquelle il a modifié quelques pixels dont l'emplacement a été convenu ; ces pixels ont été remplacés par d'autres dont les numéros codent les lettres du message. Si le nombre de pixels modifiés est assez faible, il est impossible de détecter quoi que ce soit en regardant l'image très peu modifiée. De plus, si l'image est interceptée, elle ne peut donner de renseignements à l'analyse puisque l'analyste ne dispose pas de l'image originale pour comparer et trouver les modifications. Notons au passage que ce procédé est utilisable également sur des fichiers son. En fait, cela revient à incorporer un « bruit » dans le fichier (image ou son) sans que l'on puisse déterminer si ce bruit est d'origine ou ajouté. Exemple :

L'image du haut est l'image originale, l'image dessous est l'image codée. Nous avons convenu avec le destinataire de coder les pixels de coordonnées multiples de 20 à partir du premier pixel de la première ligne. Cette image comporte 283 pixels de large sur 189 pixels de haut. Nous disposons donc de 126 pixels modifiables (283/20) + (189/20). Soit 126 signes utilisables. Nous avons établi également une « clé » arbitraire, chaque lettre ayant une valeur numérique. Cette clé est la suivante :

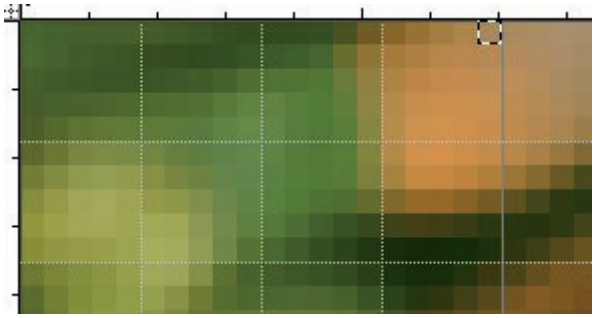
S = 16 ; T = 18 ; G = 13 etc.

Nous nous proposons de coder le mot STÉGANOGRAPHIE et selon la clé précédemment définie, cela nous donne :

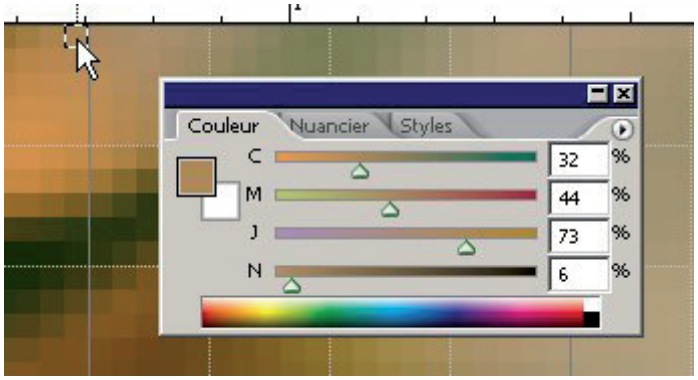
S TE GANOG RAPHIE
16 18 4 13 5 14 3 13 11 5 6 1 2 4

Pour coder notre image, nous changeons seulement la valeur du noir de chaque pixel sélectionné en additionnant la valeur attribuée à la lettre à la valeur du noir relevée sur l'image originale. Ainsi, le premier pixel positionné en 20 sur la ligne 1 qui a une valeur de noir de 6, passe à 22 (6 + 16), voir illustration, et ainsi de suite. Ce marquage est quasi invisible à l'œil, surtout si l'on prend soin de choisir une image présentant peu de surface de même couleur et densité (à plat)

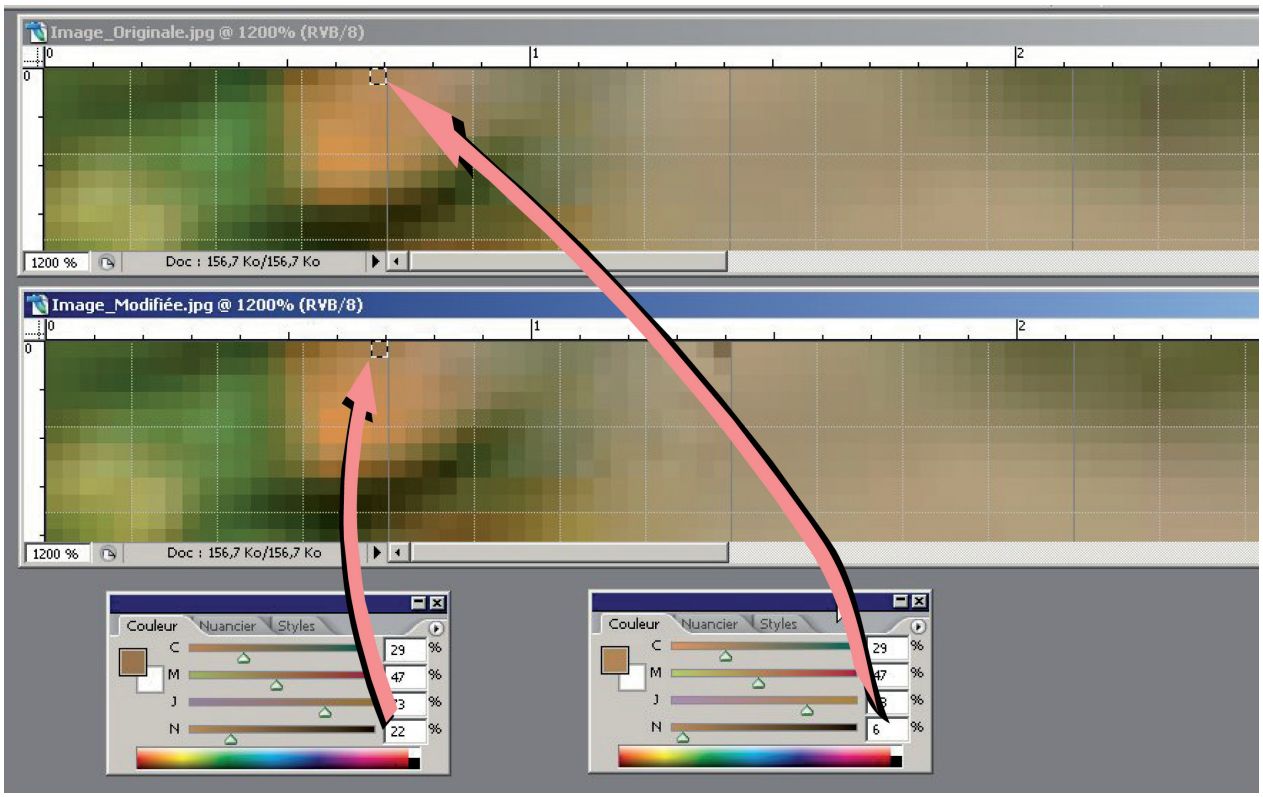
vers la mise au point d'un programme qui repérerait automatiquement les images comportant des textes cachés en balayant des grandes masses de messages interceptés. Car dans la pratique, décodé systématiquement, le message, après avoir été repéré (séparer les lettre des pixels), ne représente plus d'obstacle majeur. Une petite société d'ingénierie informatique basée à New-York, Westone Technologies Inc., y parvient depuis 1999, à l'issue de recherches menées conjointement avec le Air Force Rome Laboratory. Une fois de plus, la NSA est confrontée à son défi majeur, l'analyse de vastes volumes de communications électroniques. Dans ce domaine, les budgets nécessaires pour disposer des outils les plus puissants justifieraient les dernières complaintes de son directeur, le général Michael Hayden. Lors d'un congrès sur la guerre de l'information qui s'est tenu à Baltimore le 16 octobre dernier, il a réitéré sa volonté que la NSA représente la figure de proue du Pentagone pour toute la défense du Cyberespace. (Source : *Le Monde du renseignement*, 26-10-2000).



La grille des pixels avec le pixel 1-20 sélectionné



Mesure de la valeur en noir du pixel sélectionné



La comparaison des deux pixels donne les valeurs du noir et par différence, on obtient la valeur numérique de la lettre codée.

Un bon programmeur est sans doute capable de créer un programme plus ou moins automatique de codage et de décodage par ce procédé. L'avantage principal est l'invisibilité totale du masquage.

Le marquage des images

Pour bien comprendre les méthodes de marquage ou de stéganographie appliquées aux images, il est nécessaire de rappeler rapidement les définitions d'une image numérique.

On désigne sous le terme d'image numérique toute image (dessin, icône, photographie…) acquise, créée, traitée ou stockée sous forme binaire (suite de 0 et de 1) :

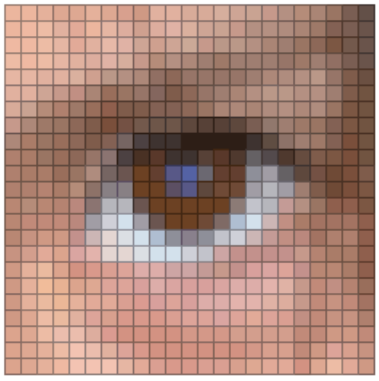
– Acquise par des dispositifs comme les scanners, les appareils photo ou caméscopes numériques, les cartes d'acquisition vidéo (qui numérisent directement une source comme la télévision).

– Créée directement par des programmes informatiques, via la souris, les tablettes graphiques ou par la modélisation 3D (ce que l'on appelle par abus de langage les « images de synthèse »).

Traitée grâce à des outils informatiques. Il est facile de la modifier en taille, en couleur, d'ajouter ou supprimer des éléments, d'appliquer des filtres variés, etc.

On distingue deux types d'images à la composition et au comportement différents : images matricielles et les images vectorielles.

Images matricielles (ou images bitmap)



Elle est composée comme son nom l'indique d'une matrice (tableau) de points à plusieurs dimensions, chaque dimension représentant une dimension spatiale (hauteur, largeur, profondeur), temporelle (durée) ou autre (par exemple, un niveau de résolution).

Dans le cas des images à deux dimensions (le plus courant), les points sont appelés pixels[164]. D'un point de vue mathématique, on considère l'image comme une fonction de $\mathbb{R}$ x $\mathbb{R}$ dans $\mathbb{R}$[165] où le couplet d'entrée est considéré comme une position spatiale, le singleton de sortie comme un codage.

Ce type d'image s'adapte bien à l'affichage sur écran informatique (lui aussi orienté pixel) ; il est en revanche peu adapté pour l'impression, car la résolution des écrans informatiques, généralement de 72 à 96 PPP (« points par pouce », en anglais *dots per inch* ou *dpi*) est bien inférieure à celle atteinte par les imprimantes, au moins 600 PPP aujourd'hui. L'image imprimée, si elle n'a pas une haute résolution, sera donc plus ou moins floue ou laissera apparaître des pixels carrés visibles.

Résolutions :
300 dpi *150 dpi* *72 dpi*

Images 2D + t (vidéo), images 3D, images multi-résolution

– Lorsqu'une image possède une composante temporelle, on parle d'animation.

– Dans le cas des images à trois dimensions, les points sont appelés des *voxels*. Ils représentent un volume.

Ces cas sont une généralisation du cas 2D, la dimension supplémentaire représentant respectivement le temps, une dimension spatiale ou une échelle de résolution.

D'un point de vue mathématique, il s'agit d'une fonction de $\mathbb{R}$ x $\mathbb{R}$ x $\mathbb{R}$ dans $\mathbb{R}$.

[164] Le pixel (px en abrégé), ou point, est l'unité de base d'une image numérique. Son nom provient de la locution anglaise *picture element*, qui signifie, « élément d'image » ou « point élémentaire ». Pour informatique, un point est codé sur plusieurs bits (le mot « bit » est la contraction de l'anglais *binary digit*, qui signifie « chiffre binaire ». Un bit ne peut prendre que deux valeurs : 0 ou 1). La place mémoire occupée par un point dépend de la « profondeur », c'est-à-dire du nombre de couleurs affichables : noir et blanc : un bit (1/8e d'octet) ; 16 couleurs (standard VGA) : 4 bits ; 256 couleurs : 1 octet ; 65 536 couleurs (« milliers de couleurs ») : 2 octets (16 bits) ; 16 777 216 couleurs (« 16 millions de couleurs », « *true colors* ») : 3 octets (24 bits).

[165] $\mathbb{R}$ = ensemble de nombres réels

Images stéréoscopiques

Il s'agit d'un cas particulier dans lequel on travaille par couples d'images, ces derniers pouvant être de n'importe lequel des types précédents.

Images vectorielles

Le principe est de représenter les données de l'image par des formules géométriques qui vont pouvoir être décrites d'un point de vue mathématique. Cela signifie qu'au lieu de mémoriser une mosaïque de points élémentaires, on stocke la succession d'opérations conduisant au tracé. Par exemple, un dessin peut être mémorisé par l'ordinateur comme « une droite tracée entre les points (x1, y1) et (x2, y2) », puis « un cercle tracé de centre (x3, y3) et de rayon 30 de couleur rouge ».

L'avantage de ce type d'image est la possibilité de l'agrandir indéfiniment sans perdre la qualité initiale, ainsi qu'un faible encombrement. L'usage de prédilection de ce type d'images concerne les schémas qu'il est possible de générer avec certains logiciels de DAO (Dessin Assisté par Ordinateur) comme *AutoCAD* ou *CATIA*. Ce type d'images est aussi utilisé pour les animations *Flash*, utilisées sur Internet pour la création de bannières publicitaires, l'introduction de sites web, voire des sites web complets.

Étant donné que les moyens de visualisation d'images actuels comme les moniteurs d'ordinateur reposent essentiellement sur des images matricielles, les descriptions vectorielles (Fichiers) doivent préalablement être converties en descriptions matricielles avant d'être affichées.

Définition et résolution

Les images matricielles sont également définies par leur *définition* et leur *résolution*.

La *définition* d'une image est caractérisée par le nombre de points la composant. En image numérique, cela correspond donc au nombre de pixels qui compose l'image en hauteur (axe vertical) et en largeur (axe horizontal) : 200 pixels par 450 pixels par exemple, abrégé en « 200×450 ».

La *résolution* d'une image est définie par un nombre de pixels par unité de longueur de la structure à numériser (classiquement en point par pouce – PPP –). Ce paramètre est défini lors de la numérisation (passage de l'image sous forme binaire), et dépend principalement des caractéristiques du matériel utilisé lors de la numérisation. Plus le nombre de pixels par unité de longueur de la structure à numériser est élevé, plus la quantité d'information qui décrit cette structure est importante et plus la résolution est élevée. La résolution d'une image numérique définit le degré de détail de l'image. Ainsi, plus la résolution est élevée, meilleure est la restitution.

Cependant, pour une même dimension d'image, plus la résolution est élevée, plus le nombre de pixels composant l'image est grand. Le nombre de pixels est proportionnel au carré de la résolution, étant donné le caractère bidimensionnel de l'image : si la résolution est multipliée par deux, le nombre de pixels est multiplié par quatre. Augmenter la résolution peut entraîner des temps de visualisation et d'impression plus longs, et conduire à une taille très importante du fichier contenant l'image et à de la place excessive occupée en mémoire. (voir illustration résolutions ci-contre)

Représentation des couleurs

Il existe plusieurs modes de codage informatique des couleurs, le plus utilisé pour le maniement des images est l'espace colorimétrique Rouge, Vert, Bleu (RVB ou RGB). Cet espace est basé sur une synthèse additive des couleurs, c'est-à-dire que le mélange des trois composantes R, V, et B à leur valeur maximum donne du blanc, à l'instar de la lumière. Le mélange de ces trois couleurs à des proportions diverses permet de reproduire à l'écran une part importante du spectre visible, sans avoir à spécifier une multitude de fréquences lumineuses.

Il existe d'autres modes de représentation des couleurs :

– Cyan, Magenta, Jaune, Noir (CMJN ou CMYK) utilisé principalement pour l'impression, et basé sur une synthèse soustractive des couleurs ;

– Teinte, Saturation, Luminance (TSL ou HSL), où la couleur est codée suivant le cercle des couleurs ;

– Base de couleur optimale YUV, Y représentant la luminance, U et V deux chrominances orthogonales.

Les images bitmap en couleurs peuvent dont être représentées soit par une image dans laquelle la valeur du pixel est une combinaison linéaire des valeurs des trois composantes couleurs, soit par trois images représentant chacune une composante couleur. Dans le premier cas, selon le nombre de bits (unité d'information élémentaire qui peut prendre deux valeurs distinctes) alloués pour le stockage d'une couleur de pixel, on distingue généralement les différents types d'images suivants :

Images 24 bits (ou « couleurs vraies »)

Il s'agit d'une appellation trompeuse, car le monde numérique (fini, limité) ne peut pas rendre compte intégralement de la réalité (infinie). Le codage de la couleur est réalisé sur trois octets[166], chaque octet représentant la valeur d'une composante couleur par un entier de 0 à 255. Ces trois valeurs codent généralement la couleur dans l'espace RVB. Le nombre de couleurs différentes pouvant être ainsi représenté est de 256 x 256 x 256 possibilités, soit près de 16 millions de couleurs. Comme la différence de nuance entre deux couleurs très proches, mais différentes dans ce mode de représentation, est quasiment imperceptible pour l'œil humain, on considère par commodité que ce système permet une restitution exacte des couleurs, c'est pourquoi on parle de « *couleurs vraies* ».

R	V	B	Couleur
0	0	0	noir
255	0	0	rouge
0	255	0	vert
0	0	255	bleu
128	128	128	gris
255	255	255	blanc

Les images bitmap basées sur cette représentation peuvent rapidement occuper un espace de stockage considérable, chaque pixel nécessitant trois octets pour coder sa couleur.

Images à palettes, images en 256 couleurs (8 bits)

Pour réduire la place occupée par l'information de couleur, on utilise une palette de couleurs « attachée » à l'image. On parle alors de *couleurs indexées* : la valeur associée à un pixel ne véhicule plus la couleur effective du pixel, mais renvoie à l'entrée correspondant à cette valeur dans une table (ou palette) de couleurs appelée *look-up table* ou *LUT* en anglais, dans laquelle on dispose de la représentation complète de la couleur considérée.

Selon le nombre de couleurs présentes dans l'image, on peut ainsi gagner une place non négligeable : on considère en pratique que 256 couleurs parmi les 16 millions de couleurs 24 bits sont suffisantes. Pour les coder, on aura donc une palette occupant 24 bits x 256 entrées, soit 3 x 256 octets, et les pixels de l'image seront associés à des index codés sur un octet. L'occupation d'une telle image est donc de 1 octet par pixel plus la LUT, ce qui représente un peu plus du tiers de la place occupée par une image en

[166] Un octet est une unité de mesure en informatique mesurant la quantité de données. Un octet est lui-même composé de 8 bits, soit 8 chiffres binaires.

couleurs 24 bits (plus l'image contient de pixels, plus le gain de place est important, la limite étant le tiers de la place occupée par l'image en couleurs vraies).

Une autre méthode consiste à se passer de palette, et de coder directement les trois couleurs en utilisant un octet : chaque composante couleur est codée sur deux bits, le bit restant peut servir soit à gérer plus de couleurs sur une des composantes, soit à gérer la transparence du pixel. Avec cette méthode, on obtient des images bitmap avec un codage couleur effectivement limité à 8 bits, bien que la plage des couleurs possibles soit très réduite par rapport à celle qu'offre la méthode utilisant une palette.

Dans le cas des images en couleurs indexées, il est possible de spécifier que les pixels utilisant une des couleurs de la palette ne soient pas affichés lors de la lecture des données de l'image. Cette propriété de transparence est très utilisée (et utile) pour les images des pages web (format GIF), afin que la couleur de fond de l'image n'empêche pas la visualisation de l'arrière-plan de la page.

Images en teintes (ou niveaux) de gris

On ne code ici plus que le niveau de l'intensité lumineuse, généralement sur un octet (256 valeurs). Par convention, la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255 le blanc (intensité lumineuse maximale) :

000	008	016	024	032	040	048	056	064	072	080	088	096	104	112	120	128
	255	248	240	232	224	216	208	200	192	184	176	168	160	152	144	136

Ce procédé est fréquemment utilisé pour reproduire des photos en noir et blanc ou du texte dans certaines conditions (avec utilisation d'un filtre pour adoucir les contours afin d'obtenir des caractères plus lisses).

Ce codage de la simple intensité lumineuse est également utilisé pour le codage d'images couleur : l'image est représentée par trois images d'intensité lumineuses, chacune se situant dans une composante distincte de l'espace colorimétrique (par exemple, intensité de rouge, de vert et de bleu).

Images avec gestion de la translucidité

On peut attribuer à une image un canal supplémentaire, appelé *canal alpha*, qui définit le degré de transparence de l'image. Il s'agit d'un canal similaire aux canaux traditionnels définissant les composantes de couleur, codé sur un nombre fixe de bits par pixel (en général 8 ou 16). On échelonne ainsi linéairement la translucidité d'un pixel, de l'opacité complète à la transparence.

Structuration, utilisation de métadonnées[167]

La plupart des formats sont composés d'un en-tête contenant des attributs (dimensions de l'image, type de codage, LUT, etc.), suivi des données (l'image proprement dite). La structuration des attributs et des données diffère pour chaque format d'image.

De plus, les formats actuels intègrent souvent une zone de métadonnées (*metadata* en anglais) servant à préciser les informations concernant l'image comme :

– la date, l'heure et le lieu de la prise de vue,

– les caractéristiques physiques de la photographie (sensibilité ISO, vitesse d'obturation, usage du flash…)

Ces métadonnées sont par exemple largement utilisées dans le format Exif (extension du format JPEG), qui est le format le plus utilisé dans les appareils photo numériques.

[167] Une métadonnée (du grec meta « après » et du latin data « information ») est une donnée servant à définir ou décrire une autre donnée quel que soit son support (papier ou électronique).

Formats d'images

Un format d'image est une représentation informatique de l'image, associée à des informations sur la façon dont l'image est codée et fournissant éventuellement des indications sur la manière de la décoder et de la manipuler.

Quelques précautions à prendre concernant les formats d'images :

– les formats dits « propriétaires », peuvent différer selon le logiciel qui les manipule. De plus, leur pérennité n'est pas garantie : réaliser de nouveaux programmes pour les lire peut s'avérer difficile (surtout si leurs spécifications n'ont pas été rendues publiques), cela peut même s'avérer illégal si les algorithmes utilisés sont protégés par des brevets.

Il faut prêter attention aux différentes versions que peut recouvrir un format particulier. Notamment pour le format TIFF qui varie selon les versions ; certaines d'entre elles ne sont pas reconnues par certains logiciels.

Tableau comparatif

	Type (matriciel/ vectoriel)	Compression des données	Nombre de couleurs supportées	Affichage progressif	Animation	Transparence
JPEG	matriciel	Oui, réglable (avec pertes)	16 millions	Oui	Non	Non
JPEG 2000	matriciel	Oui, avec ou sans perte	32 millions	Oui	Oui	Oui
GIF	matriciel	Oui, sans perte	256 maxi (palette)	Oui	Oui	Oui
PNG	matriciel	Oui, sans perte	Palettisé (256 couleurs ou moins) ou 16 millions	Oui	Non	Oui (couche Alpha)
TIFF	matriciel	Compression ou pas, avec ou sans perte	de monochrome à 16 millions	Non	Non	Oui (couche Alpha)
SVG	vectoriel	compression possible	16 millions	Ne s'applique pas	Oui	Oui (par nature)

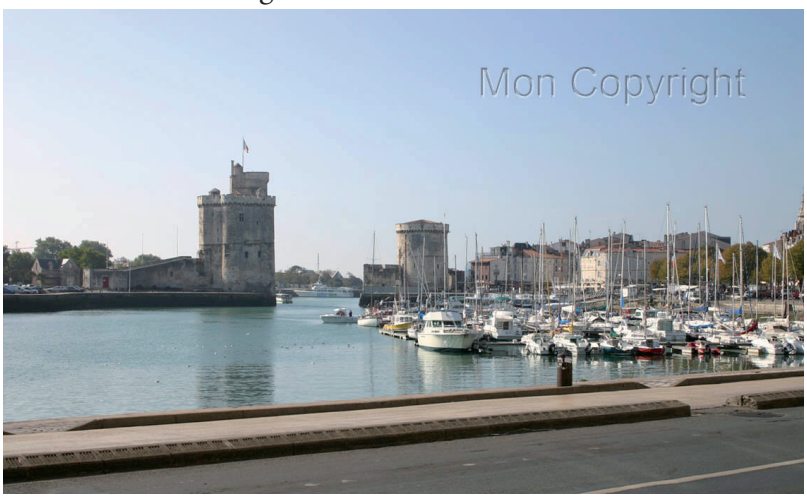
Formats propriétaires

Le format TIFF est considéré comme un format propriétaire, le brevet étant contrôlé par la firme Aldus.

Dans le passé, le format GIF était soumis au brevet *Unisys* contrôlé par le société *CompuServe*, c'était donc un format propriétaire. Mais il est à noter que les brevets d'*Unisys* sont arrivés à expiration le 20 juin 2003 aux États-Unis, le 18 juin 2004 dans la plupart des pays d'Europe, le 20 juin 2004 au Japon et le 7 juillet 2004 au Canada. Il est donc devenu depuis un format libre de droits.

Image numérique et droits d'auteur, une application de la Stéganographie

Pour tenter de faire respecter le droit d'auteur (en France) et le copyright (dans presque tous les autres pays), il existe des techniques de marquage numérique d'une image. Ces techniques, que l'on nomme *empreinte*, sont de plus en plus utilisées. L'empreinte est supposée conserver une preuve de l'origine de l'image, sous la forme d'une signature visible ou invisible, qui doit résister aux traitements susceptibles d'être appliqués à l'image. Ce « tatouage » peut se faire selon deux méthodes, généralement désignées par le même terme de filigrane :



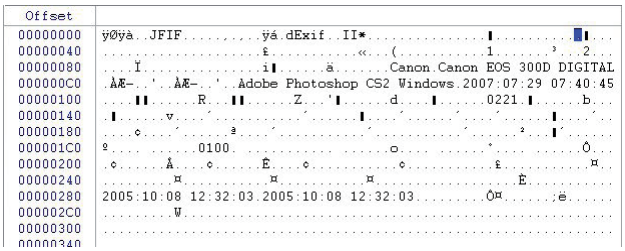
Protection par signature visible

Cette technique consiste à intégrer une indication sur l'image, par exemple le nom de l'organisme ou de l'auteur à qui appartient l'image, afin de dissuader les pirates de s'en servir. L'inconvénient de cette méthode est qu'il est très facile d'éliminer ce type de tatouage avec un outil de traitement d'images, puisque le tatouage est visible.

Protection par signature cryptée

Cette technique consiste à cacher le tatouage dans les données de l'image. Cette approche a l'avantage de ne pas gêner la lecture de l'image par le simple spectateur tout en permettant une facile identification. L'auteur en tire un avantage complémentaire : l'éventuel pirate inattentif ne sera pas tenté de retirer ou modifier la signature ; le pirate plus volontaire verra son activité illégale rendue un peu plus difficile ou facilement prouvable (par la seule présence du tatouage).

Le marquage peut se faire simplement dans les métadonnées qui figurent dans l'en-tête de tout fichier image. Par exemple, la lecture des métadonnées de l'image ci-dessus nous donne les informations suivantes : la prise de vue a été faite avec un appareil Canon EOS 300D DIGITAL (la date et l'heure sont indiquées plus bas : 10/08/2005 à 12 h 32) et le fichier a été modifié à l'aide de Photoshop CS2 pour Windows le 29/07/2007 à 07 h 40. En parcourant le fichier, on trouve également les indications de prise de vue : vitesse 1/200e, diaphragme : f11, sensibilité ISO : 100 ASA, etc. Notons qu'à l'aide de Photoshop Album, il est possible d'ajouter une « étiquette » contenant d'autres informations, comme justement un copyright.



Les indications ci-dessus ont été obtenues à l'aide d'un simple éditeur hexadécimal[168]. Avec ce type de logiciel, il est possible de changer ces indications et de les remplacer éventuellement par un message, codé ou non, sans modifier l'apparence de l'image. Ces modifications passeront inaperçues et ne seront pas détectées par d'éventuels systèmes de contrôle à la volée.

[168] Un éditeur hexadécimal permet d'éditer les fichiers binaires afin de modifier les valeurs qui y sont contenues. Cela permet de modifier certaines informations présentes dans un fichier. Le système hexadécimal est un système de numération utilisant la base 16. Le nom hexadécimal provient du fait qu'il utilise les 10 premiers chiffres arabes (décimal, dix) puis les 6 premières lettres de l'alphabet latin (hexa, six) : 0 1 2 3 4 5 6 7 8 9 A B C D E F. Ce fut l'entreprise Américaine IBM qui commença à utiliser ces chiffres-là en 1963. Il s'agit du standard actuellement reconnu.

En effet, les applications de *tatouage* ou de *marquage* sont très nombreuses, et les méthodes à utiliser sont assez complexes (comparées à celles utilisées pour le texte). Le marquage d'images a de nombreux buts : copyright des images (très important à l'époque d'Internet où des milliers d'images circulent sur le web), mais aussi marquage de papiers ou de billets (pour éviter la photocopie), vérification de l'intégrité de documents, etc. À chaque utilisation correspond une méthode. En fait, les techniques doivent répondre à certaines règles très importantes et souvent difficiles à concilier : endommager le moins possible le support sur lequel le marquage va avoir lieu et l'œil ne doit pas être choqué.

– le marquage doit pouvoir supporter le plus grand nombre de transformations possible sans être dégradé (compression JPEG, filtres, passage analogique-numérique, changement de palettes, etc.)

– la complexité de l'algorithme doit être minimum afin de pouvoir effectuer le marquage et/ou la détection en temps réel.

Le marquage peut avoir lieu au niveau de l'image dans le domaine des fréquences :

– Technique de *Watermarking (tatouage numérique)* tenant compte de la corrélation HVS-Canaux RGB ou même plus traditionnellement dans le domaine spatial :

– Bits de poids faible

– Signature par modulation d'amplitude

– Watermarking par DCT à taille de blocs variable

Nous parlerons également du watermarking de la seconde génération (un exemple proche est celui par modification géométrique). Certaines méthodes utilisent même la palette pour marquer l'image (dans le cas ou l'image possède une palette, comme pour le marquage *EzStego*). Les premières méthodes de signature d'images ont été proposées en 1993 par Caronni (bien que des articles plus anciens fassent déjà allusion à ce type de pratique). Les méthodes les plus récentes portent les noms de Anderson, Aucsmith, et Swansonet. Les méthodes utilisées dans la stéganographie dépendent surtout du type de marquage que l'on désire.

Attaques sur les marquages

Il existe deux grands courants d'attaques sur les images watermarkées :

– Les attaques « destructives » au cours desquelles on fait subir des transformations (souvent violentes) à l'image. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer que ces attaques ne sont pas forcément voulues. En effet, sans le savoir on peut dégrader suffisamment l'image pour que le tatouage soit effacé. En théorie, si le marquage est suffisamment fort, il doit résister à ces transformations ou tout au moins il doit rester tant que l'image reste exploitable.

Les attaques plus « subtiles » au cours desquelles le pirate va intentionnellement chercher à laver l'image sans l'endommager. Pour cela il va procéder par différents moyens à la recherche de la clef qui a permis de tatouer l'image (on peut alors qualifier cela de « stéganalyse »). Lorsqu'il l'aura trouvée il pourra alors lire le watermark, le changer, le supprimer etc....Nous verrons cela en deuxième partie.

Commençons par le premier type d'attaques

Voici une liste non exhaustive des différentes attaques possibles contre les images marquées. Ce que l'on appelle « *attaque* » est en fait une transformation que l'on va faire subir à l'image et qui va plus ou moins l'endommager, mais qui risque d'être fatale au marquage. Comme vous pouvez vous en douter, la confiance que l'on donne à un marquage dépend de sa capacité à résister à une attaque.

Compression JPEG :

Ceci est un mode de compression très en vogue (surtout depuis l'avènement de l'Internet). L'avantage de cette méthode se situe dans les taux de compression importants que l'on peut obtenir, mais son désavantage se situe dans le fait qu'il s'agit d'une compression destructive. En effet plus l'on compresse l'image plus des défauts apparaissent. Pour comprendre le pourquoi de ces défauts il faut se pencher ra-

pidement sur le principe de compression JPEG (qui se rapproche assez du format de compression MP3 pour le son). On découpe d'abord l'image en blocs carrés de 8 pixels sur 8 pixels. On effectue ensuite une Transformée de Fourier[169] en 2 dimensions du bloc. Ensuite, applique un filtre passe-bas (c'est-à-dire que l'on enlève les hautes fréquences), et c'est là que l'on choisit le taux de compression. Plus celui-ci va être élevé, plus l'on va supprimer une gamme de fréquences importantes et plus l'image va être dégradée.

Image originale

Image compressée (JPEG)

On applique ensuite une compression conservative. Vu l'importance de ce système de compression, tout bon algorithme de marquage doit pouvoir lui résister au moins dans les faibles taux de compression.

Les transformations géométriques :

– ***Symétrie horizontale*** : certaines images peuvent être « flippée » sans perdre de leur sens (par exemple un paysage). Bien qu'il ne s'applique qu'à peu d'images, lorsqu'il se produit, très peu de marquages lui survivent. Ce serait une grave erreur de penser que l'on ne peut pas appliquer ce genre d'attaque à un film. En effet, essayez vous-même de regarder un film qui a subi cette transformation, et vous ne vous apercevrez de rien du tout (sauf dans les scènes où de l'écriture intervient).

[169] La transformée de Fourier est un analogue de la théorie des séries de Fourier pour les fonctions non périodiques, et permet de leur associer un spectre en fréquences. On cherche ensuite à obtenir l'expression de la fonction comme « somme infinie » des fonctions trigonométriques de toutes fréquences qui forment son spectre. Une telle sommation se présentera donc sous forme d'intégrale. L'analyse non standard permet de la présenter sous forme d'une série et justifie le point de vue intuitif. Séries et transformation de Fourier constituent les deux outils de base de l'analyse harmonique. La **transformée de Fourier** $\mathcal{F}$ est une opération qui transforme une fonction intégrable en une autre fonction, décrivant le spectre en fréquences de *f*. Si *f* est une fonction intégrable, sa transformée de Fourier est la fonction *F(f)* et donnée par la formule :
$F(f) : s \mapsto \hat{f}(s) = \int_{-\infty}^{+\infty} f(x)\, e^{-isx}\, dx$ L'ensemble de départ est l'ensemble des fonctions intégrables f d'une variable réelle x. L'ensemble d'arrivée est l'ensemble des fonctions F(f) d'une variable réelle *s*. Concrètement lorsque cette transformation est utilisée en traitement du signal, on dit que x est la variable temps, que f est dans le *domaine temporel*, que s est la fréquence et que F est dans le *domaine fréquentiel*. La formule dite de transformation de Fourier inverse, opération notée *TF* -1, est celle qui permet (sous conditions) de retrouver f à partir du spectre : $f(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} F(w)\, e^{iwx}\, dw$

– ***Rotation*** : C'est une transformation qui est très utilisée après avoir scanné une image. Elle sert à réaligner des images (avec des petits angles) et peut être fatale à certains types de marquages.

– Le ***recadrage*** : Dans certains cas, les personnes ne sont intéressées que par un morceau de l'image (par exemple le centre). Elle recadre (en anglais « *crop* ») alors l'image, ce qui peut détruire le marquage.

– ***Changement d'échelle*** : Ce genre de transformations peut être séparé en deux groupes : les transformations uniformes (pour lesquelles on conserve les proportions, l'échelle en X varie comme l'échelle en Y) et bien sûr les transformations non uniformes (où l'échelle en X ne varie pas comme l'échelle en Y).

– ***Transformations géométriques aléatoires*** (ex : morphing, procédé par lequel une image synthétique se fond et devient une autre image.).

– ***Filtres passe-bas*** : Encore une fois, on utilise la transformée de Fourier pour travailler dans l'espace des fréquences de l'image et on ne laisse alors passer que les basses fréquences. En fait, dans des termes un peu plus mathématiques, il ne s'agit ni plus ni moins que d'un produit de convolution du signal (ici l'image) avec une fonction passe-bas (dont la transformée de Fourier est une Gaussienne, une fonction porte, etc.).

– ***Accentuation des contours*** : Ou encore appelé filtre « passe-haut » (car il supprime les basses fréquences), ou « *Sharpen* ». Il s'agit de l'inverse du filtre passe-bas (encore appelé « *Blur* »). L'intérêt d'une telle attaque est assez faible, sachant que l'on conserve le bruit (et les forts gradients de l'image), et que c'est souvent à ce niveau-là que se situe le tatouage (car c'est dans ces zones ou l'on cache de préférence de l'information).

– *Attaque par Mosaique* : Il s'agit ici d'utiliser le « *crop* » d'une façon beaucoup plus violente et qui se prête assez bien aux pages HTML. Il suffit de découper l'image en autant de morceaux que l'on désire (plus il y a de morceaux plus l'attaque à des chances d'aboutir), puis de recoller cette image au moment de l'affichage en créant par exemple en HTML un tableau dont chacune des cellules contiendra un morceau de l'image. Cette attaque est d'une rare efficacité si l'on se donne les moyens de bien découper l'image.

Technique de Watermarking tenant compte de la corrélation HVS-Canaux RGB

Dans cette technique de marquage, A.Piva, F. Bartolini, V. Cappellini et M. Barni se proposent de s'attacher uniquement aux images couleur et de réellement chercher une façon de jouer sur les couleurs tout en tenant compte du HVS (*Human Visual System*). L'idée est la suivante : marquer les 3 canaux de façons différentes selon la sensibilité de l'œil aux 3 longueurs d'onde. Voici comment marche plus précisément le marquage : On commence par faire la DCT de chacune des trois voies R,G, et B. Pour chacune des voies, les coefficients sont réorganisés en zigzag. Nous prenons alors n de ces coefficients pour chaque couleur, et nous obtenons ainsi 3 vecteurs à n composantes (contenants donc des coefficients de DCT). On applique ensuite la traditionnelle transformation suivante :

$$v'r(k+i) = vr(k+i) + AlphaR*|vr(k+i)|*xi$$
$$v'g(k+i) = vg(k+i) + AlphaG*|vg(k+i)|*xi$$
$$v'b(k+i) = vb(k+i) + AlphaB*|vb(k+i)|*xi$$

avec :

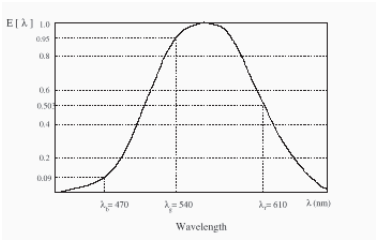
– xi : le marquage.

– AlphaR, AlphaG, AlphaB : l'intensité du marquage pour chaque voie.

– vr, vg, vb : les coefficients de la DCT non marqués.

-– v'r, v'g, v'b : les coefficients de la DCT marqués.

Les coefficients ainsi marqués sont remis en zigzag et l'on applique ensuite une DCT inverse. Le concept intéressant dans cette méthode, c'est le fait que chaque voie possède un coefficient d'énergie du watermaking différent. En fait, ces coefficients vont être réglés en fonction de l'efficacité relative du spectre lumineux. Soit la courbe suivante :



On tire de cette courbe les relations suivantes :

$$AlphaR + AlphaG + AlphaB = AlphaRGB$$
$$AlphaR / AlphaG = E(LanbdaG) / E(LanbdaR) = 1.89$$
$$AlphaB / AlphaG = E(LanbdaG) / E(LanbdaB) = 10.48$$

La détection du watermark :

On commence par appliquer une DCT à chacune des voies de l'image I' dont on pense qu'elle a été marquée. Puis on fait la traditionnelle mise en zigzag des coefficients. On calcul ensuite la corrélation totale *RhoRGB = RhoR + RhoG + RhoB* issue du calcul des différentes corrélations *RhoR, RhoG, RhoB* entre les coefficients *V'r, V'g, V'b* et le marquage *X*. On compare ensuite *RhoRGB* et un seuil global *Trgb* calculé sur l'image. Si les deux valeurs sont suffisamment proches alors on peut en conclure que l'image a été marquée.

Marquage sur les bits de poids faibles

Il s'agit là très certainement de la méthode la plus simple de *data hiding*[170] sur une image. Imaginons que l'on travaille sur une image en niveaux de gris (pour les images en couleurs, il suffit de travailler sur la luminance), et que l'on ait seulement 256 niveaux de gris possibles (de 0 à 255). On considère qu'entre 2 niveaux de gris consécutifs l'œil humain ne fait pas la différence (en fait, cela dépend des niveaux de gris ou l'on se situe, mais nous verrons cela un peu plus loin). Si l'on considère le niveau de gris en binaire, nous sommes en présence de 8 bits (<=> 256). Le changement du dernier de ces bits (*le bit de poids faible*) ne change le niveau de gris que de 1 unité (quasi imperceptible à l'œil). On peut donc raisonnablement considérer que ce dernier bit n'est pas important, donc que l'on peut y mettre ce que l'on veut. Et c'est ce que l'on fait, on prend une image en 2 couleurs (1 bit) et on la place sur le bit de poids faible. Ça y est votre image est dissimulée.

Bon, il faut avouer que cette méthode présente de nombreux problèmes (en tout cas présentée de cette façon). En effet, il est très simple d'enlever ce marquage en mettant par exemple à 0 tous les bits de poids faible. De plus, tous les « nettoyages » de l'image ou les filtres sont radicaux pour ce marquage. Par exemple, la compression JPEG ne lui laisse quasiment aucune chance (voir les *attaques* plus haut). De plus, le système visuel humain peut être sensible à ces petits changements.

En effet, l'œil humain réagit de façon différente selon les contrastes. Ainsi, il est très sensible aux contrastes dans les gris de faibles intensités et beaucoup moins dans les teintes proches du blanc. Ainsi, certaines méthodes profitent de cela en adaptant le nombre de bits de poids faibles à coder en fonction de la teinte en cours et de la teinte adjacente (tout en se référant à des données physiologiques sur les couleurs).

[170] Le data-hiding regroupe un ensemble de techniques qui permettent de dissimuler des données dans un document quel qu'il soit (texte, image, vidéo…). Il est divisé en deux techniques principales : la stéganographie et le watermarking.

Malgré ses faiblesses de nombreuses méthodes dérivent de ce principe, bien que ce type de marquage soit de moins en moins à la mode.

Les images .GIF (par *Compuserve*) sont le lieu d'une méthode de stéganographie bien particulière. En effet, dans les .GIF on commence par définir une palette de 256 couleurs prises sur 2^24 possibilités (2^8 pour le rouge, 2^8 pour le vert, 2^8 pour le bleu).

Dans un premier temps, on crée une copie de la palette. Mais cette copie est triée. Le tri de la palette s'effectue de façon à ce que la différence entre 2 couleurs l'une à côté de l'autre soit quasi imperceptible. Ce tri est plus délicat qu'il ne peut y sembler au premier abord. En effet, un simple tri sur la luminance ne donne pas de bons résultats.

À partir de cela, voici comment l'on procède pour introduire l'image :

– on balaye toute l'image et pour chaque pixel on procède la manière suivante :

– on cherche l'index du pixel dans la palette triée.

– on regarde quel bit l'on doit coder sur le pixel en cours (pour cela on se réfère à l'image en 2 couleurs qui va servir de masque). Et l'on met ce bit sur le bit de moindre importance de l'octet en cours (celui de l'index de la palette triée).

Ainsi, on se décale ou non de 1 index dans la palette triée. Si la palette est bien triée alors la différence entre les deux couleurs va être imperceptible.

– Ce nouvel index dans la palette triée correspond à un index dans la palette non triée. On remplace alors le pixel en cours par l'index de la palette non triée, et ainsi de suite pour tous les pixels...

Pour retrouver l'image marquée, on procède de la façon suivante :

– on cherche l'index du pixel en cours dans la palette triée.

– le bit de poids le plus faible de cet index vient du masque appliqué sur l'image.

Cette méthode est une sorte de généralisation du marquage sur le bit de poids faible aux images indexées (c'est-à-dire qui ont une palette ou chaque pixel se réfère, contrairement aux images *true color* ou chaque pixel à ses propres composantes RGB).

De plus, ce marquage dépend réellement du format de l'image que l'on veut marquer. En effet, cette méthode ne peut s'appliquer à des formats tels que le GIF (de *Compuserve*). Ici les couleurs des pixels ne sont pas indépendantes, mais codées selon une palette de 256 couleurs. Je m'explique : on donne une valeur comprise entre 0 et 255 à chaque pixel et lorsque l'on lit les pixels, on se réfère à la palette pour y mettre la couleur. Cela signifie que si l'on s'amuse à changer le bit de poids faible des pixels on peut changer complètement de couleurs.

Ex :

11111111 <=> 255 : et la couleur 255 est définie comme étant un rouge vif.

11111110 <=> 254 : et la couleur 254 est définie comme étant un bleu foncé.

Si l'on ne modifie que le dernier bit, on détruit complètement l'image...

Comment remédier à ce problème ? Il existe plusieurs solutions pour marquer les palettes. La plus basique consiste à n'utiliser que 128 couleurs et à créer une palette où les couleurs marchent par pairs :

couleur 00 : Rouge=150, Vert=12, Bleu=59
couleur 01 : Rouge=152, Vert=10, Bleu=50
couleur 10 : Rouge=50, Vert=200, Bleu=98
couleur 11 : Rouge=50, Vert=212, Bleu=95

En ne changeant que le bit de poids faible des pixels, on reste quasiment sur la même couleur. En théorie, on pourrait même mettre deux fois exactement la même couleur à la suite, mais cela serait vraiment trop voyant...

On pourrait ainsi mettre 2 bits par pixel en se limitant à une palette de 64 couleurs...

Signature par modulation d'amplitude sur les images couleur

Cette méthode à été proposée en 1998 par Martin Kutter. Elle repose essentiellement sur des arguments statistiques.

Nous travaillons ici sur des images en couleurs (Rouge, Vert, Bleu). Nous savons que le but du marquage est (entre autres) d'être invisible pour l'œil humain. C'est pour cette raison que nous allons appliquer la signature uniquement sur la composante bleue de l'image, car c'est au bleu que l'œil est le moins sensible. De plus, nous utilisons un générateur pseudo-aléatoire pour nous générer une succession de positions au sein de l'image à marquer *I*. Ces positions représentent les positions où vont avoir lieu les marquages, et servent donc en l'occurrence de clef secrète *K* pour retrouver la signature. Pour chacun des pixels de la clef (situés en i,j) on applique la transformation suivante :

$Blue(i,j)=Blue(i,j)+(2*s-1)*L(i,j)*q$

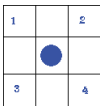
Avec :

$L(i,j)=0.299*Red(i,j)+0.587*Green(i,j)+0.114*Blue(i,j)$ (c'est la luminance !)

s : le bit à coder.

q : une constante qui représente la force du marquage.

Pour retrouver le bit qui a été marqué, nous avons besoin de prédire la valeur du pixel d'origine. Pour cela nous partons du principe bien connu que la valeur d'un pixel dépend de celle de ses voisins. Ici nous nous limitons à une interpolation linéaire avec ses plus proches voisins. Ainsi, on interpole la valeur du pixel en faisant tout simplement la moyenne des 4 pixels (on se limite toujours à la composante bleue) situés comme indiqué sur l'image suivante :



On mesure alors la différence entre la valeur du pixel courant et celle du pixel interpolé, et si cette dernière est trop importante, on peut considérer que le pixel a été marqué.

Bien que cela marche souvent, il est nécessaire d'augmenter les performances de cet algorithme. C'est pour cela que l'on tatoue le même bit à plusieurs endroits. C'est l'ensemble des positions de marquage de ce bit qui va jouer le rôle de clef secrète *K*. Notre but, est de ne plus être tributaire de facteur comme la taille de l'image. Pour cela, on définit une valeur de densité de marquage variant de 0 à 1, qui va donner la probabilité pour que l'on marque un pixel. Ainsi, pour chaque pixel on regarde de façon aléatoire si l'on doit marquer le pixel ou non. Si la densité vaut 0 alors aucun pixel ne sera marqué et inversement si la densité vaut 1, tous les pixels seront marqués. On parcourt ensuite l'image en zigzag pour s'affranchir de la taille de celle-ci.

On fait la somme des différences des pixels trouvés avec ceux interpolés, et l'on renormalise cela par le nombre de pixels de l'image en cours (qui peut alors être différent de celui de l'image d'origine) multiplié par la densité de pixels à marquer. En fait, ce produit correspond au nombre moyen de pixels marqués en tenant compte de la densité de probabilité de marquage. C'est ce résultat qui va nous dire si l'image a été marquée ou non.

Watermarking par DCT à taille de blocs variable

Dans cette méthode O-Hyung Kwon, Young-Sik Kim et Rae-Hong Park proposent une variante pour l'intégration du watermark dans les coefficients de la DCT de l'image d'origine. Comme d'habitude, on considère une séquence pseudo-aléatoire $W=[w1,w2,...,wM]$ représentant le tatouage (distribution normale, moyenne à zéro, variance de 1...). L'idée principale de cette méthode est la suivante : on utilise l'image originale dans le domaine spatial pour déterminer les blocs de contours, et les blocs de « non-contours ». Par défaut la DCT se fait sur des blocs de dimension N*N (N étant une puissance de 2 pour

la FFT[171]). Mais dans cette méthode on subdivise le bloc en 4 (la division de N par 2 permet de rester une puissance de 2), si au cours du traitement dans le domaine spatial nous nous sommes aperçus que nous avions à faire à un bloc de contour. Il reste bien sûr à déterminer ce qu'est un bloc de contour et un bloc de « non-contour ». Pour cela, on s'intéresse aux composantes fréquentielles. Et l'on classe les blocs selon la relation suivante :

Bloc contour <=> *Variance^2 >= Seuil*

Bloc non-contour <=> *Variance^2 < Seuil*

Si le bloc n'est pas un contour, on le remplace en entier par sa valeur moyenne, sinon on le découpe en 4 blocs de dimensions N/2*N/2, et l'on recommence. On obtient alors l'image *I'h*.

On procède ensuite de la façon suivante :

– Calcul de la DCT de *I(x,y)* (image d'origine) => *I'(u,v)*.

– Calcul de la DCT de *Ih(x,y)* (image traitée en blocs) => *I'h(u,v)*.

– Pour chaque bloc de *I'h(u,v)* on ne conserve que la valeur *M* la plus importante de la DCT, ce qui nous donne *Lh* (comme une sorte de filtre non linéaire maximum dans l'espace fréquentiel).

On incorpore ensuite le watermarking par la formule suivante :

I'wk = I'k(Lh,k)(1+Alpha*wk)*

Avec Alpha qui détermine la force du watermaking. On effectue enfin une IDCT (Inverse Discret Cosinus Transform) sur *I'w(u,v)* ce qui nous donne l'image marquée *Iw(x,y)*.

Processus de détection :

Pour vérifier si une image à été marquée voici comment l'on procède:

– On recherche *Lh* à partir de l'image originale.

– On effectue la DCT de l'image à vérifier => *Icw*.

– On extrait le possible tatouage *W'c* par la formule suivante :

$$W'ck = \frac{I'cw(Lh,k) - I(Lh,k)}{Alpha * I(Lh,k)}$$

Il suffit ensuite de mesurer la ressemblance du watermark supposé *W'c* et du watermark original *W*. Et ainsi, on peut savoir si l'image a été marquée.

Un regard sur la seconde génération de watermarking

Pour créer un marquage (watermarking) robuste, le tatouage doit être placé dans les endroits ou les données sont importantes. La seconde génération de watermarking va encore plus loin dans cette direction en se proposant de tenir compte des caractéristiques géométriques des images (ou des films). Par exemple, dans une image, ces caractéristiques peuvent être les bordures, les coins, les textures... Il faut malgré tout faire attention, car toutes les caractéristiques ne sont pas forcément bonnes à prendre en considération. Ainsi, il faut que, si possible, elles aient les propriétés suivantes :

– Invariance au bruit (compression non conservative, etc.), il faut donc sélectionner uniquement les caractéristiques significatives.

– Covariance aux transformations géométriques.

– Localisation (c'est-à-dire que le recadrage ne doit pas altérer les caractéristiques restantes).

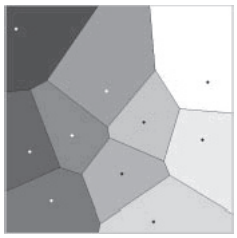
On peut remarquer tout de suite que ce genre de recherches rejoint les techniques utilisées dans la reconnaissance de formes.

[171] Le calcul numérique d'une transformation de Fourier prend énormément de temps, ce qui la rendait très peu exploitable à ses débuts. Une autre façon d'effectuer ce calcul a été inventée et a permis de la rendre accessible (en fait il s'agit réellement d'une petite révolution) au commun des mortels. C'est ce que l'on appelle la FFT (*Fast Fourier Transform*).

Ainsi M.Kutter, S.K. Bhattacharjee et T. Ebrahimi proposent dans une de leurs publications un exemple de watermarking de seconde génération.

– Dans un premier temps, ils recherchent des points caractéristiques de l'image. Il existe de nombreuses méthodes pour trouver ce genre de points (comme celles du *tracking*, directement venues du traitement d'images ou de la reconnaissance de formes). Dans leur exemple, ils ont choisi une décomposition de l'image par l'utilisation d'ondelettes de type « chapeau-mexicain ». Il est intéressant de remarquer ici, que dans le cas d'un watermarking de seconde génération la robustesse du marquage face aux diverses transformations repose en grande partie sur la stabilité des points caractéristiques (c'est-à-dire retrouver toujours les mêmes points quels que soient les transformations infligées à l'image).

– Dans une seconde partie, ils segmentent l'image par l'algorithme des diagrammes de Voronoï[172], en prenant comme base les points trouvés précédemment. Pour ceux qui ne sont pas habitués à tous les termes, une segmentation, c'est tout simplement un découpage de l'image en différentes régions qui sont étiquetées. Le résultat obtenu est le suivant :



– On passe ensuite au marquage proprement dit. C'est-à-dire que l'on va marquer chacune des régions trouvées précédemment. Dans leur exemple, ils utilisent la modulation d'amplitude sur la composante bleue. Ce watermarking est appliqué sur chacune des régions.

Il est intéressant à ce niveau de revenir en arrière pour se rendre compte de l'utilité de cette méthode. En effet, avec cette méthode on remarque que le watermarking est lié aux points les plus importants de l'image. Donc si l'attaque porte sur ces points, il est vrai que le watermarking va disparaître, mais l'image perdra complètement de sa valeur, car ses caractéristiques les plus importantes auront été altérées.

Watermarking par modification géométrique

Ces méthodes marquages sont relativement nouvelles et sont assez différentes de tous les marquages reposant sur des pseudo-bruits ajoutés à l'image. En effet, ici il ne va pas y avoir de petits changements au niveau des couleurs, mais au niveau des particularités géométriques de l'image. Le tatouage est formé par des pixels placés de façon particulière (telle qu'une collection de lignes). Ainsi, la méthode de tatouage proposée par M.J.J.J.B. Maes et C.W.A.M. van Overveld passe par 3 étapes :

– On détermine le tatouage comme étant un ensemble de pixels choisis pseudo-aléatoirement. Par exemple, on peut prendre une collection de lignes. Nous devons malgré tout nous attacher à un détail très important, il faut que la collection de lignes soit dense. Cela signifie qu'un grand nombre de pixels (au moins 50 %) de l'image à marquer doivent se trouver dans le voisinage d'une ligne (si l'on superpose le tatouage sur l'image).

[172] Les diagrammes de Voronoï sont des structures très utiles, rencontrées fréquemment car elles permettent de représenter des relations de distance entre objets et des phénomènes de croissance : il n'est pas étonnant de les voir utilisés pour modéliser des cristaux ou les grandes structures de l'univers, et de les trouver souvent dans la nature, par exemple sur la carapace d'une tortue ou sur le cou d'une girafe réticulée. Les diagrammes de Voronoï sont aussi des structures de données permettant de résoudre de nombreux problèmes : recherche de plus proches voisins et planification de mouvements notamment. L'étude des diagrammes de Voronoï, de leurs propriétés mathématiques, de leur calcul et de leurs nombreuses variantes a été, et reste, un sujet d'importance majeure de la géométrie algorithmique. Les contributions du projet *Prisme* portent sur les aspects combinatoires et algorithmiques, l'extension à différentes métriques non euclidiennes et l'application aux problèmes de reconstruction de formes

– On divise l'image en un certain nombre de blocs et l'on cherche un nombre fixé de points les plus significatifs (appelés aussi points saillants) dans chacun des blocs. La détermination des points saillants peut se faire de différentes façons comme par exemple en utilisant un filtre de détection des frontières. Appelons S l'ensemble de ces pixels.

– On introduit une déformation petite, locale, et géométrique sur l'image, de façon à ce qu'une grande partie de S soit déplacée à l'intérieur du voisinage des lignes.

Nous pouvons maintenant passer à la détection de ce marquage.

– On commence par redéterminer un ensemble S' de points saillant (avec card(S) = card(S')) par la même méthode que celle utilisée lors du marquage.

– On met ces points sur l'ensemble des lignes du tatouage. Si un pourcentage important de ces points appartient au voisinage des lignes, c'est que l'image à été marquée.

Le problème de cette méthode, c'est qu'il faut faire attention à ce que la déformation ne crée pas trop de nouveaux points saillants.

Un jeune informaticien, Niels Provos a réalisé un logiciel de détection de stéganographie, *Stegdetect*, dans les images JPEG. Le logiciel fonctionne de manière distribuée sur plusieurs machines et utilise des attaques par dictionnaire sur les images. Il a amélioré les techniques d'intégration de stéganographie dans les images et l'a implémenté dans *Outguess*, le principal logiciel libre de stéganographie sur Internet, dont il est l'auteur. Cependant, une récente loi américaine interdit l'usage de la stéganographie dans plusieurs États, compte tenu de la complexité d'analyser les millions d'images circulant sur Internet.

Une image dans une image ?

Pour en terminer sur la stéganographie, nous allons détailler le fonctionnement d'un programme permettant de cacher une image dans une autre. Bien sûr, un texte peut aussi être caché de cette façon, il suffit simplement qu'il soit transformé lui-même en image ce qui ne pose aucun problème particulier.

Cette suite de programmes a été développée par : Julie Brat, Lucien Loiseau, Nicolas Jean, Thomas Vincent et Simon Thépot. Nous disons suite de programme, car en fait il est fourni un ensemble de trois programmes : StegaIn, StegaOut, StegaTools. Ces programmes sont écrits en C++[173] et le code source est disponible. Le tout est à compiler[174] et est prévu pour fonctionner sous *Linux*[175], mais les auteurs affirment qu'en compilant sous *Windows* il ne devrait pas y avoir de problème particulier.

– *StegaIn* permet, au moyen d'une clé, de cacher un (ou plusieurs) fichier dans un fichier : des images au format BMP, du son au format Wav ou mp3, à peu près ce que vous voulez tant que vous connaissez précisément la structure du fichier.

[173] Langage de programmation, le langage C++ est une « amélioration » du langage C (le langage C a été mis au point par M.Ritchie et B.W.Kernighan au début des années 70). Bjarne Stroustrup, un ingénieur considéré comme l'inventeur du C++, a en effet décidé d'ajouter au langage C les propriétés de l'approche *orientée objet*. Ainsi, vers la fin des années 80 un nouveau langage, baptisé *C with classes* (traduisez « C avec des classes »), apparaît. Celui-ci a ensuite été renommé en C++, clin d'œil au symbole d'incrémentation ++ du langage C, afin de signaler qu'il s'agit d'un langage C amélioré (langage C+1).

[174] En informatique, la compilation est le travail réalisé par un *compilateur* qui consiste à transformer un code source lisible par un humain en un fichier binaire exécutable par une machine.

[175] Au sens strict, *Linux* est le nom du noyau de système d'exploitation libre, multitâche, multiplate-forme et multi-utilisateur de type UNIX créé par Linus Torvalds, souvent désigné comme le *noyau Linux*. Par extension, *Linux* désigne couramment le système d'exploitation libre combinant le noyau et un ensemble d'utilitaires système. Pour désigner cet ensemble, la *Free Software Foundation* (FSF) soutient la désignation GNU/Linux afin de rappeler que le noyau *Linux* est généralement distribué avec de nombreux logiciels ainsi que l'infrastructure du projet GNU. Pour l'utilisateur final, *Linux* se présente sous la forme d'une *distribution Linux*, c'est-à-dire du système d'exploitation accompagné d'une collection de logiciels très variés. Originellement développé pour les compatibles PC, *Linux* est utilisé sur tout type de matériel, du téléphone portable au superordinateur. Son premier marché est celui des serveurs informatiques, suivi par les systèmes embarqués.

– *StegaOut* permet d'extraire d'un fichier un (ou plusieurs) fichier grâce à une clé.
– *StegaTools* permet de simplifier la tâche de l'utilisateur pour chercher la clé adéquate.

L'utilisation de StegaIn et de StegaOut nécessite de bien comprendre leur principe de fonctionnement. C'est pourquoi, avant d'expliquer comment utiliser ces deux programmes, nous allons d'abord expliquer comment ils fonctionnent.

Que fait StegaIn ?

StegaIn permet de cacher un ou plusieurs fichiers dans un fichier. Prenons exemple pour une image BMP[176]. Sans rentrer dans les détails d'un fichier BMP, il faut juste savoir qu'un BMP est constitué de 2 parties :
– les informations du fichier (qu'il ne faut pas toucher)
– un tableau de pixel (que nous allons modifier pour stocker les fichiers)
Dans un BMP 32 bits, chaque pixel est codé sur 4 octets suivant ce schéma :
– 1 octet pour le bleu
– 1 octet pour le vert
– 1 octet pour le rouge
– 1 octet réservé
On a donc pour chaque pixel, 255 nuances de rouge, 255 nuances de vert et 255 nuances de bleu, comme nous l'avons déjà vu plus haut. Or à l'œil nu, la différence de couleur entre la 254e nuance et la 255e est invisible que ce soit pour le bleu, le vert ou le rouge.
Exemples :

	réservé	R(ouge)	V(ert)	B(leu)
pixel 1 :	XXXXXXXX	11111110	11111110	11111110
pixel 2 :	XXXXXXXX	11111111	11111111	11111111

À l'œil nu, le pixel 1 et le pixel 2 seront identiques, pourtant ils sont différents.
Cela signifie que l'on peut modifier tous les bits de poids faible (le plus à droite) de l'image sans altérer cette dernière.
Application : si on veut dissimuler le caractère « A », on prend sa représentation en binaire : 01000001 (65 en décimal) et on stock chaque bit sur 8 octets (sans toucher aux octets réservés pour garantir l'intégrité de l'image originale).

	réservé	R(ouge)	V(ert)	B(leu)
pixel 1 :	XXXXXXXX	XXXXXXX0	XXXXXXX1	XXXXXXX0
pixel 2 :	XXXXXXXX	XXXXXXX0	XXXXXXX0	XXXXXXX0
pixel 3 :	XXXXXXXX	XXXXXXX0	XXXXXXX1	...

On a donc une méthode très efficace qui permet de stocker un fichier quelconque dans une image. Cela dit avec cette méthode (en changeant simplement le bit de poids faible) il y a quatre inconvénients majeurs :
– il faut utiliser 10 octets de l'image pour stocker 1 seul octet du fichier à cacher.
– tout le monde connaît cette technique il est donc très facile de retrouver le fichier.

[176] BMP, acronyme de *Bitmap*, est un format d'image numérique ouvert développé par *Microsoft* et *IBM*. C'est un des formats d'images les plus simples à développer et à utiliser pour programmer. Il est lisible par quasiment tous les visualiseurs et éditeurs d'images. Il s'agit d'images matricielles

– ce n'est pas un algorithme très portable entre les différents types de fichiers BMP.
– on aimerait peut-être stocker des fichiers dans autre chose que des images BMP.

Aussi pour pallier à ce problème les auteurs ont mis en place un principe de masque, que nous allons détailler ci-dessous.

Les masques

Un masque est un octet qui n'a pas pour but de représenter une information (un nombre, un caractère) mais de masquer les bits inintéressants d'un autre octet en effectuant une opération logique bit à bit (dans notre cas l'opérateur &).

L'opérateur logique & permet de comparer 2 bits et rend 1 si, et seulement si, les deux bits sont à 1.

A	B	A & B
0	0	0
0	1	0
1	0	0
1	1	1

Exemples avec des octets :

		Exemple 1	Exemple 2	Exemple 3
Octet	11010101	11000101	00110101	00011101
Masque	00010000	00000010	00100100	00100100
Octet & Masque	00010000	00000000	00100100	000000100

Extension de la théorie

Revenons à notre stéganographie. Notre but est de cacher un fichier dans une image (par exemple). En possession des masques, nous allons pouvoir avoir une approche différente de la situation. Le but n'est plus de modifier uniquement le dernier bit, 3 octets sur 4 (pour ne pas toucher au réservé) mais d'appliquer à chaque octet un masque, qui spécifiera quels bits seront à modifier. Par exemple si le masque est 00000101 (5 en décimal) on modifiera non plus le dernier, mais le 6^{e} et le 8^{e} bit de chaque octet.

On peut même augmenter le contrôle en appliquant non pas un seul masque, mais plusieurs masques. C'est ce qui fait la force de *StegaIn*, la possibilité de rentrer une liste de masques. Si vous rentrez une liste de 3 masques par exemple, alors le programme modifiera :

– le 1er octet en fonction du 1er masque
– le 2^{e} octet en fonction du 2^{e} masque
– le 3^{e} octet en fonction du 3^{e} masque
– le 4^{e} octet en fonction du 1er masque
– le 5^{e} octet en fonction du 2^{e} masque
etc..

Exemple :

On rentre la chaîne de masque (en décimal) suivante 0:1:2:5 et on tente de stocker « A » dans un fichier image : Rappelons que :

A = 01000010
0 = 00000000
1 = 00000001
2 = 00000010
5 = 00000101

octet 1 : XXXXXXXX <--- on applique le masque 1 c'est-à-dire 0
octet 2 : XXXXXXX0 <--- on applique le masque 2 c'est-à-dire 1
octet 3 : XXXXXX1X <--- on applique le masque 3 c'est-à-dire 2
octet 4 : XXXXX0X0 <--- on applique le masque 4 c'est-à-dire 5
octet 5 : XXXXXXXX <--- on applique le masque 1 c'est-à-dire 0
octet 6 : XXXXXXX0 <--- on applique le masque 2 c'est-à-dire 1
octet 7 : XXXXXX0X <--- on applique le masque 3 c'est-à-dire 2
octet 8 : XXXXX1X0 <--- on applique le masque 4 c'est-à-dire 5

Ceci est extrêmement puissant, car le masque peut être aussi long que l'on veut (on peut très bien par exemple faire 0:1:2:4:0:1:1:1:0:4:6:2:0:1:2:1...) Avantages :

– on peut choisir de stocker un peu plus d'information sur chaque octet au détriment de la qualité du fichier original.

– il devient plus difficile en fonction du masque de retrouver le fichier.

– si on connaît bien la structure du fichier, on peut lui appliquer un masque adéquat.

Afin de le rendre un peu plus portable, on peut également ajouter un « *seek* ». La plupart des structures de fichiers possèdent des « *headers* » contenant des informations sur le fichier. Ainsi, pour une image BMP, les 54 premiers octets sont importants (on y trouve notamment la taille du fichier en octets, un offset pour l'accès aux données, le nombre de bits par pixels dans l'image, le type de compression utilisé, le nombre de couleurs dans la palette, la largeur et la longueur de l'image, etc.), et on ne doit pas y toucher sinon on risquerait de fausser l'affichage, pour un fichier WAV[177], l'en-tête commence dès le premier octet (offset 0). Il a une taille de 44 octets, et est constitué des champs suivants (listés dans l'ordre) :

TAG1	(4 octets) : Constante « RIFF[178] »	(0x52,0x49,0x46,0x46)
SIZE1	(4 octets) : Taille du fichier moins 8 octets	
TAG2	(8 octets) : Identifiant « WAVEfmt »	(0x57,0x41,0x56,0x45,0x66,0x6D,0x74,0x20)
LGDEF	(4 octets) : Nombre d'octets utilisés pour définir en détail le contenu	
FORMAT	(2 octets) : Format de fichier (1: PCM, ...)	
NBCANAUX	(2 octets) : Nombre de canaux (1 pour mono ou 2 pour stéréo)	
FREQ	(4 octets) : Fréquence d'échantillonnage (en Hertz)	
BYTEPERSEC	(4 octets) : Nombre d'octets par seconde de musique	
NBRBYTE	(2 octets) : Nombre d'octets par échantillon	
NBBITS	(2 octets) : Nombre de bits par donnée	
TAG3	(4 octets) : Constante « data »	(0x64,0x61,0x74,0x61)
SIZE2	(4 octets) : Taille du fichier moins 44 octets	

On ne devra donc en aucun cas toucher aux 54 premiers octets.

C'est pourquoi il convient de rajouter un entier que nous appellerons *Seek* qui précisera à combien d'octets doit avancer le curseur (pointeur de fichier) par rapport à la position courante (position du curseur à un moment donné) avant de commencer à cacher le fichier.

Avec tous ces outils en mains, nous pouvons par exemple refaire la 1re technique de stéganographie, c'est à dire changer le bit de poids faible 3 octets sur 4 afin de ne pas modifier le réservé. Pour cela il suffit de prendre un *Seek* = 54 et un masque = 1:1:1:0

[177] WAV (ou WAVE), une contraction de *WAVEform audio format*, est un standard pour stocker l'audio digital de *Microsoft* et IBM. C'est le format le plus courant pour l'audio non compressé sur les plates-formes de *Microsoft*, mais il est bien courant sur les systèmes *GNU/Linux* aussi.

[178] Le *Resource Interchange File Format* (RIFF), est un ensemble de spécifications définies par *Microsoft* pour les fichiers multimedia intégrant des identificateurs pour chacun de leurs éléments (son, vidéo, etc.). Les fichiers WAV, AVI, RMI, CDA Compact Disc Audio track et PAL sont tous conformes aux spécifications RIFF.

Utilisation de StegaIn et StegaOut

Syntaxe de *StegaIn* : La syntaxe de *StegaIn* est la suivante :

./StegaIn fic0 Cle1 fichier1 Cle2 fichier2 .....

– fic0 : c'est le fichier où nous allons cacher les autres fichiers (pas nécessairement une image)

– Cle : La clé est une composante de 2 informations, un *Seek* et une liste de masque sous la forme Seek:ListeMask

– o seek : déplacement du curseur depuis sa position courante à position courante + seek (position courante = 0 au début)

– o Listmask : liste de masque permettant de cacher le fichier. ListMask de la forme M1:M2:...Mn, n masques où chaque masque est compris entre 0 et 255 inclus. En somme, une clé se présente sous la forme Seek :n1:n2:n3:....

– fichier : fichier à cacher en fonction de la clé.

StegaIn va créer un nouveau fichier qui portera le même nom que l'original + new et va renvoyer pour chaque fichier caché une nouvelle clé permettant de le retrouver

fichier0new :

– fichier : Seek:ListMask:SeekFin

– le Seek de cette dernière clé est la position de début du fichier à cacher dans le fic0

– la ListMask est la même que celle rentrée pour le cacher

– le SeekFin est la position du dernier octet du fichier à cacher dans le fic0.

Cette dernière clé est indispensable pour retrouver le(s) fichier(s) dans leurs intégralité(s) avec *StegaOut*.

Syntaxe de *StegaOut* : La syntaxe de *StegaOut* est la suivante :

./StegaOut Cle1 fichier1 Cle2 fichier2....

– fic0new : c'est le fichier où nous allons récupérer les fichiers cachés.

– Cle : Comme vu précédemment, la Cle est de la forme Seek:ListMask:SeekFin

– o Seek : déplacement du curseur depuis le début du fichier à Seek

– o ListMask : liste de masque permettant de récupérer le fichier. ListMask de la forme M1:M2:... Mn, n où chaque masque est compris entre 0 et 255 inclus.

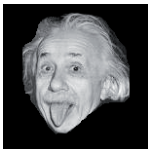
– o seekfin1 : lorsque le curseur atteint SeekFin, cela signifie (sauf erreur) qu'il a fini de récupérer le fichier

– fichier : nom du fichier caché (attention, s'il porte le même nom qu'un autre fichier, ce dernier sera écrasé).

StegaOut renvoie à titre d'information la taille du fichier récupéré.

– taille du fichier = XXXX octets

Application

Nous nous proposons de cacher cette image :  dans celle-ci :

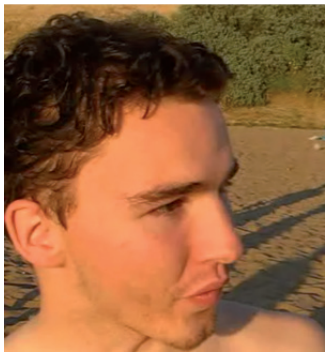
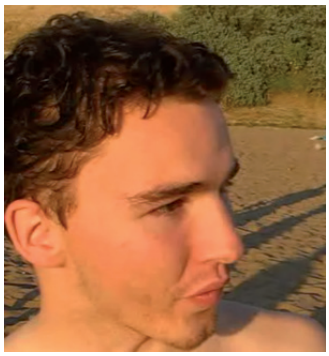


Image originale

Avec un masque de valeur : 1:1:1:0, (modification d'un seul bit, le 8e, de poids faible) nous obtenons l'image ci-dessous :

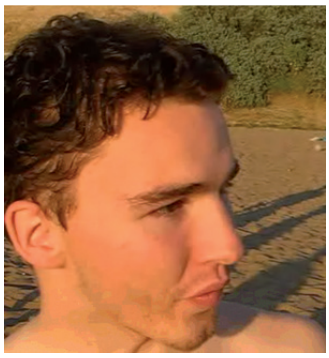


masque = 1:1:1:0

Si nous avions modifié le bit de poids fort, le 1er, en appliquant le masque devaleur:128:128:128:0, nous aurions obtenu cette image :

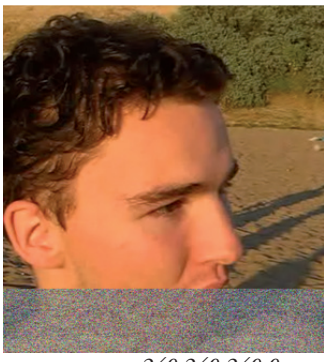
masque = 128:128:128:0

Avec une modification de 4 bits sur celle de gauche le 8,7,6 et 5e et sur celle de droite le 1,2,3 et 4e on obtient ces images :



masque = 15:15:15:0

On observe, sur l'image de droite une forte dégradation, alors que sur celle de gauche, c'est à peine perceptible.



masque = 240:240:240:0

Nous pouvons observer dans les exemples ci-dessus l'importance du choix des paramètres du masque, mais aussi qu'il est parfaitement possible de cacher une image (ou un texte) dans une image « porteuse ».

Il existe de nombreuses autres méthodes de stéganographie basées sur l'utilisation des images numériques, ce qui complique la tâche des organisations de surveillance. Deux universitaires ont quant à eux scanné deux millions d'images sur *eBay*. Ils en ont certes trouvé 15 000 qui avaient été estampillées (la stéganographie servant aussi à copyrighter les images), mais aucune ne contenait de message secret. Seule certitude dans cette histoire : elle a tout du fait divers à sensation, et sert d'une part tous ceux qui luttent pour restreindre la liberté d'utiliser la cryptographie, d'autre part à la désinformation ambiante à même de générer les pires craintes et inquiétudes.

Un expert britannique aurait ainsi déclaré que la stéganographie représentait la troisième plus grosse crainte des États-Unis, juste après les attaques biologiques et chimiques. Un journaliste de *France Info*, quant à lui, avance qu'il faut « environ une semaine aux services secrets américains » pour venir à bout d'un message crypté, quand les cryptographes expérimentés parlent, eux, de plusieurs milliers d'années. Un autre rapporte que Mike Hayden, directeur de la National Security Agency, maître d'œuvre d'Eche-

lon, avança l'an passé que les technologies dont se servait ben Laden (la stéganographie...) dépassaient de beaucoup les capacités de son service de renseignement, alors même que la NSA se targue d'être à la tête de la plus formidable équipe qui soit de cryptographes, mathématiciens et autres scientifiques.

Reste que, pour pouvoir lire ce message caché, la personne recevant l'image doit connaître la clef permettant de lire les informations contenues dans celle-ci. Sans cette clef privée, il est impossible de lire le contenu caché, et l'image garde tout son mystère. La plupart du temps, le message est crypté, puis posté dans une image avant d'être envoyé. Ainsi, cryptographie et stéganographie sont complémentaires.

Cette technique présente un autre avantage : elle permet de passer outre les systèmes tels que *Carnivore*[179], censés repérer certains mots contenus dans les messages électroniques circulant sur le Net.

[179] Le *Wall Street Journal* du 11 juillet 2000 dévoile le programme *Carnivore* mis en place par le FBI depuis début 1999 afin de surveiller, à la volée, les communications électroniques de personnes suspectées de crimes. Carnivore est un programme installé sur une machine reliée dans les locaux d'un fournisseur d'accès (FAI). Il fonctionne comme un « sniffer » très spécialisé, capable de filtrer les paquets de données qui transitent entre l'utilisateur et le FAI et de reconstituer les messages échangés : courriers électroniques, mais aussi pages Web visitées, et conversations en direct (chats). Carnivore utilise des filtres pré-définis en fonction de la nature de l'écoute afin, par exemple, de n'intercepter le trafic qu'en provenance ou à destination d'un utilisateur donné. Mais ces filtres peuvent-être modifiés à distance à l'insu du FAI. Un membre du FBI est chargé de collecter quotidiennement les données. Avant Carnivore il y a eu *Etherpeek* puis *Omnivore* (1997) qui scannait 6 Go de données par heure. Carnivore serait moins rapide (quelques millions d'e-mails par seconde quand même !) mais est capable de reconstituer les pages Web et les cessions de discussion en ligne (les chats). Son coût de développement est estimé à 6,8 millions de francs. Carnivore devrait être adapté au protocole de téléphonie IP (VoIP) dans le cadre du projet nommé « *Dragon Net* ». Les conversations vocales privées transitant par l'Internet pourraient alors être écoutées.

La cryptographie

- 83 - ADJ JNA -
LMHNX WEKLM UERDS EVHLC JSQQK VLDES ANEVT YEDGI ZQDOD RMDKG
SXGSQ SHDQP VIEAP IENLI CLZCL LAGWC BJZD

- 149 - TLS CMU -
FTMKV DRJMG FBUDK LZCTR FLTUU IWVJL OYKYX GDCKJ TMDFB WNLZQ
JAXHP GGKFG SBZOQ KQKUK TINMH BAJOO AUILA QVFTK LSTMM XGAQL
CNHUW LFHKA ULTXT BIVIF EWWDY PUCNS TPJHR OBWHE KYUSB CANYC
W

- 167 - MRJ
KLIBM ERJAR WE SCTCH
NRNBL ZPEBH GUI UCBZN
ZTFJA EKOMU HT EMAVD
FXKAY MLWC

- 186 - DQ
PBNXA SMDA ZPT UNSWA
DDSTI GQQC HAS QYRWF
WVAVG CCUD CLUP GSWCL
MBCZS SYXPG MGMQX AUFUL NUZEQ HNHET ZZAKL C

- 195 - EHW TNH -
ABTWU GWDMP OGKMQ KBHGK HROUP RMYQY INHSA MWFBP CDQRG LDBFK
YNXPP DIQHE AOIFQ AOLRZ ZFPDJ MCGEC TAHHQ MVUYA JIAWM WSOYU
UTLEP AVZKG HJWCD LOQHW IMSTC LQDNP VCFCN FRUYR GSSJH ORQMU
IFFYU WYNTA XPYIX MYTEE FTDCV EHUOA DCPLM APCAU JJYUK

Les grandes dates de l'histoire de la cryptographie

DATE	COMMENTAIRES
1900 avant J.-C.	Un scribe égyptien a employé les hiéroglyphes non standards dans une inscription. David Kahn cite ceci comme le premier exemple documenté de cryptographie écrite.
1500 avant J.-C.	Une tablette de Mésopotamie contient une formule chiffrée pour la fabrication de vernis pour la poterie.
500-600 avant J.-C.	Des scribes hébreux, notant le livre de Jérémie, ont employé un chiffre simple de substitution, simple alphabet inversé, connu sous le nom d'ATBASH. (Jérémie a commencé à dicter à Baruch en 605 avant J.-C., mais les chapitres contenant ce peu de chiffre sont attribués à une source marquée « C' (pensé pour ne pas être de Baruch) qui pourrait être une écriture de rédacteur après l'exil babylonien en 587 avant J.-C., quelqu'un de contemporain de Baruch ou même de Jérémie lui-même. ATBASH était l'un des quelques chiffres hébreux de cette époque.
487 avant J.-C.	Les Grecs ont utilisé un dispositif appelé scytale – un bâton autour duquel une longue et mince bande de cuir a été enroulée et écrite dessus. La bande est déroulée et portée comme ceinture. Le destinataire avait un bâton identique. (note : Un article dans *Cryptologia* datant de 1998 dit que l'utilisation comme procédé cryptographique du scytale est peut-être un mythe. Nous pensons qu'il s'agit plutôt de stéganographie.
50-60 avant J.-C.	Jules César (100-44 avant J.-C.) a employé une substitution simple avec l'alphabet normal (décalant juste les lettres par quantité fixe) dans des communications de gouvernement. Ce chiffre était moins fort qu'ATBASH, mais à une époque où peu de gens savaient lire, il était assez bon. Il a également employé la translittération du latin dans les lettres grecques et un certain nombre d'autres chiffres simples. On dit qu'en fait c'était surtout pour gérer sa fortune qu'il employait ce système de cryptage.
0-400 ?	Le Kama Sutra de Vatsayana énumère la cryptographie dans le quarante-quatrième et le quarante-cinquième art (yoga) sur les 64 que les hommes et femmes devraient savoir et pratiquer. Dans cette liste d'arts, le quarante-quatrième et le quarante-cinquième sont : • L'art de l'écriture cachée et chiffrée, et l'écriture des mots d'une manière particulière. • L'art de parler en changeant les formes de mots. Il est de diverses sortes. Certains parlent en changeant le commencement et la fin des mots, d'autres en ajoutant les lettres inutiles entre chaque syllabe d'un mot, et ainsi de suite. Le verlan et le javanais ont repris ces méthodes.
200	Le Papyrus de Leyde utilise le chiffre pour cacher les parties cruciales de recettes magiques importantes.
725-790 ?	Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi a écrit un livre (maintenant perdu) sur la cryptographie, inspiré par sa solution d'un cryptogramme en grec pour l'empereur byzantin. Sa solution a été basée sur le texte clair (correctement deviné) connu au début de message – une méthode de cryptanalyse standard (mot probable), utilisée même pendant la 2e guerre mondiale contre les messages d'Enigma.
855	Abu Bakr Ahmad ben Ali ben Wahshiyya an-Nabati a édité plusieurs alphabets de chiffre qui ont été traditionnellement employés pour la magie.
1226	Dès 1226, une cryptographie politique, faible, est apparue dans les archives de Venise, où des points ou des croix ont remplacé les voyelles dans quelques mots.
environ 1250	Roger Bacon a non seulement décrit plusieurs chiffres mais a écrit : « Un homme est fou qui écrit un secret de n'importe quelle autre manière qu'une qui la cachera au vulgaire ».
1379	Gabrieli di Lavinde sur demande du pape Clément VII, a compilé un alphabet de substitution de combinaison et un petit code – le premier exemple de ce type trouvé par David Kahn. Cette classe de code/chiffre devait rester en général en usage parmi des diplomates et quelques civils pendant les 450 années à venir, malgré le fait que des chiffres plus forts furent inventés ensuite.
1300	Abd al-Rahman Ibn Khaldun écrit « *le Muqaddimah* », un aperçu substantiel de l'Histoire qui cite l'utilisation des « noms des parfums, des fruits, des oiseaux, ou des fleurs pour indiquer les lettres, ou des formes différentes des formes admises des lettres comme chiffre parmi des bureaux d'impôts et d'armée. Il inclut également une référence à la cryptanalyse, notant « des écritures bien connues sur le sujet sont en possession du peuple ».
1392	« *The Equatorie of the Planetis* », probablement écrit par Geoffrey Chaucer, contient des passages chiffrés. Le chiffre est une substitution simple avec des lettres, des chiffres et des symboles.

1412	Shihab al-Din abu l'Abbas Ahmad ben Ali ben Ahmad Abd Allah al-Qalqashandi a écrit « *Subh al-a sha* », une encyclopédie arabe en 14 volumes qui a inclus une section sur la cryptologie. Cette information a été attribuée à Taj ad-Din Ali ibn ad-Duraihim ben Muhammad ath-Tha alibi al-Mausili qui a vécu de 1312 à 1361 mais dont les écritures sur la cryptologie ont été perdues. La liste des chiffres de ce travail a inclus la substitution et la transposition et, pour la première fois, un chiffre avec les substitutions multiples pour chaque lettre de texte clair. En outre, on attribue à Ibn Al-Duraihim un exposé sur la cryptanalyse, y compris l'utilisation des tables des fréquences de lettre et des ensembles de lettres qui ne peuvent pas se produire ensemble dans un mot.
1466-7	Leon Battista Alberti (un ami de Leonardo Dato, un secrétaire pontifical qui pourrait avoir instruit Alberti à la cryptologie) a inventé et édité le premier chiffre polyalphabétique, concevant un disque de chiffre (connu de nous en tant que *Captain Midnigh Decoder Badge*) pour simplifier le processus. Cette classe de chiffre n'a pas été apparemment cassée avant le 18e siècle. Alberti a également employé un disque pour chiffrer. Ces systèmes étaient beaucoup plus forts que le *nomenclator* en service par les diplomates de l'époque et pendant des siècles de venir.
1473-1490	Un manuscrit par Arnaldus de Bruxella emploie cinq lignes de chiffre pour cacher la partie cruciale de l'opération d'alchimie pour fabriquer la pierre philosophale.
1518	Johannes Trithemius a écrit le premier livre imprimé sur la cryptologie. Il a inventé un chiffre stéganographique dans lequel chaque lettre a été représentée comme mot pris dans une succession des colonnes. La série résultante de mots serait une prière légitime. Il a également décrit des chiffres polyalphabétiques sous la forme maintenant standard de tables rectangulaires de substitution. Il a présenté la notion des alphabets changeants avec chaque lettre.
1553	Giovan Batista Belaso a présenté la notion d'employer un mot de passe comme clef pour un chiffre polyalphabétique répété. (c'est le *chiffre de Vigenère* mal nommé par la plupart des auteurs à ce jour.)
1563	Giovanni Battista Porta a écrit un texte sur des chiffres, présentant le chiffre digraphique. Il a classifié les chiffres en : transposition, substitution et substitution de symbole (utilisation d'un alphabet étrange). Il a suggéré l'utilisation des synonymes et des fautes d'orthographe pour embrouiller le cryptanalyste.
1564	Giovanni Battista Bellaso a édité un chiffre par mot-clé améliorant sur le travail de Gerolamo Cardano qui semble avoir inventé l'idée. Ce dernier est également associé à une méthode de stéganographie utilisant une grille à trous masquant une partie d'un texte pour révéler les mots utiles. Elle deviendra plus tard une méthode de cryptographie quand la grille sera être tournée d'un quart de tour (technique utilisée par exemple dans le roman *Mathias Sandorf* de Jules Verne).
1623	Monsieur Francis Bacon a décrit un chiffre qui porte maintenant son nom, connu aujourd'hui comme codage 5-bit binaire.
1585	Blaise de Vigenère a écrit un livre sur des chiffres, y compris les premiers systèmes authentiques de mot-clé de texte clair et de texte chiffré. Tous les deux ont été oubliés et ré inventés au 19e siècle. L'idée de mot-clé survit aujourd'hui dans les modes modes DES, CBC et de CFB.
1790	Thomas Jefferson, probablement aidé par Dr. Robert Patterson (un mathématicien à U. Penn.), invente sa roue à chiffrer. Ceci a été réinventé sous plusieurs formes plus tard et employé pendant la deuxième guerre mondiale par la marine des USA comme le système de chiffrement sous le nom de M-138-A.
1817	Colonel Decius Wadsworth a produit un disque adapté du précédent avec un nombre différent de lettres dans les alphabets clairs et de chiffres – ayant pour résultat un chiffre progressif dans lequel des alphabets sont employés irrégulièrement, selon le texte clair utilisé.
1854	Charles Wheatstone a inventé ce qui est devenu notoire comme *chiffre de Playfair*, du nom de son ami Lyon Playfair. Ce chiffre emploie un choix verrouillé de lettres pour faire un chiffre digraphique qu'il est facile d'employer sur le champ de bataille. Il a également réinventé et complété le dispositif de Wadsworth.
1857	L'amiral Sir Francis Beaufort utilise une variante du chiffre de Vigenère. Il a été édité par son frère, après sa mort sous forme de cartes de format 4x5 pouces.
1859	Pliny Earle Chase a édité la première description de fractionnement d'un chiffre.
1854	Charles Babbage semble avoir ré inventé la roue de chiffrement.
1861-1980	Une étude des brevets des États-Unis pour l'établissement du premier brevet cryptographique entre 1861 et 1980 a identifié 1.769 brevets qui sont principalement liés à la cryptographie.

1861	Friedrich W. Kasiski a édité un livre donnant la première solution générale d'un chiffre polyalphabétique avec mot de passe, de ce fait marquant la fin de plusieurs centaines d'années d'efforts pour casser le chiffre polyalphabétique.
1861-5	Pendant la guerre civile, probablement entre autres chiffres, l'Union a employé la substitution des mots choisis d'un dictionnaire de transposition de mots, tandis que la Confédération employait le chiffre de Vigenère (dont la solution avait été juste éditée par Kasiski).
1891	Le Major Étienne Bazeries invente sa version de roue chiffrante après que l'armée française l'ait rejetée ; il a divulgué son fonctionnement en 1901.
1913	Le Capitaine Parket Hitt a réinventé la roue de chiffrement, sous la forme de bande, menant au système M-138-A utilisé pendant la deuxième guerre mondiale
1916	Le Major Joseph O. Mauborgne invente le dispositif de chiffrement appelé M-94.
1917	William Frederick Friedman, est considéré comme étant le père de la cryptanalyse des USA (et homme qui a inventé ce terme), a été employé en tant que cryptanalyste civil (avec son épouse Élisabeth) aux laboratoires de Riverbank et a travaillé comme cryptanalyste pour le gouvernement des USA.
1917	Gilbert S. Vernam, travaillant pour la AT&T, a inventé une machine polyalphabétique pratique de chiffre capable d'employer une clef qui est totalement aléatoire et sans répétition : le masque jetable, « One-Time Pad ». Cette machine a été offerte au gouvernement pour l'usage dans la première guerre mondiale mais elle a été rejetée. Elle a été mise sur le marché en 1920. Son système a longtemps protégé le fameux « téléphone rouge », qui reliait la Maison Blanche au Kremlin.
1918	Le système d'ADFGVX a été mis en service par les Allemands à la fin de la première guerre mondiale. C'était un chiffre qui effectue une substitution (par une rangée verrouillée), le fractionnement et puis la transposition des fractions de lettres. Il fut cassé par un cryptanalyste français, le lieutenant Georges Painvin.
1919	Hugo Alexandre Koch dépose un brevet aux Pays-Bas sur une machine de chiffre basée sur un rotor. Il transfère ses propriétés industrielles en 1927 à Arthur Scherbius qui avait inventé et commercialisé la machine Enigma à partir de 1923.
1919	Arvid Gerhard Damm a déposé un brevet en Suède pour une machine mécanique de chiffre à rotor. Cette machine à servi de base au développement d'une famille des machines de chiffrement sous la direction de Boris César Wilhelm Hagelin qui était le seul des cryptographes commerciaux de cette période faisant des affaires prospères. Après la guerre, une loi suédoise ayant permis au gouvernement de s'approprier des inventions, Hagelin s'est installé à Zug, en Suisse et fondé Crypto AG. La compagnie existe encore, bien que faisant face à la polémique pour avoir affaibli prétendument un produit de chiffrement vendu à l'Iran.
1921	Edouard Hugh Hebern a créé « *Hebern Electric Code* », une compagnie faisant les machines électromécaniques de chiffre basées sur les rotors qui tournent, à la façon d'un odomètre, à chaque caractère chiffré.
1923	Scherbius de Arthur crée « *Chiffriermaschinen Aktiengesellschaft* » pour commercialiser sa machine Enigma.
1924	Alexander von Kryha produit sa machine de codage qui a était encore employée par les corps diplomatiques allemands, dans les années 50. Cependant, elle était cryptographiquement faible. Un cryptogramme d'essai de 1135 caractères a été résolu par les cryptanalystes des USA Friedman, Kullback, Rowlett et Sinkov en 2 heures et 41 minutes. Néanmoins, la machine a continué à être vendue et utilisée.
1927-33	Les utilisateurs de la cryptographie n'ont pas été seulement les banquiers, les amoureux, les chercheurs et autres légitimes. Il y avait également une poignée de criminels, « la plus grande ère de la contrebande internationale – la prohibition – a créé la plus grande ère du « criminel cryptologique ». À cette époque, le FBI dirige un bureau cryptanalytique pour traiter la cryptographie criminelle. Les systèmes des contrebandiers se sont développés et sont de plus en plus plus compliqués ; « certains sont d'une complexité jamais atteinte par n'importe quel gouvernement pour ses communications plus secrètes » a écrit Mme Friedman (Elizebeth Smith) dans un rapport au milieu des années 1930. À aucun moment, pendant la guerre mondiale, quand les méthodes secrètes de communication ont atteint leur développement le plus élevé, on n'a employé des ramifications impliquées telles que celles trouvée dans une partie de la correspondance des navires trafiquants de rhum sur la côte occidentale.

1929	Lester S. Hill publie « *Cryptography in an Algebraic Alphabet* » dans lequel un bloc de texte clair est chiffré par une opération matricielle.
1933-45	La machine Enigma n'était pas un succès commercial mais elle a été améliorée pour devenir le fer de lance cryptographique de l'Allemagne Nazie.
1937	La machine Purple japonaise a été inventée en réponse aux révélations faites par Herbert O. Yardley et cassée par une équipe dirigée par William Frederick Friedman. La machine Purple a utilisé des relais de téléphone au lieu des rotors et a ainsi eu une permutation totalement différente à chaque étape plutôt que les permutations relatives d'un rotor dans différentes positions.
les années 30	Kahn attribue le SIGABA américain (M-134-C) à William F. Friedman tandis que Deavours l'attribue à une idée de Frank Rowlett. SIGABA est une amélioration des inventions à rotors de Hebern et Scherbius en employant la progression pseudo-aléatoire des rotors multiples sur chaque étape chiffrante plutôt qu'une progression uniforme, façon odomètre. Il a également employé 15 rotors (10 pour la transformation de caractère, 5 probablement pour le contrôle de rotation) plutôt que 3 ou 4 dans Enigma.
les années 30	La machine britannique TYPEX était un dérivé de l'Enigma commerciale achetée par les Anglais pour l'étudier dans les années 20. C'était une machine à 5 rotors avec les deux rotors fixes, atteignant l'objectif du tableau de connexion de l'Enigma allemande.
1970	Dr. Horst Feistel a mené un projet de recherche au laboratoire de recherches d'IBM dans les années 60 qui ont développé le chiffre Lucifer. Ceci plus tard a inspiré le DES des USA (ci-dessous) et d'autres familles de chiffrement appelée chiffres de Feistel (*product cipher*).
1976	Une conception d'IBM, basé sur le chiffre de Lucifer et avec des changements et améliorations par la NSA, a été choisie pour être la base de chiffrement américaine des États-Unis. Elle a depuis lors trouvé l'acceptation mondiale, en grande partie parce qu'elle s'est montrée forte contre 20 années d'attaques.
1976	Whitfield Diffie et Martin Hellman ont édité « *New Directions in Cryptography* », présentant l'idée de la cryptographie à clé publique. Ils également ont mis en avant l'idée de l'authentification par la puissance d'une fonction à sens unique. Ils concluent par une observation : la compétence dans la cryptanalyse de production a toujours été fortement du côté des professionnels, mais l'innovation, en particulier dans la conception de nouveaux types de systèmes cryptographiques, est venue principalement des d'amateurs.
Avril 1977	Inspiré le commentaire de Diffie et Hellman et en agissant en tant que débutants complets dans la cryptographie, Ronald L. Rivest, Adi Shamir et Leonard M. Adleman avaient étudié comment faire un système principal à clé publique pratique. Pendant une nuit d'avril, Ron Rivest était étendu avec un fort mal de tête et l'algorithme de RSA lui est venu. Il l'a évalué puis transmis à Shamir et Adleman le lendemain matin. C'était un chiffre pratique à clef publique pour la confidentialité et les signatures numériques, basé sur la difficulté de factoriser de grands nombres. Ils ont soumis ceci à Martin Gardner la 4 avril pour la publication dans *The Scientific American* qui parut en septembre 1977.
1978	L'algorithme RSA a été édité dans les communications de l'ACM.
1984-5 ?	Le chiffre Rot13 a été présenté dans le logiciel de nouvelles *Usenet* pour permettre au chiffrage des « posts » afin d'empêcher les yeux innocents d'être assailli par des textes répréhensibles. C'est le premier exemple d'utilisation d'un chiffrement par clé connue de tous.
1990	Xuejia Lai et James Massey, en Suisse, ont publié « *Une proposition pour un nouveau standard de chiffrage de bloc* », International Data Encryption Algorithm (IDEA), pour remplacer le DES. IDEA emploie une clef à 128 bits et utilise des opérations qui sont faciles pour les ordinateurs personnels, donc rendant des réalisations de logiciels de chiffrage plus efficaces.
1990	Charles H. Bennett, Gilles Brassard ont publié leurs résultats expérimentaux sur la Cryptographie Quantique, qui emploie les photons simples pour communiquer en suivant les lois de la mécanique quantique. La Cryptographie Quantique fournit non seulement le secret mais une indication positive de l'écoute clandestine ainsi que du nombre de signes qu'une oreille indiscrète pourrait avoir capturés. La cryptographie quantique exige l'emploi d'un câble de fibre optique entre les deux correspondants.

1991	Phil Zimmermann a divulgué sa première version de PGP (*Pretty Good Privacy*) en réponse à la menace du FBI d'exiger l'accès au texte en clair des communications des citoyens. La sécurité élevée offerte par PGP au citoyen normal pourrait avoir été vue comme un concurrent aux produits commerciaux comme *Mailsafe* de *RSADSI*. Cependant, le PGP est particulièrement notable parce qu'il a été libéré comme freeware (logiciel libre) et est devenu une norme mondiale de fait tandis que ses concurrents restent peu connus.
1994	Le professeur Ron Rivest, auteur des algorithmes RC2 et RC4, a édité un algorithme proposé, RC5, sur l'Internet. RC5 est un chiffrement par bloc, fonctionnant grâce à une clé dont la longueur varie de 0 à 2048 bits

La cryptographie, ou l'art du code secret

Nous allons faire une étude des différents procédés de cryptographie historiques.

Vers 1900 av. J.-C., un scribe égyptien a employé des hiéroglyphes non conformes à la langue correcte dans une inscription. David Kahn[180] le qualifie de premier exemple documenté de cryptographie écrite.

Le *Kama-sutra* est un texte écrit au 5e siècle par le brahmane Vatsayayana, mais fondé sur des manuscrits du 4e siècle avant J.-C. Le Kama-sutra recommande que les femmes apprennent 64 arts, entre autres cuisiner, s'habiller, masser et élaborer des parfums. La liste comprend aussi des domaines moins évidents, comme la prestidigitation, les échecs, la reliure et la tapisserie. Le numéro 45 de la liste est le mlecchita-vikalpa, l'art de l'écriture secrète, qui doit leur permettre de dissimuler leurs liaisons.

Abu Bakr ben Wahshiyya publie, en 855, plusieurs alphabets secrets utilisés à des fins de magie, dans son livre *Kitab shauk almustaham fi ma'arifat rumuz al aklam*, le livre de la connaissance longuement désirée des alphabets occultes enfin dévoilée.

La science arabe en matière de cryptologie est exposée dans la subh al-asha, une énorme encyclopédie en 14 volumes datant de 1412, écrite pour fournir à la bureaucratie une connaissance exhaustive de toutes les principales branches du savoir. Son auteur, qui vivait en Égypte, était Abd Allah al-Qalqashandi. La section intitulée *De la dissimulation des informations secrètes dans les lettres* comporte deux parties, l'une traitant des représentations symboliques et du langage convenu, l'autre des encres invisibles et de la cryptologie.

Giovan Batista Belaso fait paraître, en 1553, un petit livre intitulé *La cifra del Sig. Giovan Batista Belaso*. Il y proposait, pour le chiffrement en substitution polyalphabétique, l'emploi de clefs littérales, faciles à garder en mémoire et à changer. Il les appelait « mot de passe ». Les clefs littérales furent immédiatement adoptées et l'innovation de Belaso est à l'origine de certains systèmes actuels très complexes où plusieurs clefs – et non pas une seule – sont utilisées et changées de façon irrégulière. Il a également écrit « *De Futivis Literarum Notis* ». Ces quatre livres, traitant respectivement des chiffres anciens, des chiffres modernes, de la cryptanalyse, des caractéristiques linguistiques qui favorisent le déchiffrement, représentent la somme des connaissances cryptologiques de l'époque. Parmi les procédés modernes, dont beaucoup sont de son invention, apparaît la première substitution bigrammatique[181] : deux lettres sont représentées par un seul symbole. Il inventa aussi le premier chiffre polyalphabétique[182]. Il fut le premier à classer les deux principes cryptographiques majeurs : la substitution et la transposition.

La cryptographie, comme nous l'avons écrit précédemment, est l'art de transformer un message clair en un message inintelligible par celui qui ne possède pas les clefs de chiffrement. Cependant, on utilise souvent le mot ***cryptographie*** comme synonyme de ***cryptologie***.

Comme Belaso l'a dit, il y a deux grands groupes de méthodes cryptographiques :

— 1. ***Méthodes par substitution***, comprenant tous les systèmes de transposition, de signes codés, de « chiffre » utilisant des tableaux, etc.

[180] David KAHN, journaliste et historien (américain) du renseignement, auteur de *The codebreakers*.

[181] Bigramme : séquence de deux lettres consécutives. Exemples : ee, th, ng...

[182] Se dit d'un chiffre où plusieurs alphabets de chiffrage sont utilisés en même temps. Exemples : le chiffre de Porta et le chiffre de Vigenère.

— 2. ***Méthodes par transformation***, consistant en l'utilisation de formules mathématiques plus ou moins complexes. Ce groupe comporte les méthodes modernes de chiffrement[183].

Méthodes par substitution

Le chiffre de César

La plus connue est sans conteste le « Chiffre de César ». Il consiste en une substitution mono-alphabétique, où la substitution est définie par un décalage de lettres. Par exemple, si on remplace A par D, on remplace B par E, C par F, D par G, etc. Donnons un exemple sur à partir de ce décalage de 3 lettres :

Texte clair	A	B	C	D	E	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Texte chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Le texte que nous souhaitons coder est le suivant :

JE LEVAI LES YEUX VERS LE SOLEIL IL ETAIT BAS ; DANS MOINS D'UNE HEURE IL ARRIVERAIT JUSTE AU-DESSUS DES BRANCHES SUPERIEURES DU VIEUX CHENE.

Le texte codé est alors :

MH OHYDL OHV BHXA YHUV OH VROHLO LO HWDLW EDV ; GDQV PRLQV G'XQH KHXUH LO DUULYHUDLW MXVWH DX-GHVVXV GHV EUDQFKHV VXSHULHXUHV GX YLHXA FKHQH.

Il n'y a que 26 façons différentes de crypter un message avec le code de César. Cela en fait donc un code très peu sûr, puisqu'il est très facile de tester de façon exhaustive toutes les possibilités. Pourtant, en raison de sa grande simplicité, le code de César fut encore employé par les officiers sudistes pendant la guerre de Sécession, et même par l'armée russe en 1915.

On sait que César utilisait ce code car Suétone (écrivain Romain, 70-127), en fait une description dans *La vie des 12 Césars*, une biographie des 12 premiers empereurs de Rome. Voici la traduction française du livre Premier de l'œuvre de Suétone, paragraphe LVI :

« *On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour l'A, et ainsi de suite.* »

De façon insolite, le code de César a été réemployé avec l'avènement d'Internet et des forums de News USENET, à travers le ROT-13. Le ROT-13 désigne simplement le code de César, où on a choisi une ROTation de 13 lettres (A-->N...). L'idée n'est pas de diffuser des messages cryptés, mais de faire en sorte que le message ne soit pas lu involontairement, par exemple s'il dévoile l'intrigue d'un film ou donne la réponse à une devinette.

Dans le même ordre d'idée, il est possible d'utiliser un tableau d'alphabet désordonné, tableau connu des seuls correspondants, ou en inversant l'ensemble de l'alphabet, on obtient le chiffre « Atbash » dérivé du « chiffre hébreu » (puisqu'il est composé à partir des lettres **a**leph, **t**au, **b**eth et **sh**in, les deux premières et les deux dernières lettres le l'alphabet hébreu).

[183] *Chiffre*, Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les lettres du message à chiffrer. *Chiffrement*, Procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clef d'encodage.

Le chiffre de Wolseley

Lord Garnet Joseph Wolseley fut un illustre général anglais, commandant en chef de l'armée anglaise à la fin du 18e siècle. Peut-être ne fut-il pas l'inventeur du chiffre qui porte son nom, mais il est certain qu'il en fit usage.

C'est un chiffre réversible, car un message chiffré deux fois redonnera le message en clair. Le principe est de supprimer une lettre de l'alphabet, en général le « J » (en anglais) ou le « W » (en français). Dans la première ligne de la table, on écrit la clef, puis le reste de l'alphabet sans la lettre supprimée. Ensuite, on écrit dans la deuxième ligne de la table la même séquence, mais dans l'ordre inverse pour obtenir la table de substitution.

Exemple :

* Clef : MAISON
* Lettre supprimée : W

Clair	M	A	I	S	O	N	B	C	D	E	F	G	H	J	K	L	P	Q	R	T	U	V	X	Y	Z
Chiffré	Z	Y	X	V	U	T	R	Q	P	L	K	J	H	G	F	E	D	C	B	N	O	S	I	A	M

On peut aussi présenter ce chiffre sous la forme élégante d'un escargot. La lettre de la case bleue numéro 1 est remplacée par la lettre se trouvant dans la case grise numéro 1, et vice versa. Il en va de même pour les onze autres cases numérotées excepté la case du milieu qui reste identique. On remarquera que l'alphabet désordonné obtenu est le même que celui du tableau ci-dessus.

M	A	I	S	O
N	B	C	D	E
F	G	H	J	K
L	P	Q	R	T
U	V	X	Y	Z

Le carré de Polybe

Nous arrivons maintenant à ce qui fut sans doute le premier procédé de chiffrement par substitution : le carré de Polybe.

Polybe est un historien grec qui vécut environ de 205 avant J.-C. jusqu'à 125 av. J.-C.. À 40 ans, il est emmené parmi 1000 otages par les Romains suite à la bataille de Pydna en Macédoine et à la victoire de Paul-Émile sur les Grecs. Polybe tomba en admiration devant la civilisation romaine de l'époque, et d'otage il devint même ami de la famille de Paul-Émile.

Polybe est à l'origine d'une méthode très originale pour chiffrer, et qui est même antérieure au code de César. Pour cela, il dispose les lettres dans un tableau 5*5 (nous sommes ici obligés d'identifier le i et le j) :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

On remplace alors chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne, puis la colonne. Par exemple, le A est remplacé par 11, le B est remplace par 12, le F par 21, le M par 32.... Si nous codons :

LONGTEMPS JE ME SUIS COUCHE DE BONNE HEURE

nous obtenons :

3134332244153235432415 3215 133445132315 1415 1234333315 2315454215

Le carré de Polybe possède quelques propriétés intéressantes. En particulier, il réduit le nombre de symboles utilisés pour le codage, ce qui rend son analyse plus difficile. C'est en cela un précurseur des méthodes modernes. Remarquons que nous pouvons remplir le tableau de façon différente de ce qui est fait ici, par exemple en commençant par remplir avec un mot-clé, puis par ordre alphabétique.

Le carré de Polybe a encore été utilisé au tournant du XIX^e^ et du XX^e^ siècle par les nihilistes russes. Les nihilistes russes était une organisation secrète armée (on dirait un groupe terroriste maintenant), dont le but était de supprimer le tsar, et quelques membres de sa famille, afin de couper la tête d'une société ancienne et d'établir les bases d'une société à reconstruire. De nombreux nihilistes ont été emprisonnés dans les geôles du Tsar. Pour communiquer entre eux, ils tapaient sur les murs, ou sur la tuyauterie. Par exemple, pour s'échanger le mot EVASION, ils codaient le texte avec le carré de Polybe (adapté à leur alphabet cyrillique) en 15511143243433. Puis ils tapaient la suite de coups sur le mur : 1.5--5.1--1.1--4.3--2.4--3.4--4.3, les « . » désignant des silences brefs, et les « -- » des silences prolongés. On est ici très proche du morse, sauf que l'on peut changer la clé...

Le chiffre bifide de Delastelle

Le chiffre bifide de Delastelle – du nom de son inventeur, le Français Félix-Marie Delastelle (1840-1902), qui en avait décrit pour la première fois le principe dans la « *Revue du Génie civil* » en 1895, sous le nom de « *Cryptographie nouvelle* » – utilise une grille de chiffrement/déchiffrement analogue à celle du chiffre de Polybe. Il repère les coordonnées de plusieurs lettres claires, mélange ces coordonnées, puis lit dans la grille les lettres chiffrées correspondant aux nouvelles coordonnées obtenues. Ce procédé est dit *tomogrammique*[184]. Le *Traité élémentaire de cryptographie* de Delastelle, seul cryptographe civil important de l'époque, fut publié chez Gauthier-Villars en 1902.

Méthode de chiffrement :

— 1. On choisit d'abord la longueur de séries n.

— 2. On regroupe les lettres du message clair n par n (au besoin, on rajoute des nulles pour que la longueur du message soit un multiple de n).

— 3. Sous chaque lettre, on note les coordonnées des lettres verticalement (p. ex. J=21, E=45)

— 4. On lit ensuite horizontalement les coordonnées des lettres chiffrées (24=U, 44=V, 21=J), série par série.

Exemple :

	1	2	3	4	5
1	B	Y	D	G	Z
2	J	S	F	U	P
3	L	A	R	K	X
4	C	O	I	V	E
5	Q	N	M	H	T

Grille de chiffrement

[184] Dans les systèmes tomogrammiques, chaque lettre est tout d'abord représentée par un groupe de plusieurs symboles. Ces symboles sont ensuite chiffrés séparément ou par groupes de taille fixe.

clair	j	e	v	o	u		s	a	i	m	e
1er digit	2	4	4	4	2		2	3	4	5	4
2e digit	1	5	4	2	4		2	2	3	3	5

(avec n = 5)

Coordonnées chiffrées	24	44	21	54	24	23	45	42	23	35
Message chiffré	U	V	J	H	U	F	E	O	F	X

Le déchiffrement s'effectue en sens inverse : on écrit horizontalement les coordonnées des lettres chiffrées, et on lit verticalement les coordonnées des lettres claires. La lettre claire correspondante est trouvée sur la grille.

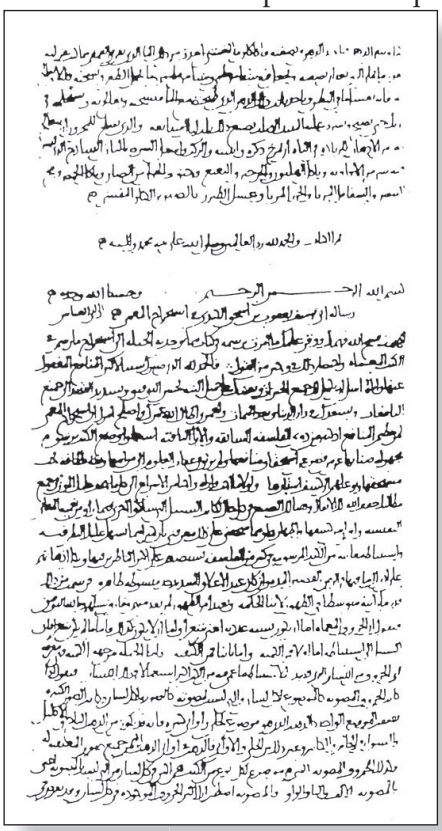
Faiblesse du procédé par substitution

La première faiblesse, comme pour beaucoup d'autres procédés de codages, tient à la clef. Il faut en effet que cette clef soit connue du destinataire pour qu'il puisse procéder au décodage. Il faut donc, soit la lui fournir avant l'envoi du message codé, soit l'incorporer à ce dernier. Nous verrons par la suite que les cryptanalystes s'attaquent toujours d'abord à la clef.

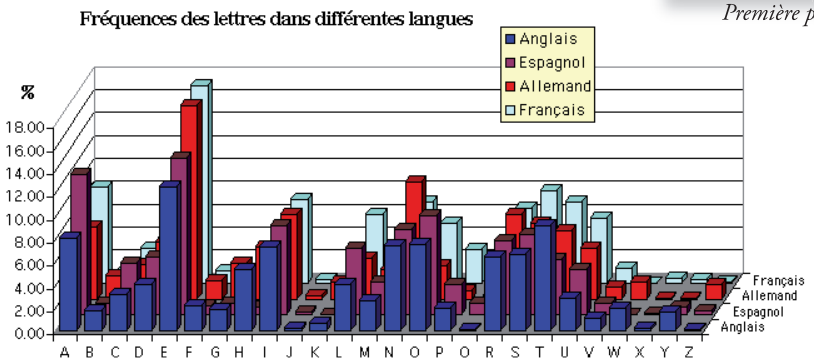
Dans le cas précis des méthodes par substitution, la deuxième faille importante du système a été mise au jour par le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi qui mit au point, au IXe siècle, une technique appelée ***analyse des fréquences***.

Al-Kindi (801-873) rédige sa méthode dans son plus important traité intitulé *Manuscrit sur le déchiffrement des messages cryptographiques*. C'est le premier manuscrit connu faisant mention des fréquences d'apparition des lettres (voir la première page de ce manuscrit ci-contre). Il explique que « *la façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre.*

Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ».



Première page du traité d'al-Kindi



Nous avons vu que pour la cryptographie par substitution mono-alphabétique, il y a a priori 26! clés possible, ce qui en soi est déjà un chiffre énorme. En fait, ce nombre de clés est illusoire, car la cryptographie par substitution possède une grosse faiblesse structurelle : dans les langues, toutes les lettres n'ont pas la même fréquence d'apparition. Dans un texte français, il y a presque toujours beaucoup plus de E que de W. Or, le E est toujours remplacé par la même lettre et le W aussi. Donc, si dans votre texte, la lettre qui apparaît le plus fréquemment est un L, il y a de fortes chances que ce soit un E. En revanche, s'il n'y a presque pas de D, on peut se dire que c'est probablement un W, ou un K, un X, etc.

On voit clairement apparaître sur le graphique précédent plusieurs groupes de lettres qui ont la même fréquence :

— le E est de loin le plus fréquent. Il y a donc de fortes chances que la lettre la plus fréquente du texte codé est en fait un E.

— Ensuite, les A,I,N,R,S,T.

— Puis les O,U,L.

Pour déterminer dans le deuxième groupe quelle lettre est un A, une méthode possible est d'étudier les lettres qui apparaissent isolées (c'est-à-dire dans un mot à une seule lettre du texte) : la lettre isolée la plus fréquente a de fortes chances d'être un A.

Ensuite, on étudie les groupes de 2 lettres (bigrammes). On peut étudier leur fréquence d'apparition dans le texte, et comparer aux fréquences possibles du texte. Par exemple, les EN, NE, TE, SE sont bien plus fréquents que les ST, NR, etc.

Le chiffre polyalphabétique

Giovanni Battista Bellaso (1505 - ?) présente en 1553, dans son livre *La Cifra del Sig. Giovan Battista Bellaso*, la notion de mot-clef. Il utilise un système polyalphabétique composé de cinq alphabets réversibles construits grâce à un premier mot-clef, par exemple IOVE. Le tableau 1 montre comment sont construits ces cinq alphabets : on écrit d'abord le mot-clef coupé en deux sur deux lignes, puis on complète les lignes horizontalement avec les lettres non utilisées (dans l'alphabet latin de cette époque, il n'y a que 21 lettres, et Bellaso a fusionné U et V). Pour construire les quatre tableaux suivants, on décale successivement d'un cran vers la droite la deuxième ligne.

Le même mot-clef permet « d'étiqueter » ces alphabets en écrivant verticalement les lettres du premier alphabet lues de gauche à droite et de haut en bas.

Un deuxième mot-clef est ensuite convenu qui permet de chiffrer le message, par exemple VALISE. À chaque mot du message clair correspond une lettre du mot-clef (celui-ci est au besoin répété). Cette lettre indique lequel des cinq alphabets utiliser (voir tableau 2). Chaque lettre du mot clair est remplacée par celle qui est dans la même colonne.

IDVQ	**i o** a b c d f g h l **v e** m n p q r s t x
OFER	**i o** a b c d f g h l x **v e** m n p q r s t
AGMS	**i o** a b c d f g h l t x **v e** m n p q r s
BHNT	**i o** a b c d f g h l s t x **v e** m n p q r
CLPX	**i o** a b c d f g h l r s t x **v e** m n p q

Tableau 1

Mot-clef	V	A	L	I	S
Clair	le	matin	du	deux	février
Chiffré	XO	CVITD	EC	QOIL	PBAHTBH

Tableau 2

Le message « Le matin du deux février » est chiffré avec les mots-clefs « IOVE » et « VALISE » : XO CVITD EC QOIL PBAHTBH.

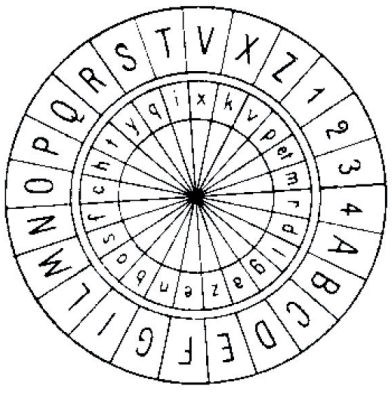
Les espaces entre les mots doivent être conservés pour pouvoir déchiffrer le message.

Léon Batista Alberti est né le 18 février 1404 à Gènes. Son père est un noble florentin, et il donne à son fils la meilleure éducation possible. La formation est alors très humaniste, Léon Batista Alberti étudie la littérature latine, puis le droit à l'Université de Bologne dont il devient docteur en 1428.

En 1432, Alberti s'établit à Rome, où il devient secrétaire à la chancellerie du pape. Son travail consiste à réécrire la biographie des Saints, dans le latin le plus élégant possible. Alberti profite de son séjour à Rome pour étudier l'architecture ancienne. En 1434, il s'installe à Florence, où il s'investit dans l'activité culturelle de la ville : il écrit des poèmes, et tente de populariser l'usage de l'italien à la place du latin. Il s'intéresse alors à la représentation en 3 dimensions des objets, à partir des travaux de Brunelleschi. En 1436, il publie le 1er traité général sur la perspective, *Della Pictura*, qui sera une référence pour des générations de peintres.

Alberti est principalement connu comme architecte. Il travaille d'abord sur l'architecture contemporaine d'un point de vue théorique. Dans son traité *De Re Aedificatoria*, il pose en 10 volumes les jalons essentiels de l'architecture de la Renaissance. Pour Alberti, les mathématiques, le cercle, les rapports de mesure (en particulier la divine proportion, ou nombre d'or), sont le fondement de la beauté. À l'avènement du pape Nicolas V, en 1447, Alberti devient le conseiller principal en architecture de l'église. Il initie alors la reconstruction de la place Saint-Pierre, la réalisation de la façade de l'église San Francisco à Rimini. Toutefois, Alberti s'en tient à la réalisation des plans, et n'intervient jamais sur le chantier.

Alberti est aussi l'auteur du premier ouvrage de cryptographie du monde occidental, l'essai *De Componendis Cyphris*, écrit vers 1460. Il y présente notamment la méthode d'analyse des fréquences, et ainsi comment casser des codes basés sur de simples substitutions. Il présente aussi le moyen de prévenir ces analyses, en changeant par exemple périodiquement d'alphabet.



Pour cela, Alberti présente plusieurs idées, la plus connue étant le *cadran d'Alberti*. Il propose d'utiliser deux disques concentriques. Sur le plus grand, fixe, on écrit l'alphabet dans le bon ordre. Sur le plus petit, mobile, on écrit l'alphabet, mais dans un ordre quelconque. L'expéditeur commence par ajuster les 2 disques de sorte que les A coïncident. Pour chaque lettre du message clair, il cherche la lettre sur le grand disque : la lettre codée est celle qu'on lit en face sur le petit disque. Ceci n'est pour le moment qu'une simple substitution. Pour compliquer les choses, Alberti suggère de tourner périodiquement, par exemple toutes les 4 lettres, le petit disque d'un caractère.

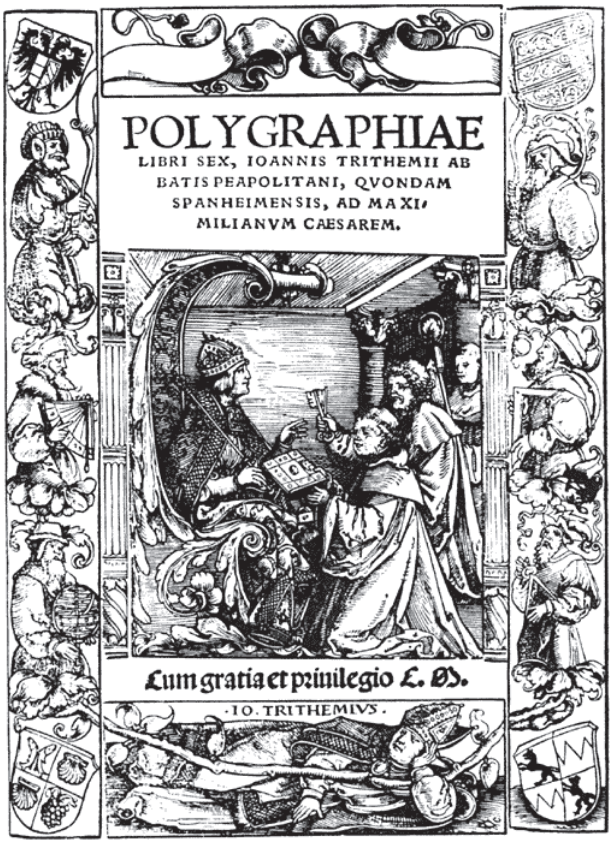
Ainsi, l'alphabet de substitution change au cours du chiffrement : Alberti a inventé le premier procédé de chiffrement polyalphabétique. Ce procédé n'est pas parfait, et ne sera presque pas utilisé. En particulier, il n'y a pas de clé de chiffrement : celui qui parvient à entrer en possession du cadran saura déchiffrer tous les messages.

Alberti décède le 3 avril 1472 à Rome. Par sa triple activité de mathématicien, architecte, et poète, il est une des figures marquantes de la Renaissance italienne, un homme universel précurseur de Léonard de Vinci. Sans doute trop en avance sur son temps, le génie d'Alberti passa inaperçu. Son cadran, longtemps oublié, ne réapparut qu'en 1867, à l'Exposition Universelle de Paris où, sous le nom de cryptographe, il passa pour la géniale invention de l'Anglais Charles Wheaston...

Jean Trithème (1462-1516), Ioannis Trithemius en latin, abbé de son état, est considéré comme un des pères de la cryptographie.

Polygraphia

Le premier ouvrage imprimé, en latin, traitant de cryptographie est de lui : « *Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem* » (*Polygraphie en six livres, par Jean Trithème, abbé à Würzburg, précédemment à Spanheim, dédiée à l'empereur Maximilien*). L'impression fut achevée en juillet 1518 par Johannes Haselberg et l'ouvrage fut réimprimé en 1550, 1571, 1600 et 1613. Une traduction française (annotée et considérablement modifiée) due à Gabriel de Collange parut en 1561 et fut réimprimée en 1625. Le premier des six livres contient 384 colonnes de mots latins, deux colonnes par page. Chaque mot représente une lettre de l'alphabet. Voici un exemple de la première page :



a	Deus	a	clemens
b	Creator	b	clementissimus
c	Conditor	c	pius

En prenant les mots représentant les lettres d'un message secret, il est possible de construire des passages qui ressemblent à d'innocentes prières. Par exemple, chiffrer le mot « abbé » donnera la phrase latine DEUS CLEMENTISSIMUS REGENS MUNDANA. Ces sont les fameuses litanies de Trithème que nous avons déjà évoqué dans le chapitre sur la stéganographie.

Les livres suivants de *Polygraphia* introduisent d'autres schémas cryptographiques, accompagnés de longues tables, pour cacher de l'information ingénieusement.

Polygraphia ne fut pas la première incursion de Trithème dans la cryptologie. En 1499, il avait composé un volume énigmatique et controversé appelé *Steganographia* (ce qui signifie « écriture couverte »). Pendant des années, il circula sous le manteau sous forme de manuscrit avant d'être finalement imprimé en 1606, puis inscrit dans la liste officielle des livres interdits en 1609. En apparence, il expliquait comment employer les esprits pour envoyer des messages secrets !

Les deux premiers livres de *Steganographia* contiennent de nombreux exemples de chiffres simples. Le livre III est largement composé de tables de nombres, dont les colonnes sont surmontées par des symboles zodiacaux et planétaires, suggérant des données astronomiques. Contrairement aux deux premiers livres, il y a peu d'indices pour aider à déchiffrer le contenu.

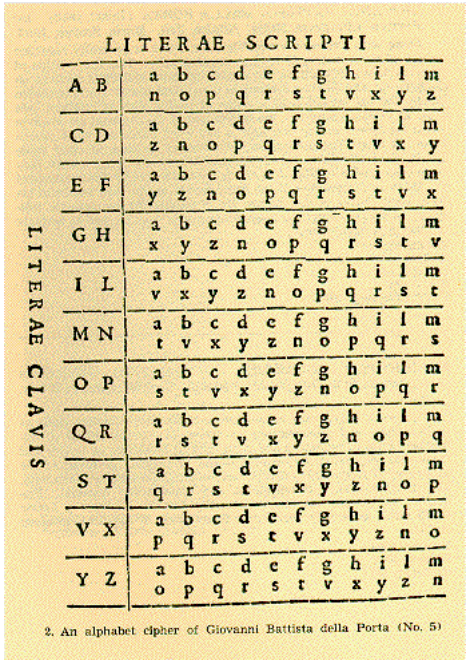
Pendant des siècles, les érudits ont débattu si le troisième livre (incomplet) de *Steganographia* contenait des messages chiffrés. Beaucoup conclurent qu'il ne contenait pas de secrets cryptographiques et donnait simplement des opérations magiques n'intéressant que les occultistes.

Néanmoins, la préface du livre III commence en annonçant que le but provocateur est de présenter une méthode de transmission de messages à distance sans l'utilisation de mot, livre ou messager. Trithème prévint cependant qu'il s'était exprimé de manière délibérément obscure :

« *J'ai fait en sorte que pour les hommes de savoir et ceux profondément engagés dans l'étude de la magie, il pourrait être, par la grâce de Dieu, intelligible à un certain point, tandis que, d'un autre côté, pour les mangeurs de navets à peau épaisse, il pourrait rester un secret caché pour toujours et être pour leurs esprits bornés un livre fermé à tout jamais.* »

Le physicien italien Della Porta (1540-1615) fut l'inventeur du premier système littéral à double clé, c'est-à-dire le premier chiffre pour lequel on change d'alphabet à chaque lettre.

Porta emploie 11 alphabets différents, qu'il désigne, comme on le voit dans la figure ci-contre par AB, CD, EF etc.



2. An alphabet cipher of Giovanni Battista della Porta (No. 5)

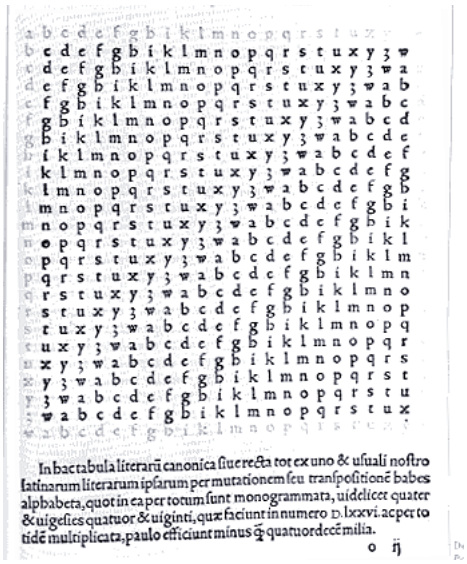
Si on veut écrire avec un de ces alphabets, on choisit pour représenter les lettres du texte clair, celles qui leur font face. Par exemple, si l'on cryptographiait avec l'alphabet A ou B, on représente a par n et vice-versa n par a.

Porta recommande d'écrire chaque lettre avec un alphabet différent. De plus, pour ne pas obliger les correspondants à prendre les onze alphabets à la suite, il propose de n'en adopter que quatre, cinq ou six et de convenir d'un mot clé dont les lettres indiqueront les alphabets qu'il faudra successivement choisir. Ce mot constitue la clé du cryptogramme. Par exemple si le mot-clé est VARI, on utilisera successivement les alphabets V, A, R, I, etc. pour crypter le message.

Bien sûr, il est déconseillé d'utiliser un alphabet régulier comme indiqué ci-dessus (a b c d e...). Il vaut mieux utiliser des alphabets composés des 26 lettres réparties aléatoirement. Della Porta le recommandait déjà lui-même dans son traité : « *De furtivis litterarum notis, vulgo de ziferis*, Naples 1563 ».

Ce fut cependant Blaise de Vigenère qui développa en 1587 le premier code réputé incassable... pendant près de trois siècles, jusqu'à ce que le mathématicien britannique Charles Babbage, connu notamment pour ses machines à différence, élabore la théorie de son décodage, vers 1854.

La paternité de ce code est discutée, le « carré de Vigenère » étant en fait une reprise améliorée du travail de Trithème (tableau ci-contre).



Dans son «*Traicté des chiffres, ou secrètes manières d'écrire* », Blaise de Vigenère passe en revue les différents procédés connus à son époque pour coder un texte. Il reprend entre autres le tableau de l'abbé Trithème en en complétant l'utilisation.

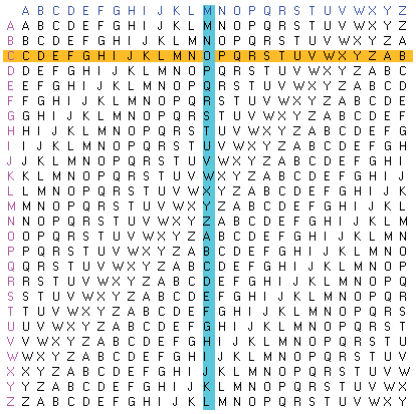
L'idée de Vigenère est d'utiliser un *chiffre de César*, mais où le décalage utilisé change de lettre en lettre. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder :

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé. Pour coder, on regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

Exemple : On veut coder le texte « CRYPTOGRAPHIE DE VIGENERE » avec la clé « MATHWEB ». On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E		D	E		V	I	G	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A	T

Pour coder la lettre C, la clé est donnée par la lettre M. on regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M.



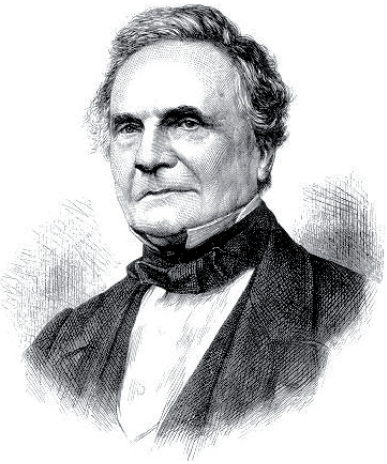
On trouve O. puis on continue. On trouve : ORRWPSHDAIOEI EQ VBNARFDE.

Cet algorithme de cryptographie comporte beaucoup de points forts. Il est très facile d'utilisation, et le décryptage est tout aussi facile si on connaît la clef. Il suffit, sur la colonne de la lettre de la clef, de rechercher la lettre du message codé. À l'extrémité gauche de la ligne, on trouve la lettre du texte clair.

En outre, l'exemple précédent fait bien apparaître la grande caractéristique du code de Vigenère : la lettre E a été codée en I, en A, en Q, et en E. Impossible par une analyse statistique simple de retrouver où sont les E. Dernière chose, on peut produire une infinité de clefs, il est très facile de convenir avec quelqu'un d'une clef donnée.

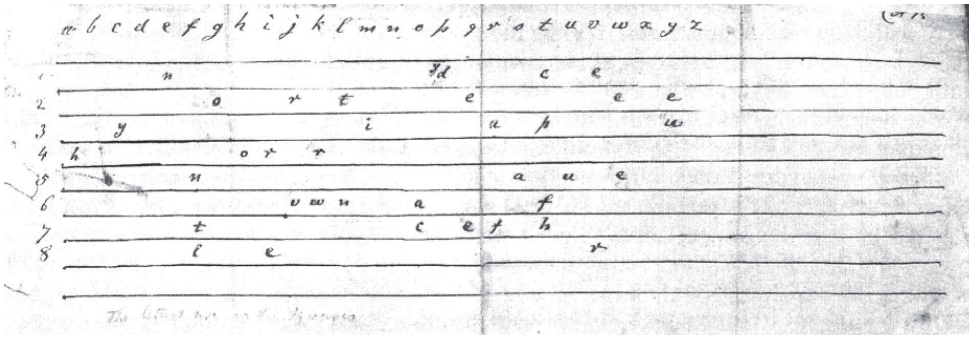
Le chiffrement à l'aide du carré de Vigenère correspond à une addition modulo[185] 26 dans l'alphabet projeté sur les entiers de 0 à 25. En 1710 apparaît le *chiffrement de Beaufort*, créé par Gionanni Sestri, correspondant, lui, à une soustraction.

Si le chiffrement de Vigenère semble d'un principe simple actuellement, il n'en était pas de même au début du dix-neuvième siècle. Au cours de mois de février 1846, l'anglais Charle Babbage[186] (1791-1871) tente le décryptage d'un texte chiffré à l'aide du carré de Vigenère. Expert en cryptographie pour la Royal Navy, Charles Babbage possède dans sa bibliothèque des ouvrages de Gauss et de Bishop Wilkins.



Charles Babbage étudie la fréquence des lettres en supposant différentes longueurs de clé. Cette méthode généralisant le principe de la *symétrie des positions* lui permet de constater l'utilisation de trois clés dans le texte complet qu'il étudiait.

Le 18 septembre 1854, Charles Babbage observe que deux segments identiques du texte clair distants de *x* positions sont chiffrés de la même manière dès que $x = 0(mod|clé|)$. En recherchant les répétitions dans le texte chiffré, il est possible de conjecturer que la longueur de la clé divise le plus grand diviseur commun de ces distances. Cette découverte, assurant la suprématie de l'Angleterre en cryptanalyse, sera gardée secrète.



[185] L'arithmétique modulaire, fut pour la première fois étudiée par le mathématicien allemand Carl Friedrich Gauss à la fin du XVIII[e] siècle et présentée au public dans ses *Disquisitiones arithmeticae* en 1801. Elle est aujourd'hui couramment utilisée en théorie des nombres, en algèbre générale et en cryptographie. C'est une arithmétique où l'on ne raisonne pas directement sur les nombres mais sur leurs restes respectifs par la division euclidienne par un certain entier : le *modulo* (généralement noté *mod* ou *n*). On parle alors de congruence.

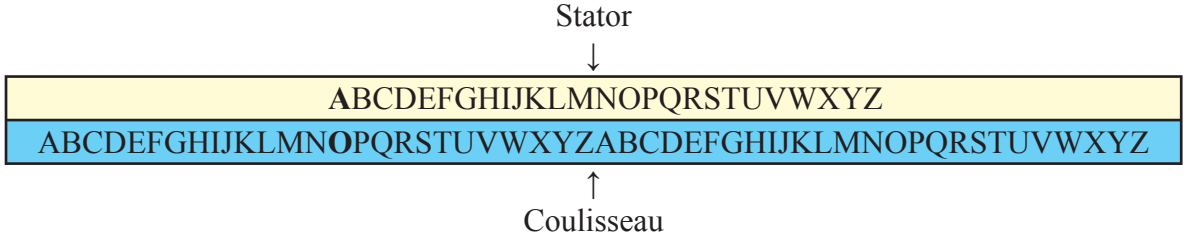
[186] Charles Babbage est né à Teignmouths, Devonshire, d'un père assez nanti qui lui a permis d'entrer à l'école privée de Forty Hill, Enfield dans le Middlesex. C'est dans cette école qu'a commencé sa passion pour les mathématiques et à la sortie de l'académie Forty Hill, il a poursuivi ses études à la maison sous la tutelle d'un professeur d'Oxford. Il a étudié au Trinity College en 1810 et au Peterhouse. Durant ce séjour au Trinity College, il fonde la Société Analytique en 1812 en compagnie de neuf autres mathématiciens universitaires et ainsi faire sa première publication en 1813. Il obtint son diplôme à Cambridge en 1814. Cette même année, il épouse Georgiana Whitmore. Dès l'âge de 24 ans, il est élu membre à la Société Royale de Londres et à celle d'Édimbourg, en 1820. La même année il a fondé la Société Royale d'Astronomie où il est secrétaire pour les quatre années de l'existence de cette société. Il eut huit enfants avec son épouse, dont seulement trois atteignirent l'âge adulte. Son épouse meurt en 1827, Babbage a alors 36 ans.

Ce n'est finalement qu'en 1863, qu'un ancien major de l'armée de Prusse, Frederich Kasiski, publie la méthode dans son livre *Die Geheimschriften und die Dechiffrir-Kunst*.

Les méthodes de cryptage-décryptage citées ci-dessus étaient longues et fastidieuses. Les militaires, principaux utilisateurs de la cryptographie à cette époque, inventèrent la réglette de Saint-Cyr qui était plus simple à manipuler qu'un tableau.

Cet instrument doit son nom à l'académie militaire française où, entre 1880 et le début du 20e siècle, il sert à instruire les aspirants cryptologues. C'est le Hollandais Auguste Kerckhoffs, figure incontournable de la cryptographie, qui baptisa ainsi la réglette.

L'instrument, qui ressemble aux anciennes règles à calcul, est relativement simple ; il s'agit d'une longue bande de papier ou de carton rigide, le « stator », sur laquelle est imprimé à l'horizontale un alphabet ordonné classique. On y fait coulisser une autre bande sur laquelle sont imprimés deux alphabets successifs. Traditionnellement, l'alphabet clair est écrit sur la partie fixe.



Cette réglette permet de faire des substitutions monoalphabétiques du type chiffre de César. Il suffit de bouger le coulisseau et de lire sous la lettre claire la lettre chiffrée (pour chiffrer), ou vice versa (pour déchiffrer). On peut donc aussi, avec plus de manipulations, utiliser la réglette pour faire des substitutions polyalphabétiques. D'ailleurs, dans la pratique, la réglette de Saint-Cyr a remplacé le carré de Vigenère, car ce dernier est souvent sujet à erreurs.

En fait, il s'agit d'une application linéaire du disque chiffrant d'Alberti que nous avons vu précédemment.

Les moyens « modernes » de décryptage du chiffre de Vigenère, puis du chiffre de la machine Enigma dont nous parlerons plus loin, furent proposés par William Friedman[187] qui inventa l'*indice de coïncidence*.

L'indice permet de savoir si un texte a été chiffré avec un chiffre mono-alphabétique ou un chiffre polyalphabétique en étudiant la probabilité de répétition des lettres du message chiffré. Il donne également une indication sur la longueur de la clé probable.

L'indice se calcule avec la formule suivante : $IC = \sum_{q=A}^{q=Z} \frac{n_q(n_q-1)}{n(n-1)}$ avec n le nombre de lettres total du message, n_A le nombre de A, n_B le nombre de B ...

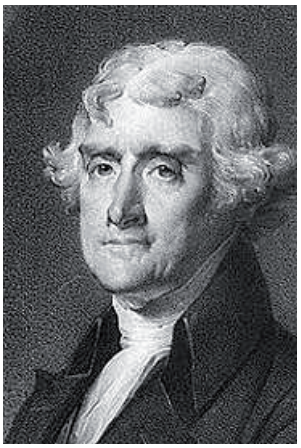
En français, l'indice de coïncidence vaut environ 0,0746. Dans le cas de lettres uniformément distribuées (contenu aléatoire sans biais), l'indice se monte à 0,0385. L'indice ne varie pas si une substitution monoalphabétique des lettres à été opérée au préalable. C'est-à-dire que si l'on remplace par exemple 'a' par 'z' et 'z' par 'a', l'indice ne changera pas.

[187] William F. Friedman (24 septembre 1891 - 12 novembre 1969), cryptologue dans l'armée américaine. Friedman participera à l'effort de guerre contre les Japonais dès 1939 en s'attaquant au code 97, le chiffre utilisé par l'armée nippone. Son équipe sera à même de déchiffrer un volume croissant de messages de l'armée impériale. En 1941, face aux responsabilités importantes qu'il endosse, Friedman fait une dépression et doit se retirer pendant un certain temps. Il visitera Bletchley Park et transmettra ses recherches aux Britanniques responsables de la cryptanalyse d'Enigma. Après la guerre, il devient cryptologue en chef à la NSA. Il part à la retraite en 1956 mais sa santé se dégrade rapidement au début des années 60, il décède en novembre 1969.

Dans le cas où plusieurs alphabets seraient utilisés, mais que le nombre d'alphabets est inconnu, l'indice de coïncidence peut être un précieux allié pour déterminer ce nombre.

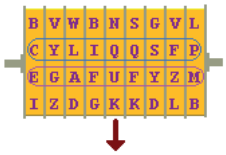
On utilise alors la formule suivante : $IC = \frac{n-m}{m(n-1)} \cdot IC_{langue} + \frac{n(m-1)}{(n-1)m} \cdot 0{,}038$ avec n le nombre total de lettres dans le message, m le nombre d'alphabets, IC_{langue} l'indice pour la langue analysée et 0.038 est un terme correspondant à un contenu uniformément distribué. En variant *m*, on peut comparer l'indice obtenu avec cette formule avec l'indice réel provenant de la formule classique.

Bien qu'ayant été la plupart du temps utilisé comme système de chiffrement monoalphabétique, le cylindre de Jefferson pouvait l'être à la manière du carré de Vigenère.



Thomas Jefferson, vers 1793, alors qu'il était secrétaire d'État de Georges Washington, et futur Président des États-Unis, avait conçu un instrument très ingénieux afin d'envoyer de petits messages codés dans le cadre d'opérations militaires « sur le terrain ». Le cylindre de Jefferson consiste en une série de 25 ou 26 roues, emboîtées le long d'un axe fixe, et pouvant tourner indépendamment les unes des autres par rapport à cet axe. Sur chaque roue, on trouve les 26 lettres de l'alphabet, mais écrites dans un ordre quelconque.

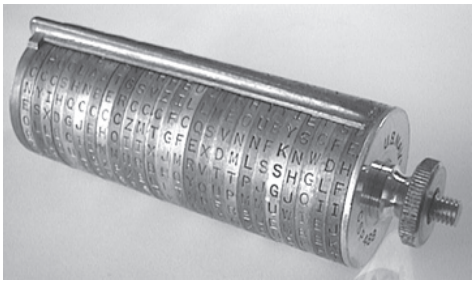
Pour coder le mot CYLINDRE, on fait tourner les roues de sorte de faire apparaître ce mot sur une ligne devant nos yeux. Puis on choisit une autre ligne, par exemple celle juste en-dessous, et on envoie la série de lettres qui s'y trouve.



Le destinataire, qui a reçu EGAFQYOR, écrit ce mot sur une des lignes du cylindre qu'il a en sa possession (il doit être exactement identique à celui de l'expéditeur), et recherche sur une autre ligne à quel message clair cela peut correspondre.

Le commandant français Étienne Bazeries réinventa en 1891 un appareil semblable au cylindre de Jefferson. Le colonel italien Ducros proposa un instrument analogue en 1900.

Le Marquis de Viaris proposa en 1893 une méthode pour décrypter les messages produits par l'appareil de Bazeries.



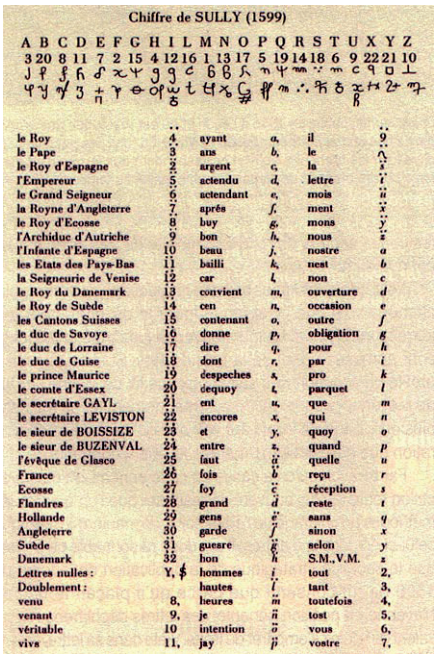
Après que le colonel Joseph O. Mauborgne (qui sera plus tard général de division) eût présenté une amélioration fondamentale dans la construction des alphabets (« Carré latin »), l'armée américaine introduisit en 1922 le cylindre chiffrant M-94 (ci-contre) avec 25 disques, qui fut utilisé par la troupe jusqu'en 1942.

Les bases de la célèbre machine Enigma sont maintenant posées, mais avant de l'étudier, nous devons parler du « ***grand chiffre*** ».

Avant Vigenère les chiffres étaient monoalphabétiques, après il y aura aussi les chiffres polyalphabétiques. Ces derniers étant assez complexes et prenant du temps pour le déchiffrement, les cryptographes durent chercher une arme plus efficace, un chiffre intermédiaire.

Ils eurent alors l'idée d'un chiffre de substitution homophonique[188]. L'idée consistait à remplacer chaque lettre par divers substituts, le nombre de substituts étant proportionnel à la fréquence d'apparition de la lettre. Les substituts seront le plus souvent des nombres par exemple à deux chiffres.

L'un des exemples les plus impressionnants d'un chiffre alphabétique renforcé fut le *grand chiffre* de LOUIS XIV. Il était employé pour les messages les plus secrets du roi. Il fut élaboré par un père et son fils Antoine et Bonaventure Rossignol. Antoine s'était distingué en 1626 en déchiffrant une lettre codée qui révélait que l'armée Hugenote qui tenait la ville de Réalmont était sur le point de céder. Ils renvoyèrent la lettre décryptée aux assiégés, qui comprenant que leur ennemi ne se retirerait pas, se rendirent. Cette réputation lui offrit la place de cryptographe du roi si bien que le père et le fils jouèrent un grand rôle dans la diplomatie française. Mais le plus grand hommage rendu à leurs capacités est l'utilisation dans la langue courante du terme *rossignol* pour désigner un outil permettant de forcer les serrures. Ils se surpassèrent en inventant le *grand chiffre* qui tint en échec tous les cryptanalystes ennemis, si bien qu'à leur mort, leur technique se perdit et qu'il était impossible de déchiffrer de nombreux documents trouvés dans les archives françaises de cette époque. En 1890 Victor Gendron un historien travaillant sur les campagnes de Louis XIV découvrit une nouvelle correspondance utilisant le grand chiffre. Dans l'incapacité de la comprendre, il s'adressa au commandant Étienne Bazeries remarquable spécialiste du service de cryptographie de l'armée qui mit trois années pour le casser. Ce chiffre a tenu deux siècles et ce n'est pas un chiffre homophonique.


Chiffre de SULLY (1599)

A B C D E F G H I L M N O P Q R S T U X Y Z
3 20 8 11 7 2 15 4 12 16 1 13 17 5 19 14 18 6 9 22 21 10

le Roy	4,	ayant	a,	il	9,
le Pape	3,	ans	b,	le	8,
le Roy d'Espagne	2,	argent	c,	la	7,
l'Empereur	5,	actendu	d,	lettre	6,
le Grand Seigneur	6,	actendant	e,	mois	5,
la Royne d'Angleterre	7,	aprés	f,	ment	4,
le Roy d'Ecosse	8,	buy	g,	mons	3,
l'Archiduc d'Autriche	9,	bon	h,	nous	2,
l'Infante d'Espagne	10,	beau	i,	nostre	a
les Etats des Pays-Bas	11,	bailli	k,	nest	b
la Seigneurie de Venise	12,	car	l,	non	c
le Roy du Danemark	13,	convient	m,	ouverture	d
le Roy de Suède	14,	cen	n,	occasion	e
les Cantons Suisses	15,	contenant	o,	outre	f
le duc de Savoye	16,	donne	p,	obligation	g
le duc de Lorraine	17,	dire	q,	pour	h
le duc de Guise	18,	dont	r,	par	i
le prince Maurice	19,	despeches	s,	pro	k
le comte d'Essex	20,	dequoy	t,	parquet	l
le secrétaire GAYL	21,	ent	u,	que	m
le secrétaire LEVISTON	22,	encores	x,	qui	n
le sieur de BOISSIZE	23,	et	y,	quoy	o
le sieur de BUZENVAL	24,	entre	z,	quand	p
l'évêque de Glasco	25,	faut	&,	quelle	u
France	26,	fois	b	reçu	r
Ecosse	27,	foy	c	réception	s
Flandres	28,	grand	d	reste	t
Hollande	29,	gens	e	sans	q
Angleterre	30,	garde	f	sinon	x
Suède	31,	guesre	g	selon	y
Danemark	32,	hon	h	S.M., V.M.	z
Lettres nulles :	Y, $	hommes	i,	tout	2,
Doublement :		hautes	l	tant	3,
venu	8,	heures	m	toutefois	4,
venant	9,	je	n	tost	5,
véritable	10	intention	o	vous	6,
vive	11,	jay	p	vostre	7,

Chiffre homophonique de Sully

Bazeries devint le premier homme à pouvoir pénétrer les secrets du grand roi et en particulier trouva une lettre ayant trait au masque de fer. C'était une lettre de Louvois rapportant une faute commise par Vivien de Bulonde alors qu'il était chargé de mener une attaque contre la ville de Cunéo sur la frontière franco-italienne. Bien qu'il ait reçu l'ordre de tenir, il prit peur et s'enfuit en voyant arriver les troupes ennemies en abandonnant armes et quantité de blessés.

La lettre donnait l'ordre d'arrêter Bulonde, de l'enfermer dans la forteresse de Pignerol ou il serait gardé jour et nuit avec comme unique per-

Selon l'historien Jean-Christian Petitfils, le Masque de fer ne serait en fait... qu'un simple valet, que le geôlier, le marquis de Saint-Mars, aurait masqué afin de faire croire à ses troupes qu'il s'occupait d'un prisonnier d'importance. Une simple mascarade donc, montée par un gouverneur en manque de reconnaissance.

Cette thèse est aujourd'hui la plus probable. Il reste néanmoins un mystère quant à l'identité même de cet Eustache Danger et aux raisons de son emprisonnement. Le valet aurait certainement été détenteur d'un secret d'État, empêchant les autorités de le juger en public. Mais lequel ? Valet de Fouquet, il aurait pu être au courant d'un projet d'assassinat de Colbert par Louvois. Valet de la Cour d'Angleterre, de la possible conversion du roi... Sans preuves valables, le mystère reste entier.

[188] Pour échapper à l'analyse de fréquences, une solution consiste à remplacer une lettre non pas par un symbole unique, mais par un symbole choisi au hasard parmi plusieurs. Dans sa version la plus sophistiquée, on choisira un nombre de symboles proportionnel à la fréquence d'apparition de la lettre ; on parle alors de renversement des fréquences. Ce type de substitution est appelé substitution homophonique (on dit aussi substitution à représentations multiples). On peut situer l'âge d'or de la substitution homophonique entre 1500 et 1750.

mission de se promener sur les remparts dans la journée en portant un masque. La controverse ne s'arrêta pas là, car Bazerie avait traduit le groupe de chiffre 330 par masque, ce qui était peut-être inexact. L'une des grandes énigmes du passé reste encore mystérieuse.

L'énigme du masque de fer semblait résolue... Les faits rapportés sur Bulonde et son insubordination (à Cuneo) sont véridiques. Reste à savoir pourquoi chiffrer un tel ordre, alors que Bulonde était coupable de désobéissance ? Pourquoi le garder au secret, alors que le motif de son arrestation était parfaitement légitime ? Des historiens démontrèrent au demeurant que Bulonde était encore vivant en 1708, cinq ans après la mort du *Masque de fer*. Des experts militaires du chiffre remirent en cause les conjectures de Bazeries (V. Emile-Arthur Soudart et André Lange, *Traité de cryptographie*, 2e édition, 1935). Enfin, si c'est bien en 1691 que Bulonde a été emprisonné à Pignerol, cela fait longtemps que Saint-Mars et le masque de fer n'y étaient plus.

La loi de Kerkchoffs

De tous les procédés de chiffrement que nous venons de voir, et il y en a beaucoup d'autres développés sur les mêmes principes, les militaires, et tous ceux qui ont besoin de transmettre secrètement des informations, tirèrent une loi clairement définie par Auguste Kerkchoffs[189].

Cette loi est encore valable actuellement même avec les procédés de chiffrement informatiques.

1) Le système doit être matériellement, sinon mathématiquement indécryptable

2) Il doit pouvoir tomber sans inconvénient entre les mains de l'ennemi

3) La clé doit pouvoir être communiquée et retenue sans le secours de notes écrites et être changée et modifiée au gré des correspondants

4) Il doit pouvoir être applicable à la correspondance télégraphique

5) Il doit pouvoir être portatif, et son maniement ne doit pas exiger le secours de plusieurs personnes

6) le système doit être d'usage facile.

Le premier de ces deux principes stipule donc que la sécurité d'un système de chiffrement n'est pas fondée sur le secret de la procédure qu'il suit, mais uniquement sur un paramètre utilisé lors de sa mise en œuvre : la clé. Cette clé est le seul secret de la convention d'échange.

Ce principe a cependant été reformulé par Claude Shannon : « l'adversaire connaît le système ». Cette formulation est connue sous le nom de la « maxime de Shannon ». C'est le principe le plus souvent adopté par les cryptologues, par opposition à la sécurité par l'obscurité.

Ce principe a plusieurs justifications. Principalement :

• La confidentialité d'un algorithme est difficile à garantir. Il est en général connu de plusieurs personnes et il est souvent diffusé dans des logiciels à des utilisateurs non habilités au secret.

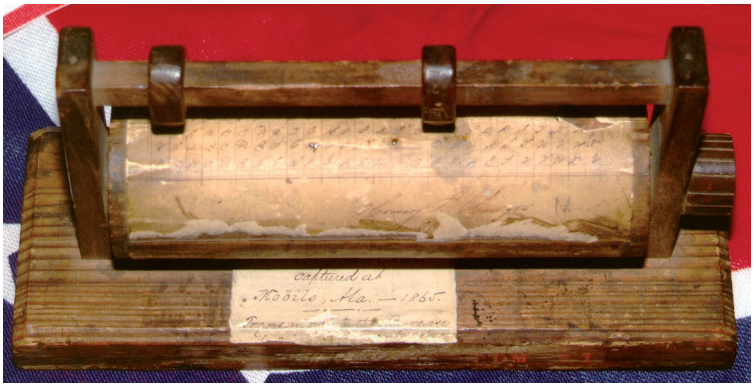
• La sécurité d'un algorithme secret est difficile à évaluer. Il est généralement admis que la meilleure garantie de sécurité d'un algorithme est apportée par une longue période d'évaluation par la communauté cryptographique mondiale.

• Un algorithme secret peut dissimuler des propriétés indésirables par l'utilisateur final (existence de clés faibles, par exemple). Il n'est donc pas adapté si la confiance envers le concepteur n'est pas établie.

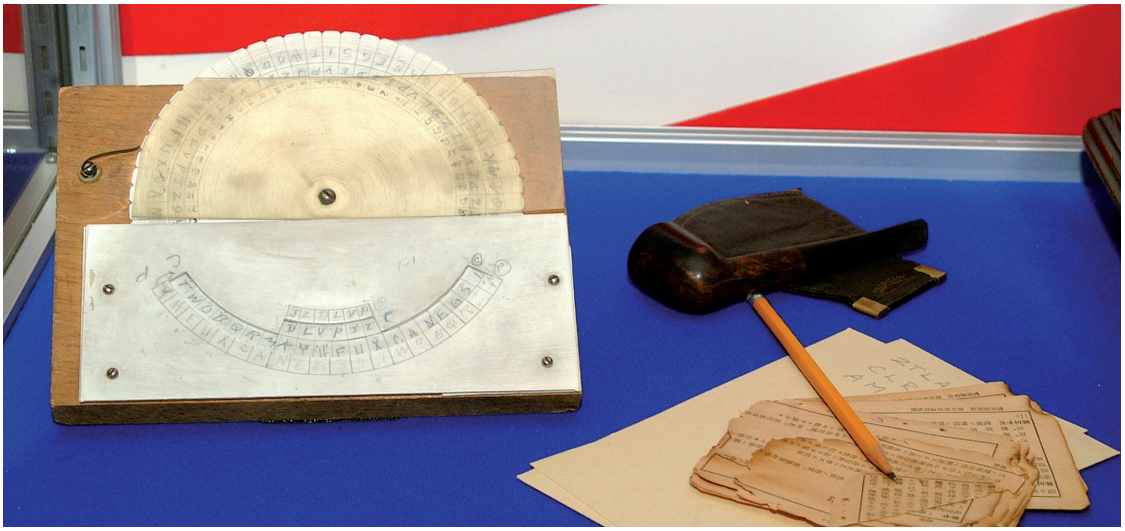
[189] Kerckhoffs est né à Nuth, en Hollande, et fut baptisé Jean-Guillaume-Hubert-Victor-Françoise-Alexandere-Auguste-Kerckhoffs von Niuewenhof. Il raccourcit son nom par la suite et entama des études à l'Université de Liège, où il obtint le grade de Docteur ès Lettres. Après une période où il enseigna en France et dans les Pays-Bas, il devint professeur d'allemand à l'École des Hautes Études Commerciales et à l'École Arago. Kerckhoffs a été quelque temps Secrétaire général de l'Association française pour la propagation du *volapük* et a propagé cette langue internationale, d'abord en France, puis dans plusieurs pays. Il publie en 1886, un cours complet de *volapük*, dans lequel il propose des simplifications, puis un dictionnaire Volapük-Français . Sa volonté de réformer le *volapük* provoque des querelles avec le prêtre Johann Martin Schleyer, créateur du *volapük*. Ceci a pour conséquence un schisme au sein du mouvement volapükiste. Il écrivit en outre un « *Examen critique de la Langue Musicale Universlle de Sudre* ».

Vers la mécanisation et l'automation du cryptage

On peut considérer que les divers types de cylindres, roues, réglettes sont déjà une « mécanisation » du cryptage. Cependant, même avec ces appareils, le chiffrage et le déchiffrage étaient des opérations longues et fastidieuses, avec en plus des risques d'erreurs qui pouvaient, soit rendre le message indéchiffrable, soit donner des informations erronées.



Machine de chiffrage de 1865



Roue de codage manuel

Avec les débuts du télégraphe se posa très rapidement le problème de la sécurité et du secret des transmissions, qu'elles fussent d'ordre privé ou non.

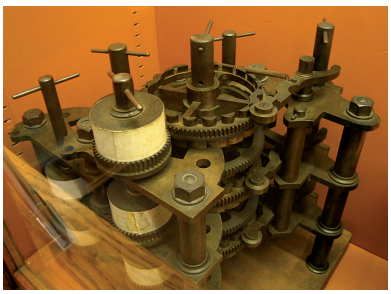
Ce problème était exposé dès 1853 dans un article publié dans la revue anglaise *Quarterly Review* :

« *Des mesures devront être prises pour parer à une sérieuse objection que l'on soulève à propos des communications privées par le télégraphe – la violation du secret – car, dans tous les cas, une demi-douzaine de personnes sont amenées à connaître chaque mot adressé par une personne à une autre. Les employés de la Compagnie anglaise du Télégraphe s'engagent au secret sous serment, mais nous écrivons souvent des choses que nous ne supporterions pas de voir lues par d'autres avant nous. C'est encore un grave défaut du télégraphe, et il faut y remédier d'une manière ou d'une autre* »

La solution était de chiffrer le message confié à l'opérateur qui traduisait en morse le message chiffré avant de le transmettre. À cette époque, le chiffre de Vigenère était le meilleur moyen d'assurer le secret. Mais sa mise en œuvre était délicate.

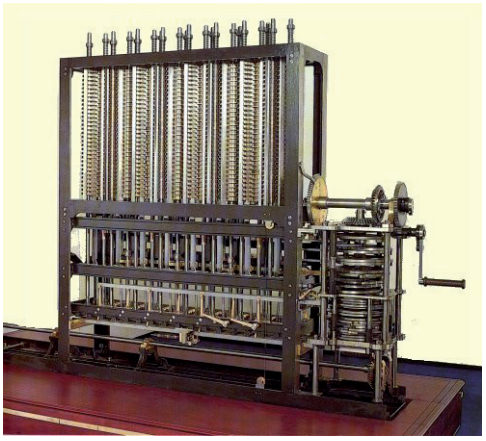
C'est ici que nous retrouvons Charles Babbage. Alors qu'il étudiait avec l'astronome John Herschell les tables mathématiques utilisées en astronomie, à la mécanique et à la navigation, les deux hommes furent affolés de trouver dans ces tables de nombreuses erreurs susceptibles d'entraîner des fautes dans les calculs importants. *Les Éphémérides nautiques pour trouver la latitude et la longitude en mer*, par exemple, contenaient plus de mille erreurs !

Cette observation marqua le début d'une tentative de construire une machine capable d'effectuer sans faute des calculs avec un haut degré de précision.



Gros plan sur les rouages de la première machine de Babbage

Dès 1823, Charles Babbage établit les plans d'un superbe calculateur appelé *Difference Engine N°1*, comprenant 25000 pièces d'une mécanique de précision. Mais le manque de financement le fit renoncer au bout de dix ans à cette réalisation. Il établit un nouveau projet et se mit à construire *Difference Engine N°2*. Pour les mêmes raisons, cette machine eut le même sort que la première : elle ne fut jamais achevée. Pourtant, la machine de Babbage possédait tous les organes d'un ordinateur moderne, et aurait donc pu être utilisée au cryptage et au décryptage.

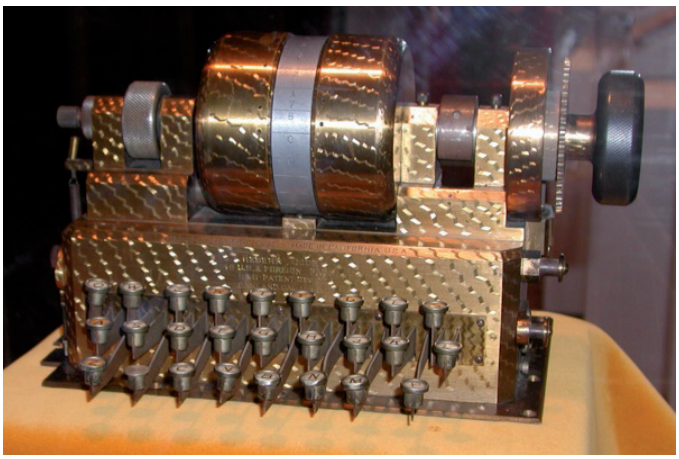


Machine à différence N°2 de Babbage. Construite en 1991 selon les plans originaux, elle fonctionne parfaitement.

Cryptographe de Wheatstone

Plusieurs appareils plus ou moins automatiques furent inventés par MM. Mouilleron, Vinay et Gaussi, Rondepierre, Wheatstone, Silas et d'autres. La plupart de ces appareils produisaient un chiffrage du type de Vigenère.

La machine de Hebern



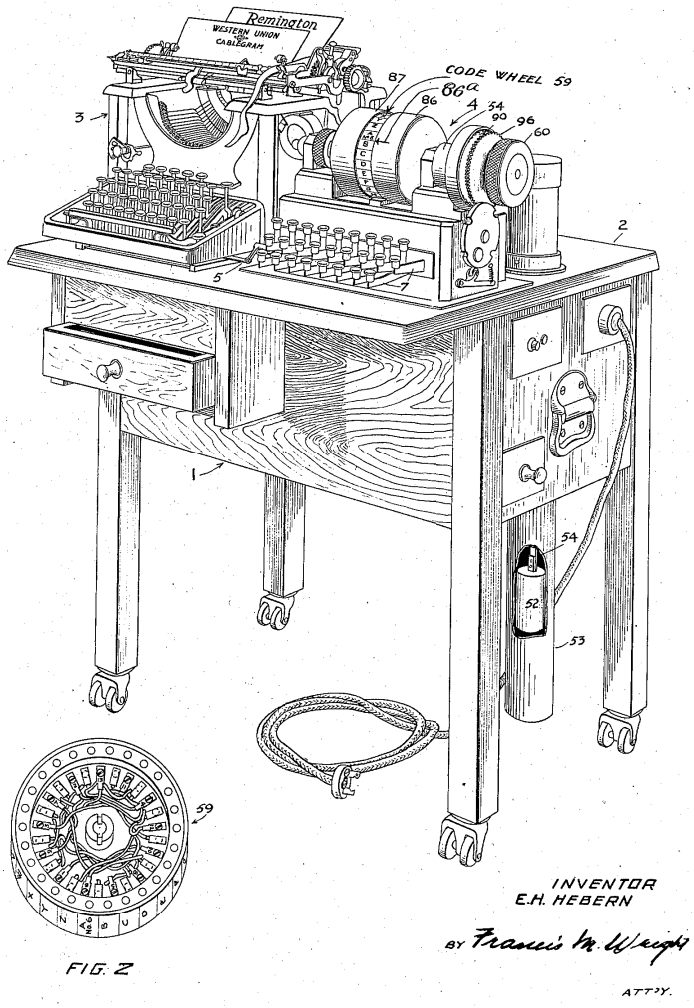
La première machine entièrement automatique fut sans doute la machine de Hebern. Edward Hugh Hebern était un charpentier et entrepreneur dans le secteur de la construction. En 1908, il est emprisonné après avoir volé un cheval. Dans sa cellule, il passe son temps à inventer et plancher sur des systèmes permettant de chiffrer des messages. Après sa sortie de prison, il ne dispose pas des fonds nécessaires à la réalisation de son idée. En 1917, son idée lui revient et il invente la machine qui porte son nom.

La machine de Hebern est une machine électromécanique de chiffrement brevetée en 1918. Une partie électrique était combinée à la partie mécanique habituellement rencontrée dans les machines à écrire de l'époque. Le chiffrement se trouvait entre-deux et était assuré par un jeu de rotors. Il s'agissait de la première machine basée sur ce principe

de rotations, concept qui fut largement repris par la suite notamment par la fameuse machine Enigma allemande.

Le brevet de la « Hebern single-rotor machine » brevet n° 1510441

La clé dans la conception de Hebern était un disque avec des contacts électriques de chaque côté, aujourd'hui appelé *rotor*. Des fils électriques reliaient entre eux des contacteurs disposés sur chacune des faces du rotor, de sorte que chaque lettre d'une face était connectée à une lettre située sur l'autre face, de manière aléatoire. Ce câblage encodait donc une simple substitution monoalphabétique.



Quand l'utilisateur pressait une touche sur le clavier de la machine à écrire, un faible courant électrique fourni par une pile circulait depuis la touche vers l'un des contacts situés sur la face d'entrée du disque, suivait le câblage interne, et ressortait par un contact différent sur l'autre face. Le courant entraînait alors le mécanisme d'une machine à écrire électrique qui frappait la lettre encryptée, ou alternativement, allumait simplement une lampe ou encore perforait un ruban de télétype.

Normalement un tel système ne devrait pas être meilleur que les systèmes de cryptage monoalphabétiques du XVI^{e} siècle. Néanmoins, le rotor de la machine de Hebern était engrené au clavier de la machine à écrire de telle manière qu'après chaque frappe d'une touche, le rotor tournait et que donc l'alphabet de substitution était légèrement modifié. Ceci rendait le système tout aussi efficace que les cryptages polyalphabétiques, mais d'une utilisation très simple. Les opérateurs prépositionnaient le rotor sur une position convenue et commençaient à entrer le texte au clavier. Pour décrypter le message, ils retournaient simplement le rotor dans son logement pour échanger les faces entrée / sortie, ce qui inversait toutes les substitutions. Ils n'avaient plus qu'à entrer le texte crypté au clavier pour que s'imprime automatiquement le texte en clair.

Mieux encore, plusieurs rotors peuvent être placés de telle sorte que les contacts de sortie de l'un soient connectés aux contacts d'entrée du suivant. Dans cette configuration, le premier rotor fonctionne comme auparavant, en avançant d'une position à chaque frappe. Les rotors additionnels sont entraînés chacun par une came placée sur le rotor qui le précède, de sorte qu'ils avancent d'une position lorsque le rotor précédent accomplit une révolution complète. De la sorte, le nombre d'alphabets de substitution augmente considérablement. Pour des rotors de 26 lettres, 5 rotors « empilés » de cette façon autorisent 26^5 = 11,881,376 substitutions différentes.

William F. Friedman s'attaqua à la machine d'Hebern peu de temps après sa mise sur le marché dans les années 1920. Il « solutionna » rapidement toute machine similaire à celle d'Hebern, construite selon le principe d'une pile de rotors dont le premier, le rotor « rapide » tournait d'un cran à chaque lettre entrée. Dans ce cas, le texte crypté se ramenait à des séries de cryptages monosubstitutifs, chacune faisant

26 caractères de long. Il démontra que des techniques éprouvées et habituelles pouvaient être utilisées contre ces systèmes, à condition d'y engager les efforts suffisants.

Bien sûr, cette démonstration devait rester secrète. Ce qui peut expliquer pourquoi l'Armée de terre et la Marine des États-Unis refusèrent de s'équiper des machines d'Hebern, à la grande surprise de ce dernier.

Typex

Typex (aussi nommée « Type X » ou « TypeX ») était une machine de chiffrement britannique mise en service en 1937. Il s'agissait d'une variante commerciale d'Enigma avec des modifications destinées à augmenter la sécurité. Cette machine était initialement appelée « RAF Enigma with Type X attachments ».

Dans les années 1920, le gouvernement britannique cherchait une solution de remplacement pour leur système de chiffrement de type dictionnaire qui était peu sécurisé et qui, avec le surchiffrement, se révéla lent et difficile à utiliser en pratique. En 1926, un comité interservices étudia la question d'utiliser des machines de chiffrement. Pendant plusieurs années le comité étudia de nombreuses options, y compris une suggestion du chef d'escadre O. G. W. G. Lywood d'adapter l'appareil commercial Enigma, mais aucune décision ne fut prise. En août 1934 Lywood commença à travailler sur une machine sans attendre l'autorisation de la RAF. Lywood travaillait avec J. C. Coulson, A. P. Lemmon, and W. E. Smith à Kidbrooke dans le comté d'Oxford, sur une unité d'impression fournie par la Creed & Company. Le premier prototype fut livré au ministère de l'Air le 30 avril 1935. Début 1937, environ 30 Typex Mk I étaient fournies à la RAF.

La conception des modèles suivants commença en février 1937. En juin 1938, une démonstration du modèle Typex Mk II était faite au comité du chiffre, qui passa commande de 350 appareils. Après quelques essais, la machine fut rapidement adoptée par l'armée et d'autres départements gouvernementaux.

Typex arriva en plusieurs versions et comportait cinq rotors avec un réflecteur statique. Dans la majorité des versions, les deux premiers rotors restaient stationnaires pendant le chiffrement, bien qu'ils pouvaient être positionnés à la main. Ces rotors stationnaires fournissaient une sorte de protection similaire au tableau statique de mélange des lettres de la machine Enigma (nommé plugboard en Anglais ou Steckerverbindung en Allemand), dont était dépourvue Typex.

Une autre amélioration de Typex par rapport à la version commerciale d'Enigma[190] était que chaque rotor contenait plusieurs crans qui faisaient tourner le rotor voisin. Alors qu'Enigma changeait de configuration à chaque 26e touche pressée, Typex pouvait changer après 5, 11, 13 et 21 pressions.

Les rotors de Typex se composaient de deux parties, un lingot contenant la gaine électrique était inséré dans un carter métallique. Différents carters contenaient des nombres différents de crans à leur périphérie, tels que 5, 7 ou 9 crans. Chaque lingot pouvait être inséré dans deux sens différents dans un carter en le retournant. À l'usage, tous les rotors de la machine utilisaient des carters d'un même nombre de crans. Normalement cinq lingots étaient choisis dans un lot de dix.

En production, les opérateurs pouvaient traiter vingt mots à la minute et le texte chiffré ou clair était imprimé sur un rouleau de papier. Pour certaines versions portables comme le Typex Mark III, un message était tapé d'une main pendant que l'autre main tournait une manivelle pour actionner l'appareil.

[190] Enigma « civile » (l'Enigma était destinée, dans sa première forme, aux banques).

Typex Mark III

Typex était utilisée par l'armée britannique et la RAF. Ces appareils étaient aussi utilisés dans les pays du Commonwealth comme le Canada et la Nouvelle-Zélande. Une grande différence entre Enigma et Typex était que cette dernière devait servir aussi parcimonieusement que possible alors que les Allemands chiffraient beaucoup de messages de différents services avec Enigma. Typex servait régulièrement seulement au haut commandement de l'armée britannique et à la RAF. Les autres armes ou services continuaient à coder avec leur système à dictionnaire. L'approvisionnement en machines de chiffrement Typex était très restreint et aucune unité de terrain ne fut autorisée à en avoir.

On dit que, ni Typex, ni SIGABA, ni CCM (que nous verrons plus loin) ne furent « cassées » par l'Axe. Bien que les tests d'attaques cryptanalytiques eussent fait d'énormes progrès, les résultats étaient moins probants que contre Enigma, à cause des évolutions de la complexité du système et du flot limité des transmissions faites via ces moyens. Une machine Typex fut récupérée par les forces allemandes, mais sans les rotors. Leur inaptitude à utiliser cette machine pour décrypter les messages alliés Typex ont pu les convaincre de la sécurité d'Enigma.

Les machines Typex restèrent en service jusque dans les années 1970 (le gouvernement néo-zélandais mit en vente ses dernières machines en 1973). C'est une des raisons du maintien du secret aussi longtemps ; une autre était que les Britanniques continuaient à lire les transmissions des pays étrangers faites avec Enigma et Typex, tant que leurs utilisateurs pensaient qu'elles étaient sûres.

SIGABA

Dans l'histoire de la cryptographie, l'***ECM Mark II*** était une machine électromécanique de chiffrement à rotors utilisée par les États-Unis d'Amérique lors de la Seconde Guerre mondiale jusqu'aux années 1950. Cet appareil était aussi connu sous l'appellation **SIGABA** ou Converter M-134 par l'armée, ou CSP-889 par l'US Navy. Pour celle-ci, une version modifiée fut nommée CSP-2900.

Comme beaucoup de machines de cette époque, elle utilisait un système électromécanique de rotors pour chiffrer les messages. Aucune cryptanalyse efficace contre elle pendant sa période de mise en service n'a été révélée à ce jour.

Bien avant la Seconde Guerre mondiale, il était clair pour les cryptographes américains que le mouvement mécanique à simple passe des rotors des nouvelles machines (*Machine de Hebern*) introduisait des schémas reconnaissables dans les textes chiffrés qui pouvaient servir de base aux attaques cryptanalytiques. William Friedman, directeur du *Signals Intelligence Service* (SIS) de l'US Army inventa un système pour corriger cette faille en rendant aléatoire le mouvement des rotors. Sa modification consistait en un lecteur de ruban de papier d'un téléscripteur attaché à un appareil avec des « tentacules » métalliques positionnés pour conduire l'électricité à travers les trous. Pour n'importe quelle lettre pressée sur le clavier, non seulement la machine brouillait les

lettres à la mode des autres appareils à rotors, mais les trous dans le ruban à cet endroit induisaient une avancée des rotors concernés, avant que le ruban lui-même n'avance. L'architecture résultante de ces modifications ne fut produite qu'en faible quantité comme la M-134, et en plus des paramètres habituels d'initialisation de la machine – qu'elle avait en commun avec Enigma parmi d'autres – on ajouta le positionnement du ruban et les réglages, via un panneau de contrôle, de l'association entre chaque ligne de trous et le rotor qui lui est lié.

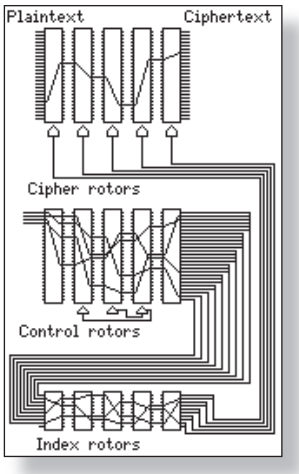


Diagramme de SIGABA (M-134)

La M-134 avait le désavantage, comparée à Enigma, que le ruban devait être identique pour toutes les machines prévues au déchiffrement de ses messages. Si le ruban venait à être intercepté, le nombre de réglages important, mais pas infini aurait remis en cause la fiabilité de son utilisation. De plus, les conditions d'utilisation sur les champs de bataille rendaient problématique la fragilité de certains rubans.

L'associé de Friedman, Frank Rowlett, apporta alors sa contribution à la méthode d'avancée des rotors en changeant ceux-ci. Cela peut paraître évident, mais il s'agissait de créer des rotors permettant de générer de un à cinq signaux de sortie pour un seul en entrée – cela permettait ainsi de faire avancer un ou plusieurs rotors – là ou Enigma faisait du un pour un.

Le budget alloué au déchiffrement était faible aux États-Unis d'Amérique avant la Seconde Guerre mondiale, donc Friedman et Rowlett construisirent une suite d'extensions appelées ***SIGGOO*** (ou ***M-229***) qui furent utilisées avec les M-134 à la place du lecteur de ruban. Il s'agissait de boîtes externes contenant un paramétrage via trois rotors qui permettaient cinq entrées actives, comme si l'on pressait cinq touches en même temps sur Enigma, et les sorties étaient également rassemblées en groupes de cinq – c'est-à-dire que les lettres de A à E seraient câblées ensemble par exemple. De cette manière, les cinq signaux d'entrée sont randomisés par l'intermédiaire des rotors, et ressortent de l'autre côté comme un seul signal sur l'une des cinq lignes. Le mouvement des rotors pouvait être contrôlé par un code renouvelé chaque jour, et les bandes de papiers étaient détruites. Cette machine, assemblage de plusieurs boîtes, était appelée M-134-C.

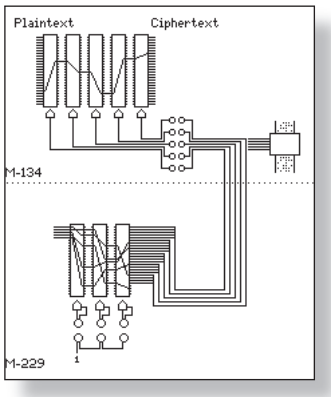


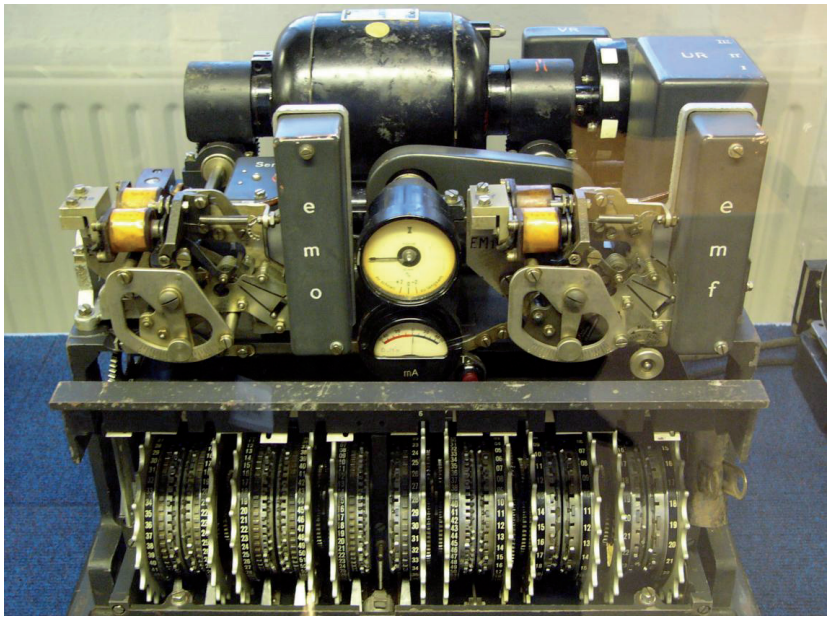
Diagramme de SIGGOO

Mais SIGABA avaient aussi des inconvénients : sa taille et son poids important, son prix élevé, sa difficulté d'utilisation, sa complexité mécanique et sa fragilité. Cela n'avait rien à voir avec un dispositif pratique comme l'Enigma, qui était plus petite et légère que les radios avec lesquelles on l'utilisait. SIGABA fut très utilisée dans les salles radio des navires de l'US Navy, mais ne pouvait être utilisée sur un champ de bataille, et, dans la plupart des théâtres d'opérations, d'autres systèmes étaient utilisés, surtout pour les communications tactiques.

La machine de Lorentz

La machine de Lorenz était utilisée pour chiffrer les communications militaires allemandes de haute importance pendant la Seconde Guerre mondiale. Les cryptanalystes de Bletchley Park, dont nous reparlerons plus loin, ont pourtant été en mesure de casser son code.

Les machines de Lorenz SZ 40 et SZ 42 (Schlüsselzusatz, signifiant « pièce jointe chiffrée ») étaient des machines allemandes de chiffrement utilisées pendant la Seconde Guerre mondiale pour les envois par téléscripteur. Les cryptographes britanniques, qui se référaient de façon générale au flux des messages chiffrés allemands envoyés par téléscripteur sous l'appellation Fish (Poissons), ont nommé la machine et ses messages ***Tunny*** (Thons). Pendant que la renommée machine Enigma servait à l'infanterie, la ma-



chine de Lorenz était destinée aux communications de haut niveau, qui pouvaient s'appuyer sur cet appareil lourd, son opérateur et des circuits dédiés. La machine elle-même mesurait 51 cm x 46 cm x 46 cm et accompagnait les téléscripteurs Lorenz standards. Ces machines appliquaient une méthode de chiffrement de flux.

La machine de Lorenz avait 12 roues comprenant 501 « pointes ».

Les téléscripteurs d'alors traitaient chaque caractère, généralement chiffré avec le code Baudot ou un procédé équivalent, comme 5 bits en parallèle sur 5 lignes. La machine de Lorenz produisait des groupes de cinq bits pseudo-aléatoires à combiner par l'opérateur ou exclusifs au texte clair. Les bits pseudo-aléatoires étaient générés par dix « roues cryptographiques », cinq d'entre elles tournant régulièrement, nommées les roues χ (chi) et cinq autres à la course irrégulière, nommées les roues ψ (psi). Le pas de rotation des roues ψ dépendait de deux autres roues, appelées les « roues motrices ». Hormis son rôle d'entraînement irrégulier de cinq roues (qui, soit avançaient ensemble, soit restaient ensemble), la machine de Lorenz constitue un générateur pseudo-aléatoire à cinq flux parallèles ; aucune autre interaction n'existe entre les cinq lignes. Les nombres de « pointes » sur toutes les roues étaient premiers entre eux.

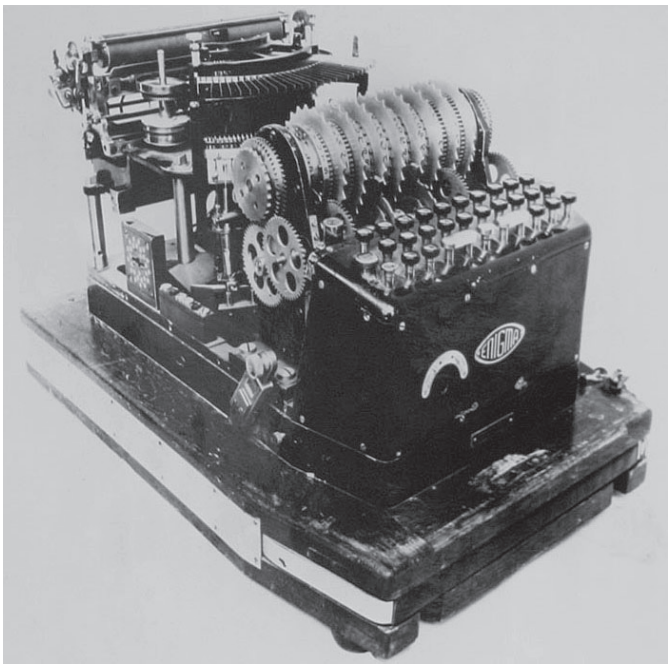
Ces machines étaient de la même veine que celles proposées en premier par le Colonel Parker Hitt de l'Armée des États-Unis d'Amérique à l'époque de la Première Guerre mondiale (cylindres de Jefferson).

Les cryptanalystes de Bletchley Park ont compris le fonctionnement de la machine dès janvier 1942 sans jamais en avoir vu un seul exemplaire. Cela fut possible à cause d'une erreur commise par un opérateur allemand. Le 30 août 1941, un message de 4 000 caractères fut transmis ; cependant, le message n'ayant pas été reçu correctement à l'autre bout, celui-ci fut retransmis avec la même clé (une pratique formellement interdite par la procédure). De plus, la seconde fois le message fut transmis avec quelques modifications, comme l'utilisation de certaines abréviations. À partir de ces deux textes chiffrés, John Tiltman a été en mesure de reconstituer à la fois le texte en clair et le chiffrement. D'après le chiffrement, toute la structure de la machine fut reconstruite par W. T. Tutte.

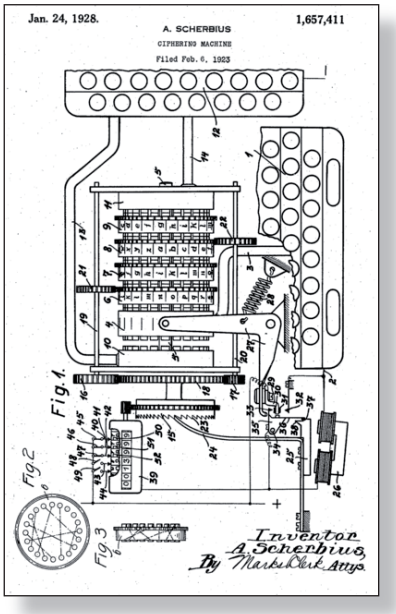
Les transmissions « Tunny » étaient interceptées à Knockholt dans le Kent, avant d'être envoyées à Bletchley Park.

Nous allons maintenant étudier la machine sans doute la plus connue et la plus performante à l'époque : **ENIGMA**.

ENIGMA



Première Enigma commercialisée



Brevet d'Enigma

Lors de la Seconde Guerre mondiale, Enigma bouleverse le monde de la cryptographie en assurant la confidentialité des communications allemandes, sur laquelle le III[e] Reich comptait dans la mise en œuvre de sa stratégie. Cette machine permettait aux Allemands de crypter les messages militaires, en se basant sur un dispositif électromécanique de chiffrement.

À l'origine de la machine Enigma, est un inventeur allemand, Arthur Scherbius[191].

Il déposa le brevet pour sa machine en 1918, et fonde avec un ingénieur du nom de Richard Ritter la société *Chiffriermaschinen AG* en 1923, pour commercialiser sa machine. Malheureusement pour lui, il n'a pas pu proposer sa machine aux militaires en raison de l'Armistice de 1918. Il se tourna alors vers les milieux financiers et les banques : pour cela, il fit des démonstrations publiques dès 1923 à Bonn, puis en 1924 à Stockholm lors du Congrès Postal International. En 1927, il acheta les brevets de la machine de Koch, qui avait inventé le « réflecteur ».

La machine de Scherbius présentait des avantages, non seulement par la force du cryptage qu'elle opérait, mais aussi par sa simplicité d'utilisation. Seules les machines Enigma pouvaient être munies d'un *réflecteur*. Alors que dans les autres machines, il pouvait être nécessaire de retourner le dispositif pour permettre le décryptage des messages, ce dispositif facilitait l'utilisation de la machine en permettant au décryptage des messages de se dérouler exactement de la même manière que le cryptage. Mais Scherbius perdit ses clients potentiels, découragés par les prix excessifs des machines.

La première machine Enigma nommée Enigma A fut notamment exposée en 1923 au Congrès de l'International Postal Union de Bern, en Suisse.

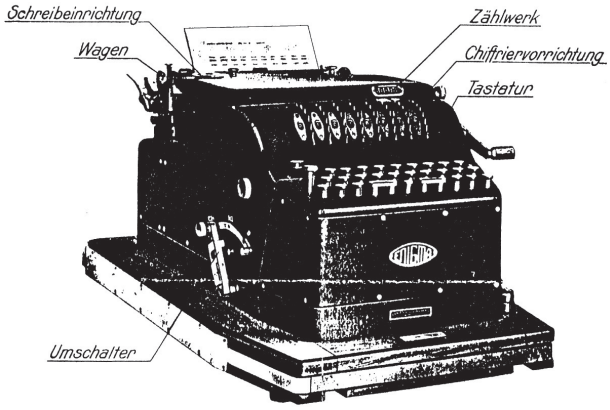
[191] Arthur Scherbius est né Francfort, en 1878. Fils d'un homme d'affaires, il étudie l'électricité au collège technique de Munich et s'inscrit ensuite au collège technique de Hanovre où il termine ses études en mars 1903. L'année suivante, il écrit sa thèse sur un système de turbine et reçoit son doctorat en ingénierie. Arthur Scherbius travaille ensuite pour plusieurs entreprises, en Allemagne et en Suisse. En 1918, il fonde son entreprise, « *Scherbius & Ritter* » à Berlin et invente différents objets : des moteurs asynchrones, des coussins électriques ou encore des corps chauffants en céramique. Ses contributions font que son nom est resté dans le domaine des moteurs asynchrones : on parle du principe de Scherbius pour désigner l'utilisation de machines tournantes au lieu de convertisseurs de puissance. Le 23 février 1918, il dépose un brevet pour sa machine de chiffrement et commence à la commercialiser. Au début, la machine n'est pas destinée à un usage militaire. Scherbius achète aussi les droits d'un autre brevet, une machine de chiffrement inventée par Hugo Koch et brevetée en 1919. Les affaires sont difficiles et l'entreprise est réorganisée à deux reprises durant les années 1920. En 1923, Scherbius vend la première version, l'Enigma-A. Trois autres versions commerciales vont suivre, et l'Enigma-D devient le modèle le plus répandu. Scherbius n'aura pas l'occasion de voir le succès de sa machine durant la guerre de 39-45, il décède en 1929 dans un accident d'attelage.

Voici la première page du document de promotion de cette machine :

Die schreibende

Enigma - Chiffriermaschine

Typenhebel – Elektrischer Antrieb



Unangreifbar in ihrer Chiffriersicherheit

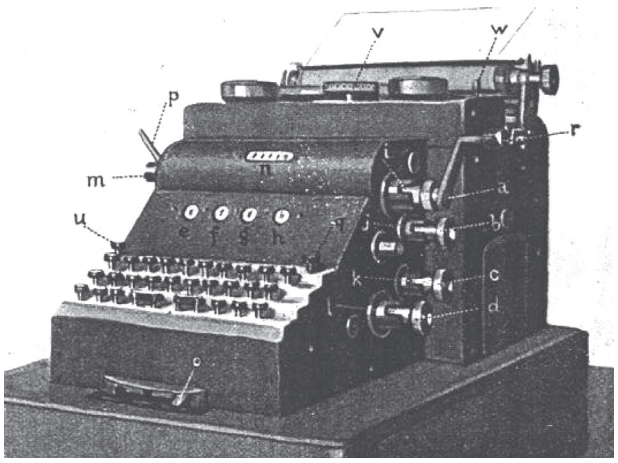
Jeder Entzifferungsversuch Zeitverschwendung

Volle Geheimhaltung auch bei Uebermittlung von Schlüsselwechseln in Klarschrift

17 576 Perioden / Jede Periode 15 777 450 Zeichen

In einer halben Minute ist jeder der 277 304 461 200 Schlüssel eingestellt

Kein Teil wird zur Schlüsseländerung ausgetauscht



Enigma Modèle A

Les spécifications techniques de cette machine étaient les suivantes :

Chiffrage/déchiffrage : 300 symboles par minute

Divise le texte chiffré en rangée de 50 et groupes de 5 lettres

Délivre le texte clair dans sa forme originale avec lettres, nombres, ponctuation

Compte tous les symboles

Déchiffre tout si c'est correctement transmis, même s'il y a des manque dans le texte chiffré

Ne fonctionne pas si mal utilisée

Utilisable après 30 minutes d'instruction

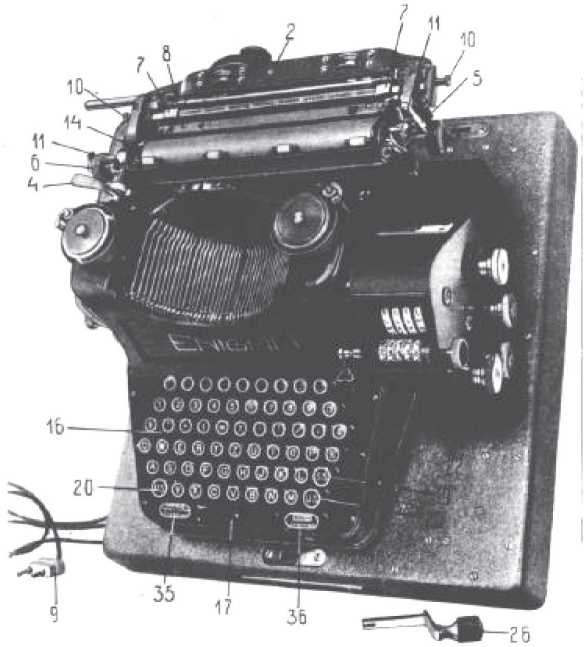
Dimensions :

Longueur : 65 cm

Largeur : 45 cm

Hauteur : 35 cm

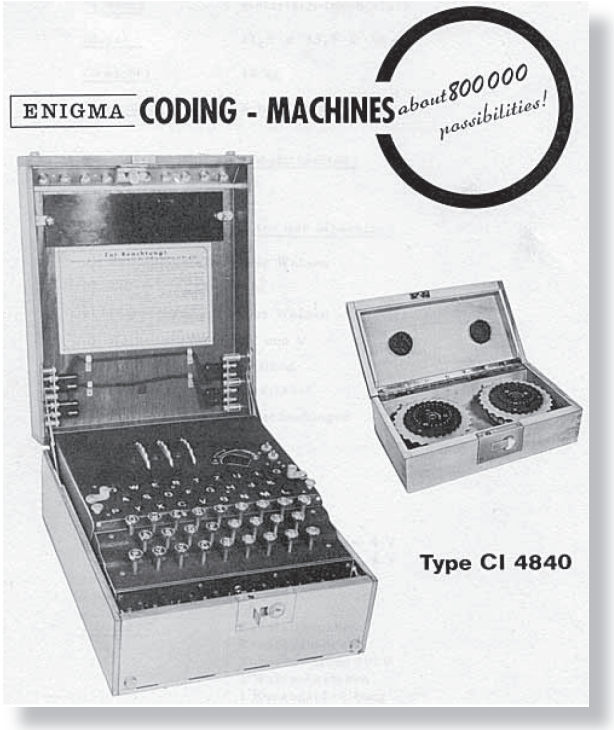
Poids : 50 kg



Enigma Modèle B

Le modèle B, ci-contre, différait du modèle A par l'utilisation de rotors à 26 contacts (nous verrons ceci en détail plus loin).

Le modèle C qui sortit quelque temps plus tard, était un modèle « portable » à la différence des modèles précédents. Mais surtout, ce fut à partir de ce modèle



Publicité anglaise du modèle commercial Enigma C

que les machines Enigma intégrèrent le *réflecteur*, invention de Hugo Koch. Grâce au réflecteur, le chiffrage produit par la machine devient réversible sans aucune manipulation. Il suffit de mettre les rotors en position de départ utilisée pour chiffrer un texte et de taper le texte chiffré pour obtenir directement le texte clair.

Si la machine était un fiasco dans sa version destinée aux civils, elle allait acquérir sa renommée grâce à l'usage qu'en firent les militaires.

Dans les années 1920, l'armée allemande se vit forcée de reconnaître la piètre sécurité offerte par son système de cryptage ADFGVX[192]. Ce changement d'état d'esprit se fit suite à la parution de deux livres, l'un de l'amiral anglais John Fisher, l'autre intitulé *The world crisis* écrit par Winston Churchill qui était alors à la tête de la marine anglaise.

Ces deux ouvrages mettaient en avant l'avantage décisif de la Grande-Bretagne dans la Première Guerre mondiale grâce aux succès des cryptanalystes britanniques sur les messages allemands.

L'armée allemande, mise devant le fait accompli, mena une enquête et conclut à la nécessité de s'équiper en Enigma. Ce fut tout d'abord la nouvelle marine allemande, la Reischmarine, en 1926 ; puis l'armée régulière, la Reichswehr, en 1928 ; et enfin l'armée de l'air, la Luftwaffe, en 1935. Mais il faut attendre l'accession de Hitler au pouvoir en 1933 pour que l'armée allemande s'équipe massivement en Enigma. Ce sont près de 200 000 machines qui furent construites jusqu'en 1945, cette production ayant été déléguée à plusieurs firmes allemandes.

[192] Depuis mars 1918, l'armée allemande utilisait un nouveau code pour communiquer, le chiffre ADFGVX, ou GEDEFU 18 (GEheimschrift DEr FUnker 18, chiffre des télégraphistes 18). Ce chiffre, inventé par le colonel Fritz Nebel, est constitué d'une substitution de type *carré de Polybe*, suivie d'une transposition. Pour réaliser la substitution, les 26 lettres de l'alphabet et les 10 chiffres sont rangés dans un tableau 6×6, aux extrémités desquelles on a ajouté les lettres ADFGVX.

Le concept de guerre de mouvement

Juste après la Seconde Guerre mondiale, pour ne plus avoir affaire à la guerre des tranchées dont les deux camps pâtissaient, on inventa le concept de guerre de mouvement.

En 1920, des généraux anglais prédisaient que les tanks, en plus de leur puissance de tir écrasante, pouvaient tirer parti de leur mobilité en rompant à travers le front ennemi et en s'attaquant à leurs positions reculées, où se trouvaient l'artillerie et le ravitaillement, ce qui saperait par la même occasion le moral des troupes ennemies.

Des officiers des armées de terre de tous les pays se sont intéressés à ce concept, comme De Gaulle, ou encore Heinz Guderian. Ce dernier écrivit plusieurs articles et reçut l'attention d'Hitler. Il fut promu au grade de général et se vit recevoir le commandement de blindés avant l'invasion de la Pologne. Il pouvait donc appliquer sa nouvelle stratégie au conflit qui allait suivre.

Cette stratégie, la ***Blitzkrieg***, guerre-éclair, a été conçue pour vaincre rapidement, sans que la guerre des tranchées n'ait le temps de s'installer. Pour la mettre en pratique, l'armée allemande s'est dotée à partir de 1933 d'une force de frappe importante, composée de blindés, les Panzer, et de bombardiers Stuka, pour éléments essentiels.

La Blitzkrieg consiste en une attaque rapide des positions ennemies, par les différentes armées coordonnées entre elles : l'infanterie, les blindés de la Wehrmacht et les bombardiers de la Luftwaffe :

1. Les unités aériennes attaquent le front, l'arrière et la logistique ennemie, de manière à les affaiblir.
2. L'infanterie attaque le front sur une étendue vaste : de cette manière, l'ennemi ne peut pas savoir où l'offensive majeure aura lieu et sera pris par surprise.
3. Les tanks attaquent de manière massive et groupée les lignes de défense principales, et progressent dans le territoire ennemi, tandis que l'infanterie, continue d'attaquer l'ennemi pour l'empêcher d'organiser une défense efficace, avant de l'encercler.
4. Les unités mécanisées progressent et paralysent les positions arrières de l'ennemi pour l'empêcher de se replier.
5. Les différentes forces se rejoignent pour en finir avec l'ennemi.

Son principe fait que la Blitzkrieg doit son efficacité à de plusieurs éléments tactiques nécessaires, que l'on peut faire correspondre avec des contraintes concernant les moyens de communication allemands.

En tout premier lieu, la Blitzkrieg est une coordination de toutes les armées. L'Allemagne a donc dû se doter d'un système de communication très vaste entre chaque unité et leur quartier général.

Deuxièmement, la Blitzkrieg se doit d'être rapide, et cette rapidité doit se retrouver dans la transmission des ordres. Une formation de Panzer avait beau aller vite, elle se mettait en danger et mettait en danger les autres unités si elle se mettait en route trop tard, à cause d'un ordre parvenu en retard.

Ces deux premiers critères étaient parfaitement remplis par la radio, celle-ci pouvant être déployée à grande échelle et permettant de communiquer rapidement, profitant de la célérité des ondes. Mais par sa nature même, les messages qui étaient transmis pouvaient être recueillis par n'importe qui disposant d'un récepteur réglé sur la bonne fréquence. L'effet de surprise, qui est le troisième élément tactique de la Blitzkrieg, aurait été inexistant si le camp adverse avait eu accès au contenu des messages, et nécessitait d'être préservé.

L'intérêt d'Enigma

C'est à la nature dispersive des ondes radio que la machine Enigma doit sa participation à la guerre mondiale. Elle occupa la place centrale dans la sécurisation des communications allemandes en permettant de crypter les messages de nombreuses unités avant qu'ils ne soient envoyés. Elle multiplie les points forts : rapide, la machine était plus simple à utiliser que d'autres procédés de cryptages, puisqu'elle faisait intervenir un dispositif électromécanique automatique pour le cryptage, et évitait donc aux opérateurs

l'effort qu'aurait nécessité un cryptage se faisant avec crayon et papier. Petite, elle était transportée aisément, ce qui augmentait le nombre de situations où elle pouvait se rendre utile, et permettait aussi de ne pas entraver la mobilité des unités, point clef de la stratégie de la Blitzkrieg. Enfin, les Allemands ont pu établir un réseau très vaste de postes de TSF équipés de machines Enigma, puisqu'ils en étaient équipés de 30 000 au début de la guerre, pour un total de 200 000 machines construites à la fin de la guerre.

Pour les Allemands, la machine Enigma était tout ce dont l'armée avait besoin, en ce qui concernait la confidentialité de ses communications, pour la mise en œuvre de la Blitzkrieg. L'Allemagne nazie a eu une confiance aveugle en cette machine pour sécuriser les communications de toutes leurs armées et de certains des services en pensant que la machine était telle que l'avait vanté son concepteur Arthur Scherbius : ***invincible***.

Les différentes machines

Il faut savoir que lorsqu'on parle de la machine Enigma, en réalité, on parle d'un ensemble de machines parfois très différentes entre elles sur le plan cryptographique.

Chaque armée disposait d'une version particulière d'Enigma. Les plus célèbres d'entre elles sont les machines de type M3 et M4 dont se servait la marine allemande, à cause de leur implication dans la Bataille de l'Atlantique et l'impact de leur décryptage sur la Seconde guerre mondiale. Mais qu'existe-t-il comme machines autres que M3 ou M4, et en quoi différaient-elles ?

Enigma standard

Toutes les variantes d'Enigma possèdent des rotors assemblés en un *brouilleur* comme pièce électromécanique servant de base au cryptage. Ce sont les caractéristiques de ce brouilleur qui différencient les machines entre elles, ainsi que l'adjonction ou non d'un tableau de fiches. La complexité du cryptage effectué par la machine augmente avec ces différents dispositifs.

La machine Enigma standard : Il s'agit de la machine employée par les armées de terre et de l'air allemandes, qui était la plus courante. Elle était dans son fonctionnement presque identique à la machine Enigma D vendue dans le commerce. Trois rotors étaient alignés dans le brouilleur.

Enigma M3

La machine Enigma M3 : La marine allemande (Reichsmarine devenue Kriegsmarine) employait cette machine à partir de 1933. Elle était sensiblement plus difficile à décrypter que la machine standard, car bien qu'elle disposât du même nombre de rotors alignés simultanément dans le brouilleur, ceux-ci étaient choisis parmi un lot plus grand, proposant deux rotors en plus des trois initiaux.

La machine Enigma M4 : Cette machine remplaça la machine Enigma M3 en 1942 dans les sous-marins et dans les stations sur la côte, et était beaucoup plus complexe d'un point de vue cryptographique : quatre rotors étaient alignés simultanément dans le brouilleur de celle-ci, les trois premiers étant choisis parmi un lot de huit rotors, et le dernier étant choisi parmi deux autres.

Enigma M4

La machine Enigma G ou Abwehr Enigma : elle était utilisée par les services secrets allemands. Il s'agit également d'une version à quatre rotors, mais démunie d'un tableau de fiches. La rotation des rotors a été choisie rapide, ce qui était perçu comme une difficulté supplémentaire pour d'éventuels cryptanalystes. Mais il s'avère que cette particularité a ajouté une faille supplémentaire à la machine, une aubaine pour les décrypteurs de Bletchley Park.

Enigma G

La machine Enigma des chemins de fer allemands ou Raildienst Enigma : celle-ci différait peu de la machine vendue dans le commerce, elle était utilisée par les services ferroviaires allemands.

Il est intéressant de noter que les différences fonctionnelles entre les machines ont eu deux conséquences. D'une part, les machines ne pouvaient pas se déchiffrer entre elles, à l'exception des machines M4 capables de communiquer avec les machines M3 avec un réglage du quatrième rotor spécifique. D'autre part, certaines machines se sont révélé être, pour les Alliés, très faciles à décrypter ; tandis que d'autres effectuaient un cryptage beaucoup plus fort.

Procédure de cryptage et d'émission d'un message

Les opérateurs chargés du cryptage des messages devaient suivre une procédure précise établie par l'état-major allemand, concernant le cryptage des messages d'une part, et l'envoi des messages d'autre part.

Comment un opérateur allemand faisait-il pour envoyer un texte tel que celui-ci en l'ayant préalablement crypté à l'aide d'Enigma ?

Auf Befehl des Obersten Befehlshabers sind im Falle, zur Zeit unwahrscheinlichen, Französischen Angriffs die Westbefestigungen jeder zahlenmässigen Überlegenheit zum trotz zu halten.

Il s'agit d'un extrait de message authentique, envoyé par le commandant en chef allemand des armées en septembre 1938. Il signifie :

Sur ordre du commandant en chef, en cas d'attaque des fortifications à l'ouest[193] *par les Français, bien que cela soit improbable pour le moment, ces fortifications doivent être défendues à tout prix, même contre des forces supérieures en nombre.*

Comment crypter ce message sur une machine dont le clavier ne contient que les 26 lettres de l'alphabet ? Tout d'abord, les signes de ponctuation sont codés par des lettres peu fréquentes en allemand, X et Y, X correspondant à un point, et Y à une virgule.

Ensuite, les nombres sont écrits en toutes lettres, et les caractères accentués ä, ö et ü, fréquents dans la langue allemande, sont remplacés par AE, OE et UE, et CH est remplacé par Q. Enfin, les abréviations sont possibles, pourvu que le texte reste intelligible. Zur Zeit deviendra par exemple z.Zt. Notre texte sera donc crypté sous cette forme :

[193] Le message fait probablement allusion à la ligne Siegfried, une ligne de fortifications allemandes faisant face à la ligne Maginot.

AUF BEFEHL DES OBERSTEN BEFEHLSHABERS SIND IM FALLE
Y Z X ZT X UNWAHRSCHEINLICHEN Y FRANZOESISQEN
ANGRIFFS DIE WESTBEFESTIGUNGEN JEDER ZAHLENMAESSIGEN
UEBERLEGENHEIT ZUM TROTZ ZU HALTEN X

Figure 43 General Heinz Guderian's command-post vehicle. An Enigma machine can be seen in use in the bottom left.

Le cryptage des textes requérait deux opérateurs, de manière à éviter les erreurs de saisie et à gagner du temps. Un opérateur chargé du cryptage crypte le texte lettre à lettre en ayant préalablement réglé la machine sur une clef de trois lettres, qu'il choisit et garde en mémoire. À chaque fois qu'une lettre est cryptée, un opérateur radio la note et récupère ainsi le message crypté entier. Ensuite, l'opérateur chargé du cryptage crypte la clef qu'il a gardée en mémoire à son tour, en se servant d'une clef du jour[194] partagée par tous les opérateurs de son armée, et répertoriée sur des documents d'instructions mensuels pour le réglage de la machine Enigma.

Ces documents étaient distribués aux unités de manière secrète, et les officiers devaient tout faire pour qu'ils ne tombent pas dans de mauvaises mains, car si un service de renseignements étranger y avait eu accès, celui-ci aurait été capable de déchiffrer tous les messages allemands[195]. La clef maintenant cryptée constituait l'indicateur, que l'on ajoutait au message crypté avec la date et la désignation du destinataire, pour former le message qui allait être envoyé.

Enfin, l'opérateur radio envoie le message en morse, sur une fréquence radio qui lui était attribuée :

AN HEERESGRUPPENKOMMANDO 2= 2109 -1750 - FRX FRX -
HCALN UQKRQ AXPWT WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV
WBLEB DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ
UPOSY EIPWJ TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH
TYGVH GFICA CVGUV OQFAQ WBKXZ JSQJF ZPEVJ RO -

Ceci n'avait évidemment aucun sens pour quiconque ne possédant ni la machine Enigma, ni la clef du jour.

Pour le destinataire du message, la procédure était analogue à celle du cryptage. Les deux opérateurs qui reçoivent le message chiffré décodent tout d'abord l'indicateur avec la clef du jour. Ils disposent alors de la clef qui a servi à crypter le message. Le décryptage est tout aussi simple : une fois l'orientation des rotors réglée sur la bonne lettre, le premier opérateur entre une à une les lettres du message chiffré. En effet, les opérations de cryptage et de décryptage sont identiques, le procédé de chiffrement étant « symétrique ». Le second opérateur recueille ainsi le texte clair, contenant les ordres pour son unité.

[194] On appelle la clef du jour ainsi, car elle changeait le plus souvent toutes les vingt-quatre heures, mais la durée durant laquelle elle était valide n'était pas la même d'armée en armée et a changé au cours de la guerre. Certaines étaient gardées deux jours, d'autres huit heures seulement.

[195] On retrouve le principe de la cryptographie à clef privée, qui pose le problème de la transmission de la clef de l'émetteur du message à son destinataire. C'est un sujet que nous traiterons plus loin.

Les messages allemands voyageaient sur des fréquences différentes, et cryptés par des versions d'Enigma différentes. Les messages étaient donc dirigés directement vers l'unité appropriée, et cela garantissait aussi qu'un officier de l'armée de terre allemande, par exemple, ne puisse pas avoir accès aux communications d'un officier de la marine. Non seulement parce que cela n'avait pas de sens, pour un char allemand, de décoder un message destiné à un sous-marin, mais en plus, certains messages très secrets n'étaient destinés qu'aux officiers les plus hauts gradés...

Principe et fonctionnement de la machine Enigma

La machine Enigma produit un ***chiffrage par substitution polyalphabétique*** rendu complexe pour éviter tout décryptage.

Nous allons procéder à l'explication du système électromécanique d'un Enigma standard, celle utilisée dans la Wehrmacht. Dans ce modèle, elle se compose de trois éléments reliés par des câbles électriques :

– Un clavier pour entrer le texte clair.

– Un dispositif de cryptage qui remplace chaque lettre du texte clair par une lettre chiffrée.

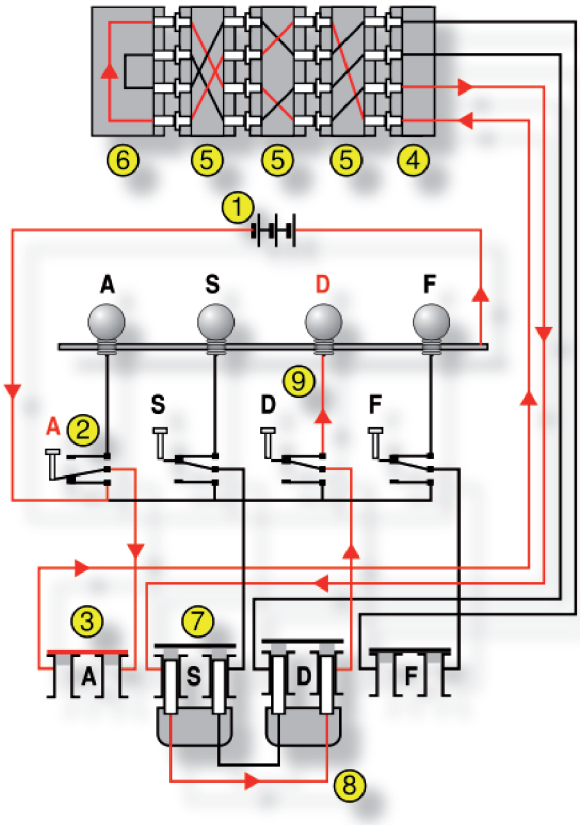
– Un tableau lumineux qui affiche la lettre chiffrée.

Ainsi, lorsqu'on appuie sur une touche du clavier, un courant électrique issu du clavier traverse le dispositif de cryptage et allume une lampe du tableau lumineux qui correspond à une lettre chiffrée.

Nous voyons sur l'illustration de la page précédente les quatre parties principales de la machine, de bas en haut :

- Tableau des fiches, ou tableau de connexions
- Clavier de saisie du texte clair
- Tableau lumineux sur lequel s'affiche le code de la lettre saisie au clavier
- Les 3 rotors mobiles à 26 positions

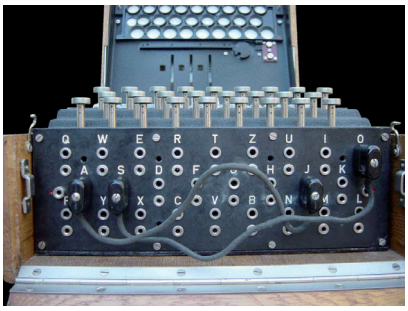
Schéma électrique de la machine et composants



Le codage Enigma effectué par la machine Enigma est à la fois simple et astucieux. Chaque lettre est remplacée par une autre, l'astuce est que la substitution change d'une lettre à l'autre. La machine Enigma est alimentée par une pile électrique. Quand on appuie sur une touche du clavier, un circuit électrique est fermé, et une lampe s'allume qui indique quelle lettre codée l'on substitue.

Concrètement, le circuit électrique est constitué de plusieurs éléments en chaîne :

- le ***tableau de connexions*** : il permet d'échanger des paires de l'alphabet, deux à deux, au moyen de fiches. Il y a 6 fiches qui permettent donc d'échanger 12 lettres. Un tableau de connexions est donc une permutation très particulière où on a échangé au plus 6 paires. Par exemple, dans le tableau suivant (avec simplement 6 lettres), on a échangé A et C, D et F, tandis que B et D restent invariants.



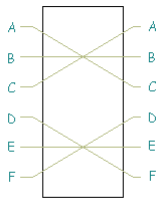
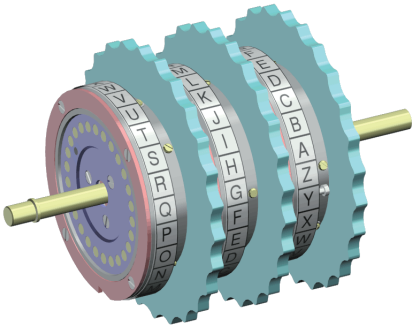


Tableau de connexions

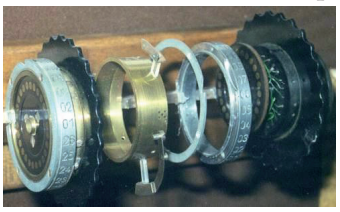
- ***Les rotors*** (aussi appelés roues ou tambours — Walzen en allemand) forment le cœur de la machine Enigma. D'un diamètre d'environ 10 cm, chaque rotor est un disque fabriqué à partir de caoutchouc dur ou de bakélite. Sur une face sont disposés en cercle des contacts électriques à aiguilles, donc équipés de ressorts. Sur l'autre face, le même nombre de contacts plats sont disposés. Les contacts plats et à aiguilles représentent l'alphabet – généralement les 26 lettres (on fera cette supposition dans la suite de cette description, même si parfois des chiffres pouvaient être utilisés suivant le même principe).

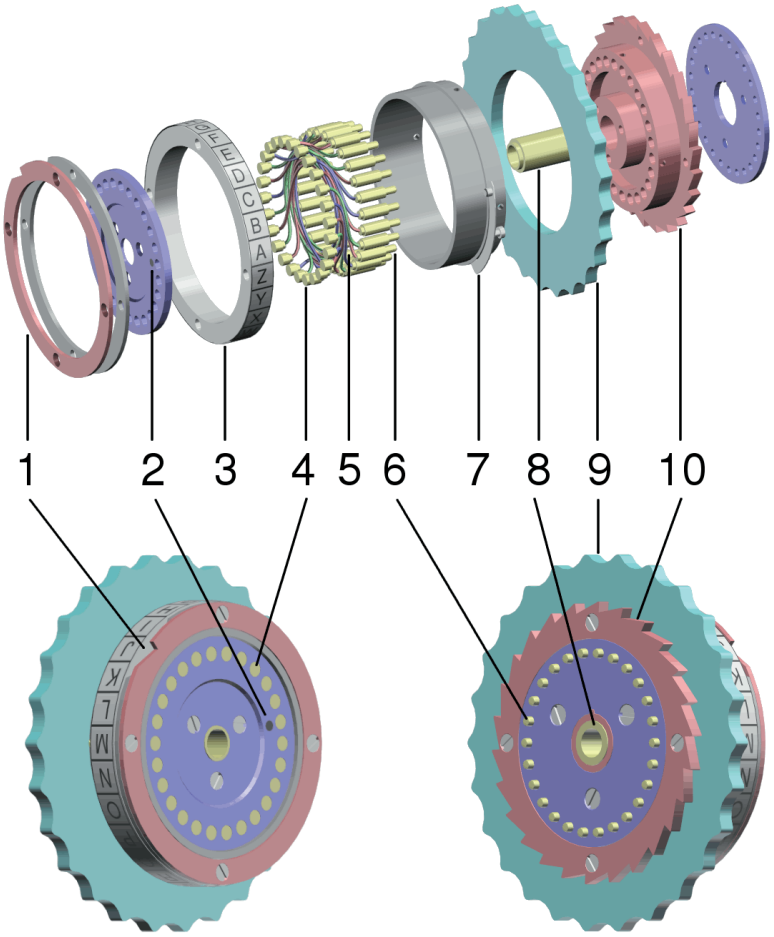


Une fois les rotors assemblés, les contacts à aiguilles d'un rotor se positionnent en face des contacts plats du rotor voisin, formant ainsi la connexion électrique. À l'intérieur du rotor, un ensemble de 26 câbles électriques assurent les connexions entre les contacts à aiguilles et les contacts plats suivant un schéma compliqué, qui permet le chiffrement des lettres. Par exemple, sur un rotor particulier, le premier contacteur d'une face peut être relié au quatorzième contacteur de la face opposée, le deuxième contac-

teur relié au vingt-deuxième de l'autre face, et ainsi de suite. D'un rotor à l'autre, les connexions internes ne sont pas les mêmes. La version d'Enigma utilisée par l'armée allemande et le parti National Socialiste possède un jeu de rotors avec des connexions différentes des versions commerciales.

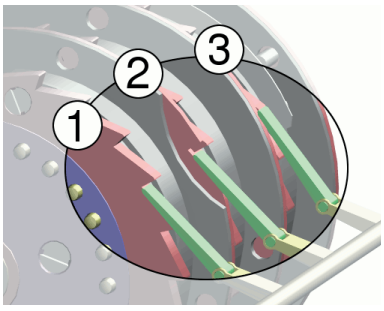
Le rotor utilisé tout seul ne réalise en fait qu'un chiffrement très simple – le *chiffrage par substitution*. Par exemple, le contact à aiguille correspondant à la lettre E peut être connecté sur la face opposée au contact plat de la lettre T. La complexité de la machine Enigma provient de l'utilisation de plusieurs rotors en série, généralement trois ou quatre, ainsi que du mouvement régulier de ces rotors. Lorsque 26 lettres ont été pressées, une came entraîne le rotor de la fente suivante et le fait tourner. L'alphabet de substitution est ainsi modifié à chaque pression de touche. Ces deux mécanismes forment un type de chiffrement beaucoup plus performant.

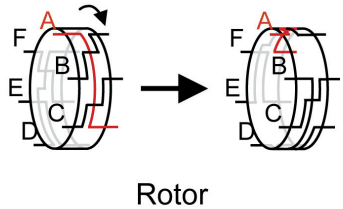




Vue éclatée de l'assemblage des rotors de la machine Enigma.

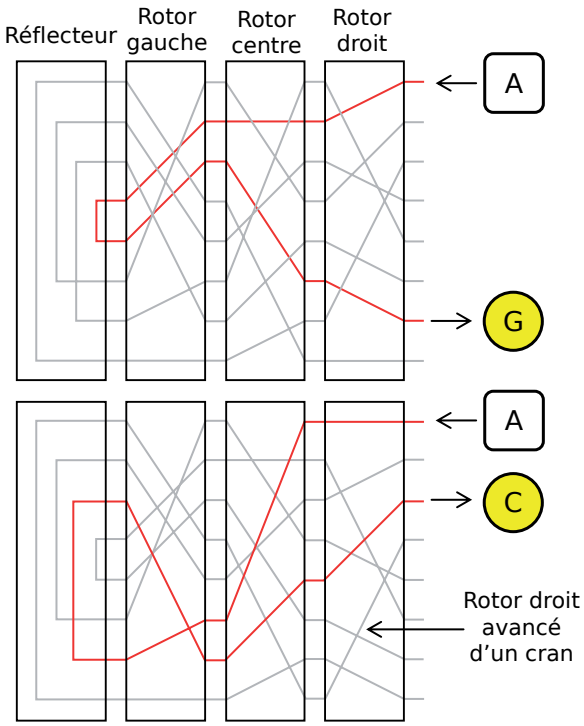
1. Anneau encoché
2. Point indiquant le contact « A » pour l'assemblage
3. Roue de l'alphabet
4. Contacts plats
5. Connexions électriques
6. Contacts à aiguille
7. Anneau élastique de réglage
8. Moyeu
9. Roue dentée de positionnement manuel du rotor
10. Roue à rochet





Un rotor du brouilleur, avant et après avoir tourné : la correspondance entre lettres change après le cryptage d'une lettre.

Chaque rotor comporte enfin une encoche (parfois plusieurs), assurant le contrôle du mouvement du rotor. Dans les versions militaires de la machine Enigma, cette encoche est située directement sur la « roue alphabet » (ci-dessus à droite).



Cryptage effectué par Enigma pour deux lettres consécutives – le courant passe à travers un assemblage de rotors, puis par le réflecteur et enfin à nouveau par les rotors. La lettre A est chiffrée de façon différente pour deux pressions consécutives sur cette même touche, la première étant chiffrée en G, la seconde en C dans cet exemple. Ceci est dû au fait que le rotor droit a tourné d'un pas entre les deux pressions de touche, conduisant à un circuit électrique totalement différent.

Les machines Enigma de l'armée et de l'aviation allemandes étaient équipées de nombreux rotors, trois exactement pour les premières versions. Le 15 décembre 1938, ce nombre fut porté à cinq, dont seulement trois étaient choisis pour être installés dans la machine. Chaque rotor était marqué d'un chiffre romain afin de pouvoir les distinguer : I, II, III, IV et V. Tous n'étaient équipés que d'une seule encoche. La version de la machine Enigma de la Wehrmacht pour la marine a toujours été équipée de plus de rotors que les autres versions. Au départ, cinq rotors équipaient les machines, puis sept et finalement huit. Les rotors supplémentaires étaient numérotés VI, VII et VIII, et avaient donc des connexions électriques différentes des autres rotors. Ils étaient en outre équipés de deux encoches, ce qui entraînait donc une fréquence de rotation différente.

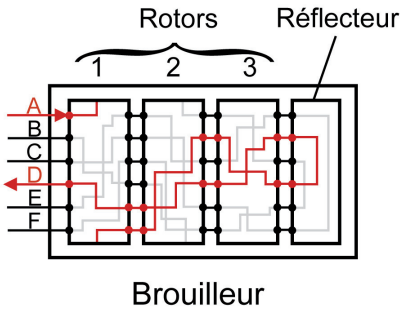
La machine Enigma à quatre rotors de la marine M4 (ci-contre avec imprimante) comptait, elle, quatre rotors dans la machine à la place des trois des autres versions. Ceci fut possible sans modifier grandement la machine, en remplaçant simplement le réflecteur d'origine par un autre beaucoup plus fin et en ajoutant un rotor spécial en quatrième position. Ce quatrième rotor pouvait être de deux types : Beta ou Gamma. Il ne tournait cependant jamais automatiquement, mais pouvait être placé manuellement sur l'une de ses 26 positions par l'opérateur.

Grâce à l'interconnexion aléatoire de chaque rotor, la séquence exacte de ces substitutions dépendait de la position initiale des rotors, de leur ordre d'installation, et du choix des rotors (câblage interne). Ces réglages appelés configuration initiale étaient inscrits dans un livre et changeaient une fois par mois au début de la Seconde Guerre mondiale. Ces changements devinrent de plus en plus fréquents jusqu'à devenir journaliers vers la fin de la guerre, voire plusieurs fois par jour sur certains réseaux.

Le réflecteur

À ce stade des explications, on sait crypter une lettre à l'aide de la machine, mais l'on ne peut, à partir de la lettre chiffrée, retrouver la lettre originale. Il existe un dernier élément à la machine permettant de résoudre ce problème : le réflecteur. Grâce à lui, le chiffrement et le déchiffrement sont « symétriques », c'est-à-dire si F est codé B alors pour une même position des rotors, B est codé F.

Le réflecteur fait partie du brouilleur et est situé après les trois rotors. Lorsqu'on enfonce une touche du clavier, un courant électrique qui en est issu traverse le tableau de fiches puis les trois rotors, le rôle du réflecteur est de renvoyer l'impulsion électrique en sens inverse dans les trois rotors puis de nouveau dans le tableau de fiches, avant qu'elle n'arrive au tableau lumineux pour afficher la lettre correspondante – cryptée ou décryptée (figure ci-contre).



Cependant, le réflecteur a également généré une faiblesse de la machine Enigma largement exploitée plus tard par les cryptanalystes alliés : une lettre ne peut pas être codée par elle-même.

Casser le chiffre d'Enigma : un exploit

La force d'Enigma réside dans le nombre immense de clefs imaginables pour tenter de décrypter un message : si l'on connaît le fonctionnement et les câblages internes de la machine, mais si l'on ne connaît pas la clef avec laquelle il a été crypté, le seul moyen pour parvenir à le lire serait a priori d'essayer toutes les combinaisons possibles. Cela s'appelle le *décryptage par la force brute*. L'exemple d'une Enigma M3 navale nous montre qu'il serait impraticable.

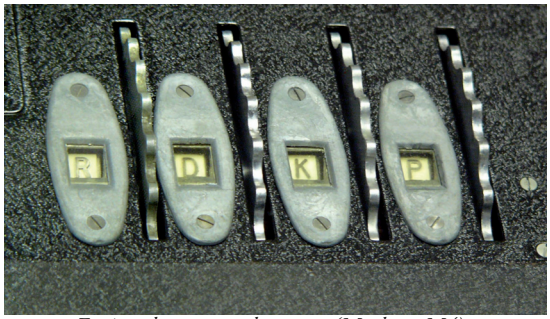
La clef

La clef d'un message se décompose en plusieurs données. Tout d'abord, il faut connaître les composantes de la clef du jour, qui changeaient en général toutes les vingt-quatre heures et étaient les mêmes pour toute une armée, c'est-à-dire :

– L'ordre dans lequel les rotors étaient positionnés : Trois rotors sont choisis sur cinq disponibles, numérotés de I à V, et placés sur la machine dans un ordre bien déterminé.

– Le placement de la bague : Chaque rotor placé a un décalage de la bague déterminé, chaque bague d'un rotor pouvant être mise dans vingt-six positions différentes.

Étant donné que la bague ajoute peu à la force du cryptage, on ne la prendra pas en compte pour calculer le nombre de clefs. En effet, même si l'on ne connaît pas son réglage, on pourra retrouver des portions de texte clair, étant donné qu'elle n'introduit qu'un décalage au niveau de l'orientation des rotors et de leur rotation.



Fenêtre de position des rotors (Machine M4)

– Les couples de lettres interchangées : Le tableau de fiches était également fixé pour la journée. Dix fiches sont ainsi branchées lors de l'utilisation de la machine.

Enfin, il faut connaître la composante de la clef propre au message. Il s'agit de l'orientation des rotors : chaque

rotor était tourné de telle sorte à ce que dans une fenêtre laissant apparaître les lettres inscrites sur la bague, apparaisse une lettre constituante de la clef. Vingt-six alignements étaient donc possibles par rotor.

Nombre de réglages possibles pour l'orientation des rotors et de leurs bagues

Le nombre d'orientations des rotors s'élève à 26^3, car l'on a 26 positions pour chacun des trois rotors.

$$\text{Nombre d'orientations des rotors} = 26^3$$

Nombre de réglages possibles au niveau de l'ordre des rotors

Ce nombre correspond au nombre de choix différents existants de trois éléments d'un ensemble en contenant cinq. On utilise une formule mathématique de dénombrement[196].

Il s'agit du nombre d'*arrangements* de 3 parmi 5 :

$$\begin{aligned}\text{nombre d'ordres des rotors} &= A_5^3 \\ &= \frac{5!}{(5-3)!} \\ &= 60\end{aligned}$$

Nombre de réglages possibles au niveau du tableau de fiches

Dix fiches étaient branchées au niveau du tableau de chiffres. On considère ce chiffre constant, car si l'on prenait en compte le fait qu'on pouvait brancher autant de fiches que l'on voulait, on obtiendrait un nombre de combinaisons bien plus important, mais qui ne correspondrait pas à l'utilisation réelle que les militaires faisaient d'Enigma.

Si l'on branche dix fiches au tableau de fiches, on va choisir dix couples de lettres toutes différentes entre elles. On va chercher à dénombrer ces choix possibles, sachant que l'ordre dans lequel le choix a été effectué ne compte pas. On utilise une autre formule du dénombrement, le nombre de *combinaisons de p parmi n*, C_n^p avec lequel l'ordre du choix n'a pas d'importance.

Prenons n pour nombre de fiches que nous nous apprêtons à brancher. On va tout d'abord choisir les $2n$ lettres qui seront reliées parmi les vingt-six pos- C_{26}^{2n} sibilités se présentent à nous pour ce choix. Parmi ces $2n$ lettres, nous choisissons la première paire, choix pour lequel nous avons possibi- C_{2n}^2 lités. Pour la deuxième paire, nous avons, et ain- $C_{2(n-1)}^2$ si de suite jusqu'à la n-ième paire, pour laquelle nous disposons de possibili- C_2^2 tés. Mais n'oublions pas que l'ordre dans lequel les fiches ont été choisies ne compte pas. On doit donc diviser le nombre de paires par le nombre de duplicata dans notre dénombrement. Nous avons choisi n paires, chacune de ces paires a été dénombrée de $n!$ manières différentes, et l'on doit donc diviser notre résultat par ce nombre.

Le nombre de possibilités lors du choix des $2n$ lettres à brancher, puis lors du choix de chacune des n paires, se multiplient entre elles, et l'on obtient, pour un cas général, le nombre de possibilités pour brancher n fiches au tableau de fiches :

$$\text{nombre de réglages de } n \text{ fiches} = \frac{C_{26}^{2n} \times \prod_{i=0}^{n-1} C_{2(n-i)}^2}{n!}$$

[196] Dénombrement : Le dénombrement s'intéresse à établir le compte des éléments d'un ensemble donné, ou des possibilités qui s'offrent à nous lors d'un choix donné. Dans des situations qui peuvent être complexes, les mathématiciens disposent de formules générales.

On obtient le compte final pour dix fiches après une simple application numérique :

$$\begin{aligned}\text{nombre de réglages de 10 fiches} &= \frac{C_{26}^{20} \times \prod_{i=0}^{9} C_{2(10-i)}^{2} \times \frac{1}{10!}}{n!} \\ &= \frac{26!}{20! \times 6!} \times \frac{20 \times 19}{2} \times \frac{18 \times 17}{2} \times \cdots \times \frac{2 \times 1}{2} \times \frac{1}{10!} \\ &= \frac{26!}{20! \times 6!} \times \frac{20!}{2^{10}} \times \frac{1}{10!} \\ &= \frac{26!}{6! \times 2^{10} \times 10!} \\ &= 1\,507\,382\,749\,377\,250\end{aligned}$$

Nombre de clefs différentes possibles

On multiplie les nombres de possibilités de chaque composante pour obtenir le nombre de clefs possibles.

nombre de clefs = nombre d'ordres des rotors
× nombres de réglages de 10 fiches
× nombre d'orientations des rotors

On obtient ainsi que le nombre de clefs qui existent pour une Enigma M3 est de 16 milliards de milliards. Si l'on parvenait à tester toutes les clefs une à une à raison d'une par seconde, le message serait décrypté au bout de cinq mille milliards d'années ! Ce chiffre impressionnant est obtenu grâce à l'adjonction d'un tableau de fiches qui augmente considérablement le nombre de clefs, mais la véritable force de la machine vient du brouilleur, car sans lui, la machine n'effectuerait qu'un cryptage monoalphabétique, que l'on savait déjà décrypter cinq siècles plus tôt.

Comparatif de différentes machines Enigma

D'après les chiffres du tableau suivant, cela pouvait sembler insensé de tenter le décryptage du code Enigma. Cela était-il pourtant irréalisable ? Tout comme nous l'avons vu précédemment, le fait qu'un code ait un nombre immense de clefs possibles ne signifie pas qu'il est invincible : le chiffrement par substitution monoalphabétique a beau proposer 4×1026 clefs différentes, il est l'un des moins sécurisés. Il en va de même pour Enigma, qui possédait des failles qui permirent aux alliés de le briser.

De manière plus simple, on peut dire qu'Enigma possède une banque de 26 x 26 x 26 = 17 576 alphabets de substitution pour toute combinaison de trois rotors. La séquence d'utilisation de ces alphabets varie selon que l'on met les rotors en position ABC, ou ACB, etc. Et tant que le message ne dépasse pas 17 576 caractères, il n'y a aucune répétition de l'alphabet de substitution. Pourtant, cette « clé » peut être communiquée de manière très facile à un autre utilisateur : il s'agit de valeurs très simples, du type numéro de rotors, position de l'anneau et position de départ.

Version de la machine Enigma	C	Wehrmacht	M3	M4
Utilisation	Version vendue dans le commerce	Version utilisée par la Wehrmacht et la Luftwaffe	Version utilisée par la Kriegsmarine	Remplaça l'Enigma M3 en 1942
Nombre de rotors alignés	3 *(le réflecteur tourne également)*	3	3	4 *(le dernier est choisi à part parmi deux)*
Nombre de rotors total	3	3	5	8
Nombre de fiches branchées	0 *(version sans tableau de fiches)*	10	10	10
Agencement des rotors	6	6	60	672
Orientations des rotors	456 976	17 576	17 576	456 976
Réglages des fiches	1	$1,51 \times 10^{14}$	$1,51 \times 10^{14}$	$1,51 \times 10^{14}$
Nombre de clefs	$2,74 \times 10^{6}$	$1,59 \times 10^{19}$	$1,59 \times 10^{20}$	$4,64 \times 10^{22}$
En testant une combinaison par seconde...	**1 mois**	$\mathbf{5,04 \times 10^{11}}$ **ans**	$\mathbf{5,04 \times 10^{12}}$ **ans**	$\mathbf{1,47 \times 10^{15}}$ **ans**

```
- 83 - ADJ JNA -
LMHNX WEKLM UERDS EVHLC JSQQK VLDES ANEVT YEDGI ZQDOD RMDKG
SXGSQ SHDQP VIEAP IENLI CLZCL LAGWC BJZD

- 149 - TLS CMU -
FTMKV DRJMG FBUDK LZCTR FLTUU IWVJL OYKYX GDCKJ TMDFB WNLZQ
JAXHP GGKFG SBZOQ KQKUK TINMH BAJOO AUILA QVFTK LSTMM XGAQL
CNHUW LFHKA ULTXT BIVIF EWWDY PUCNS TPJHR OBWHE KYUSB CANYC
W

- 167 - MRJ LLT -
KLIBM ERJAR WMMHJ STHOY OOIQB HSSZU EOOKF TASXN XVYWE SCTCH
NRNBL ZPEBH XPAQE DFNYS XHMNI HRARO UNBMD ZRZDN WTGUI UCBZN
ZTFJA EKOMJ AZILN RKVFD UNIEW ILZVL KQYYJ ANKXG NNNHT EMAVD
FXKAY MLWCV QDFWX LO

- 186 - DOQ VHZ -
PBNXA SMDAX NOOYH RCZGV VZCBI GIBGW HMXKR RVQCF JCZPT UNSWA
DDSTI GQQCS AGPKR XXLOM GFXAP HHMRF SDKYT MYPMV ROHAS QYRWF
WVAVG CCUDB IBXXD YZSAC JSYOT MWUCN WOMHH JPYWD CCLUP GSWCL
MBCZS SYXPG MGMQX AUFUL NOZEQ ENHEI ZZAKL C

- 195 - EHW TNH -
ABTWU GWDMP OGKMQ KBHGK HROUP RMYQY INHSA MWFBP CDQRG LDBFK
YNXPP DIQHE AOIFQ AOLRZ ZFPDJ MCGEC TAHHQ MVUYA JIAWM WSOYU
UTLEP AVZKG HJWCD LOQHW IMSTC LQDNP VCFCN FRUYR GSSJH ORQMU
IFFYU WYNTA XPYIX MYTEE FTDCV EHUOA DCPLM APCAU JJYUK
```

Aspect des messages produits avec ENIGMA

Contexte historique des années 20.

En 1923, la Royal Navy publia son histoire officielle de la Première Guerre mondiale. Dans ce texte, on rappelait les avantages décisifs apportés aux Alliés par l'interception et la cryptanalyse des messages allemands. Ces prouesses du renseignement britannique constituaient une condamnation implicite pour la sécurité allemande.

Il faut dire que bien après la fin de la guerre, le « *Bureau 40* »[197] décryptait régulièrement tous les messages allemands...

Cette situation de supériorité des alliés provoqua le relâchement de la cryptanalyse alliée, et du reste les effectifs du Bureau 40 fondirent et devinrent moins compétents.

La situation de la Pologne était quant à elle bien différente. Ce pays remembré après le traité de Versailles en 1919 était constamment sous la menace de ses voisins. Ainsi, le territoire de *Cieszyn* (Teschen) fut partagé en juillet 1920 entre la Pologne et la Tchécoslovaquie dans des conditions qui mécontentèrent les deux pays. La question des frontières orientales était encore plus délicate. Profitant de la guerre civile en Russie, la République polonaise souhaitait récupérer les territoires qu'elle possédait lors de sa plus grande extension au XVI^{e} siècle. Aussi refusa-t-elle la *ligne Curzon*[198] et lança-t-elle vers le sud-est une offensive qui conduisit ses troupes à Kiev en mai 1920.

En décembre 1919, les pouvoirs Alliés firent la déclaration suivante :

« *Les Principaux Pouvoirs Alliés et Associés, reconnaissant qu'il est important de mettre fin aussitôt que possible aux conditions d'incertitude politique dans laquelle la nation polonaise est placée actuellement, et sans préjuger les décisions qui doivent dans l'avenir préciser les frontières orientales de la Pologne, déclarent par la présente qu'ils reconnaissent le droit du Gouvernement polonais, selon les conditions auparavant définies par*

[197] Service de renseignement de l'Amirauté dirigé par l'amiral William R. Hall

[198] La ligne Curzon est une ligne de démarcation proposée pendant la guerre russo-polonaise de 1919-20 par le Ministre des Affaires étrangères britannique, Lord Curzon, comme une ligne d'armistice possible entre la Pologne, à l'ouest, et la Russie à l'est. Ce plan Curzon ne fut pas accepté par la nouvelle Union soviétique et, en fait, ne joua aucun rôle dans la fixation de la frontière en 1921 à cause des exigences polonaises. Finalement le traité de paix de Riga (1921) laissa à la Pologne près de 135.000 km² de territoire à l'est de la ligne (la frontière passait à environ 200 km de la ligne Curzon).

le Traité avec la Pologne du 28 juin 1919, à organiser une administration régulière des territoires de l'ancien Empire russe situé à l'ouest de la ligne ci-dessous décrite. Les droits que la Pologne peut être capable d'établir sur les territoires situés à l'est de ladite ligne sont expressément réservés. »

En mai 1920, pendant la guerre russo-polonaise de 1919-1921, les Bolcheviques eurent l'avantage et pénétrèrent en Pologne ; en juillet, les Polonais demandèrent aux Alliés d'intervenir. Le 11 juillet, Lord Curzon of Kedleston proposa au gouvernement soviétique un cessez-le-feu le long de la ligne qui avait été suggérée l'année précédente. Les Soviets, croyant avoir l'avantage, rejetèrent la proposition et les combats continuèrent. En août les Soviets furent vaincus sous les murs de Varsovie et forcés à se retirer. Au Traité de Riga en mars de 1921 les Soviets durent concéder une frontière bien plus à l'est de la Ligne Curzon, laissant à la Pologne aussi bien Lwów que Wilno (aujourd'hui Vilnius). La région autour de Wilno, appelée Lituanie Centrale, fit en 1922 l'objet d'un référendum, suivi par l'incorporation à la Pologne conformément au vœu de 65% des votants. La frontière polono-soviétique fut reconnue par la Société des Nations en 1923 et confirmée par divers accords entre les deux pays.

Biuro Szyfrów

L'instinct de survie poussa donc la Pologne à garder ses dangereux voisins sous surveillance, et dès 1920 fut fondé le ***Biuro Szyfrów*** (Bureau du Chiffre).

Dans cette seule année, il permit de déchiffrer plus de 400 messages en provenance de Russie tout en contrôlant toujours efficacement les communications allemandes.

Ce contrôle des communications chiffrées allemandes dura jusqu'en 1926, date de mise en service par les Allemands de la machine Enigma.

Le capitaine Maksymilian Ciezki était au Biuro Szyfrów, le responsable du déchiffrement des messages allemands.

Ciezki était un patriote qui avait grandi dans la ville de Szamotuty, un des foyers du nationalisme polonais. Celui-ci observa que les nouveaux messages étaient tous précédés d'un mot-clé de six lettres, mais ne put établir de lien entre eux et le message. Les cryptanalystes furent bientôt convaincus que ces textes avaient été chiffrés à l'aide d'une machine à crypter et non plus à la main comme il était alors d'usage.

Enigma conservée au musée de Varsovie

Ils se procurèrent une Enigma commerciale pour en analyser le principe, mais la version commerciale différait de la version militaire, notamment par l'agencement des fils à l'intérieur des rotors.

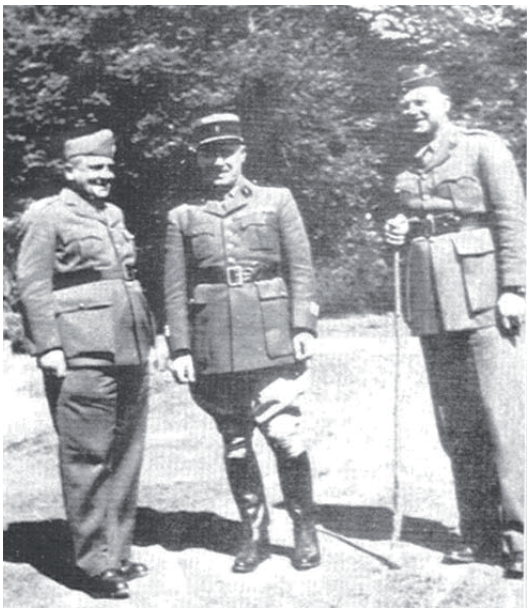
Le maillon faible, comme toujours, fut l'élément humain. C'est un espion allemand qui permit au bureau du chiffre polonais de se lancer à l'attaque d'Enigma.

Deuxième fils d'un professeur distingué, Hans-Thilo Schmidt était né à Berlin. Il avait fait carrière dans l'armée, il avait participé à la Première Guerre mondiale, mais ne fut pas maintenu dans les effectifs militaires après les réductions imposées par le traité de Versailles. Il tenta de se faire un nom avec une usine de savon, mais fit faillite suite à la dépression des années 30. Il se trouva démuni avec une famille à charge et fit appel à son frère aîné, Rudolph, resté dans l'armée, promu en 1925 à la tête du *Corps des Signaux*.

C'est lui qui, responsable de la sécurité des communications allemandes, avait imposé l'usage d'Enigma dans l'armée.

Rudolph trouva un poste à son frère Hans-Thilo dans le *Chiffrierstelle*, à Berlin, le bureau chargé de gérer les communications allemandes. C'était en fait le poste de commande d'Enigma, un établissement ultra secret où l'on manipulait des informations hautement sensibles...

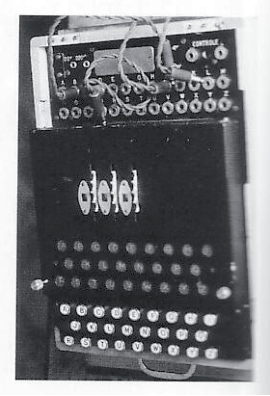
Quand Hans-Thilo déménagea, il laissa sa famille en Bavière où le coût de la vie restait raisonnable. Il vécut donc seul à Berlin, pauvre et isolé, jaloux de son frère, et animé d'un profond ressentiment envers une nation par laquelle il se sentait rejeté. Le résultat ne se fit pas attendre : en vendant des informations sur Enigma, il pouvait à la fois gagner de l'argent et se venger en portant préjudice à son pays.



Hans-Thilo Schmidt prit contact avec les services de renseignements français et rencontra le 8 novembre 1931, à Verviers en Belgique, un agent français nommé Rodolphe Lemoine (nom de code : *Rex*) ainsi qu'un cryptographe français, Gustave Bertrand (au centre sur la photo)

En échange de 10 000 marks, il permit à *Rex* de photographier deux documents : *Gebrauchsanweisung für die Chieffriermaschine Enigma*, les instructions pour l'utilisation de la machine Enigma, et *Schlüsselanleitungen für die Chieffriermaschine Enigma*, les directives pour fixer une clef sur Enigma. Pourtant, les cryptographes français jugèrent assez vite que ces documents ne les aidaient en rien à déchiffrer Enigma, tout au plus leur permettaient-ils de connaître les éléments constitutifs d'Enigma. Les Français mirent également les Anglais au courant de ces informations, mais ces derniers ne surent en tirer profit davantage.

Dix ans auparavant, les Français avaient signé un accord de coopération militaire avec les Polonais. Ces derniers avaient insisté pour être informés de tout ce qui concernait Enigma, et les Français communiquèrent donc simplement les copies des documents de Schmitd (rebaptisé *Asche*) à leur allié. Ils laissèrent le soin au Biuro Szyfrów de poursuivre la tâche qu'ils jugeaient sans espoir.



Les documents fournis par Hans-Thilo Schmidt à l'occasion d'autres rencontres avec les agents alliés permirent de comprendre le fonctionnement de base de la machine Enigma et de construire une machine prototype avec trois rotors et le tableau de connexion qui n'existait pas sur la machine commerciale. Ils avaient d'autre part obtenu les clés quotidiennes d'Enigma pour certaines périodes.

Geheim! Sonder - Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IM SN UY DF GV LJ BO KX	vyj
30.	III V II	Y V P	OR KI JV OU ZN KU DF YC BS GP	cqr
29.	V IV I	O H R	UX JC FB DR TA ED ST BS LU FI	vnf

Datum : Jour du mois

Walzenlage : Agencement des rotors dans le brouilleur

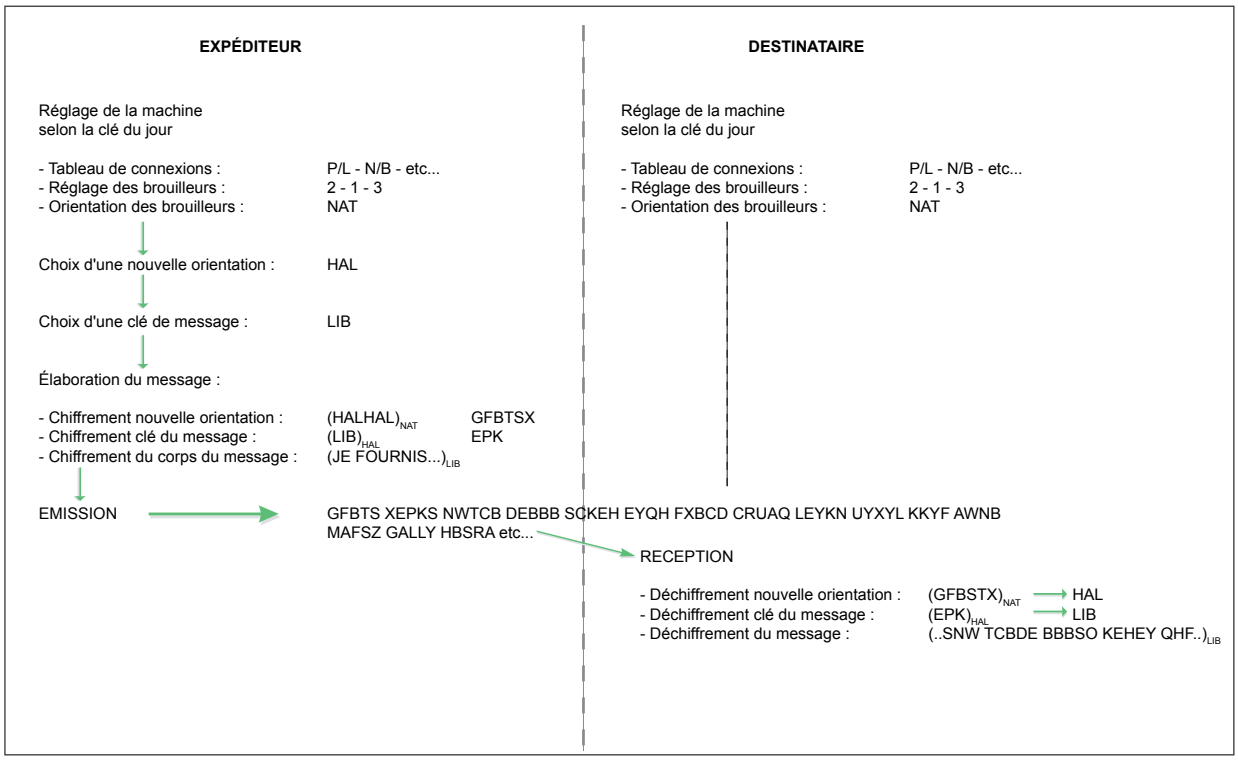
Ringstellung : Réglage de la bague (positions des rotors)

Steckerverbindungen : Couples interchangés au niveau du tableau des fiches

Nota : Sur la reproduction jointe, figure un code supplémentaire : Grundstellung qui ne fut utilisé que plus tard sur les machines de la marine.

Les Allemands, spécialistes du chiffre eurent l'intelligence de ne pas se contenter d'utiliser directement le livre de code pour coder les messages du jour, mais seulement pour crypter la position des rotors pour le message concerné (clé du message). Cette nouvelle position était laissée au choix de l'opérateur. Nous verrons plus loin que ce fut une autre erreur introduisant une faille supplémentaire. Car bien que la procédure de cryptage voulut que l'on évite absolument toute répétition, ennemi du cryptage qui offre une voie d'accès au décryptage, les opérateurs allemands plaçaient en tête de message le message-clé indiquant la nouvelle position des trois rotors, et ceci répété deux fois[199]… et bien entendu crypté selon la procédure du livre de codes. Il y avait là une petite prise pour dérouler le fil du cryptage.

La figure ci-dessous donne les éléments du protocole.

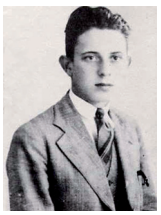


En 1929, le Bureau du Chiffre polonais, pour s'adapter à la mécanisation du codage recruta des mathématiciens. Jusqu'alors, la cryptanalyse était plutôt l'affaire des linguistes et autres spécialistes des formes du langage. Le Biuro Szyfrów organisa le recrutement de vingt mathématiciens tous appartenant à l'université de Poznam (Poznam, à l'ouest du pays avait fait partie de l'Allemagne jusqu'en 1918). Tous ces mathématiciens parlaient donc couramment l'allemand.

Trois des nouvelles recrues montrèrent une aptitude particulière à résoudre des chiffres :

Marian Rejewski (1905-1980)

Ce mathématicien n'eut pas conscience, d'abord, que sa découverte allait contribuer à précipiter la fin du Troisième Reich. Il est le seul des trois grands cryptologues polonais à être rentré en Pologne après la fin de la guerre. Il y retrouva sa femme et ses deux enfants.



Jerzy Rózycki (1909-1942)

Travailla pendant la guerre dans des centres secrets de cryptologie en France et en Algérie. Séparé de sa femme et de son enfant de quelques mois, lors du bombardement de

[199] Pour éviter les erreurs de transmission en morse ou les interférences radio. On verra une fois de plus ici que le « mieux » est l'ennemi du « bien » !

Varsovie, Jerzy Rózycki périt le 12 janvier 1942 dans le naufrage du bateau « Lamoricière » au large de l'Angleterre.

Henryk Zygalski (1907-1978)

Mathématicien et pianiste amateur. Après la guerre, il demeura en Grande-Bretagne, où il travailla dans un collège polonais. Il finit ses jours à Plymouth.

C'était Marian Rejewski qui dirigeait les travaux d'attaque d'Enigma.

Par une inspiration extraordinaire, Marian Rejewski réussit à trouver la faille dans la conception même d'Enigma. Sa stratégie se basait sur le fait que chaque jour, les six premières lettres de tous les messages d'une armée étaient chiffrées avec la même clef du jour. Chaque message allemand avait donc sa propre clef qui était annoncée en début de message en utilisant cette clef du jour. Ainsi Rejewski pouvait par exemple recevoir quatre messages commençant par les indicateurs suivants :

1er message LOKRGM...
2e message MVTXZE...
3e message JKTMPE...
4e message DVYPZX...

Pour chaque message, la première et la quatrième lettre sont deux chiffrements de la même lettre, à savoir la première lettre du message-clef. De même pour la deuxième et la cinquième lettre, ainsi que pour la troisième et la sixième lettre, qui chiffrent respectivement la même lettre. Prenons par exemple le premier message : L et R chiffrent la même lettre. Cette lettre est chiffrée différemment, car entre ces deux cryptages, le brouilleur a tourné trois fois.

Rejewski découvrit que ce lien entre L et R dépendait du positionnement initial de la machine, il releva alors toutes les relations entre la première et la quatrième lettre dans un tableau. En considérant les quatre messages ci-dessus, on peut reconstruire ce tableau :

1re lettre ABCDEFGHIJKLMNOPQRSTUVWXYZ
4ème lettre ---P-----M-RX----------

Si Rejewski avait accès à suffisamment de messages, il pouvait compléter l'alphabet des relations. Il aboutissait alors à un tableau comme celui-ci :

1re lettre ABCDEFGHIJKLMNOPQRSTUVWXYZ
4e lettre FQHPLWOGBMVRXUYCZITNJEASDK

C'est là que Rejewski eut une inspiration. Si la clef du jour utilisée pour coder ces messages avait été différente, ce tableau aurait été lui aussi entièrement différent. Il remarqua aussi que ce qui crée la complexité de la machine, c'est son tableau de connexions augmentant de $1{,}5\times10^{14}$ fois le nombre de clefs possibles pour coder un message.

Il cherchait donc un moyen d'annuler les permutations effectuées au niveau du tableau de connexions. En fin de compte, il se pencha sur un modèle qui impliquait des chaînes de lettres. Dans le tableau ci-dessus, le A de la rangée supérieure est lié au F de la rangée du bas, aussi se reporta-t-il au F de la rangée supérieure. Il est lié au W, aussi chercha-t-il le W de la rangée supérieure. Ce W est lié au A, qui est justement la lettre avec laquelle il avait commencé. La boucle était bouclée.

Avec les autres lettres de l'alphabet, Rejewski généra d'autres chaînes, il les nota toutes ainsi que le nombre de liens pour chacune d'entre elles. Il aboutit à quatre chaînes :

– A—F—W—A : 3 liens
– B—Q—Z—K—V—E—L—R—I—B : 9 liens
– C—H—G—O—Y—D—P—C : 7 liens
– J—M—X—S—T—N—U—J : 7 liens

Jusqu'ici, nous n'avons considéré que les liens entre la première et la quatrième lettre des six lettres formant le message-clef. Rejewski, lui, répéta cet exercice pour les relations entre les deuxième et cinquième lettres et les troisième et sixième lettres, établissant pour chaque cas le nombre de chaînes et de

liens dans chaque chaîne. Il remarqua que le nombre de chaînes changeait chaque jour de même que le nombre de liens dans chaque chaîne.

Toutefois il remarqua en construisant ces chaînes qu'il ne pouvait y avoir que 3 configurations différentes, encore appelées structures cycliques :

– 2 chaînes de 13 liens chacun.

– 6 chaînes respectivement de 9, 9, 3, 3, 1 et 1 liens chacun.

– 6 chaînes de 10, 10, 2, 2, 1 et 1 liens chacun.

Notons que l'exemple précédent qui contient 4 chaînes de 9, 7, 7 et 3 liens chacun ne correspond donc pas à une authentique structure cyclique. À partir d'ici, Rejewski s'écarte réellement des anciennes méthodes de décryptage s'appuyant des analyses statistiques et pour la première fois une théorie mathématique sera utilisée : la théorie des permutations[200].

Le résultat précédent permet donc de conclure que la structure cyclique d'Enigma dépendait uniquement du brouilleur et que le tableau de fiches n'avait sur elle aucune influence. En d'autres termes, les cryptanalystes polonais pouvaient désormais ignorer le tableau de fiches, ce qui leur simplifiait grandement la tâche puisque c'est essentiellement le tableau de fiches qui créait la complexité en multipliant par un facteur de 1 507 382 749 377 250 le nombre de possibilités différentes pour coder un message.

La structure cyclique que Rejewski avait découverte était produite par la substitution générée par le rotor le plus à droite dans le brouilleur encore appelé rotor rapide, car c'est celui qui tourne d'un cran à chaque fois qu'une lettre est tapée sur le clavier. En effet dans 21 cas sur 26 les rotors du milieu et de droite restaient fixes pendant que l'opérateur tapait les six lettres du mot-clef, on peut donc raisonnablement les supposer immobiles. Rejewski utilisa alors ces structures cycliques pour établir six équations qui, une fois résolues, mettraient à jour les câblages internes du rotor rapide.

Mais les inconnues de ces équations n'étaient pas si simples et pour cause : il s'agissait de collections de 26 éléments chacune. Il s'attacha alors à résoudre ce système fort complexe, mais le nombre d'inconnues le submergea. Il devint clair à Ciezki, qui lui rendait visite de temps en temps dans son bureau solitaire, que Rejewski ne trouverait pas la solution tout seul. Ciezki se résolut alors à lui fournir les informations de Hans Thilo Schmidt, qu'il lui avait volontairement cachées afin de ne pas rendre la cryptanalyse polonaise dépendante des dons de la France.

La connaissance des carnets de code permit immédiatement de dévoiler certaines inconnues et de simplifier le reste des équations. Mais elles restaient complexes et Rejewski continua de se débattre avec elles pendant plusieurs semaines. Un jour il se rendit compte que ses suppositions sur les câblages entre le clavier et la plaque d'entrée (*Eintrittswalze*, en amont du brouilleur) pouvaient être erronées. Il avait en effet supposé que la lettre `Q` du clavier était reliée à la lettre `A` de la plaque d'entrée, la lettre `W` à la lettre `B`, et ainsi de suite dans l'ordre des lettres sur le clavier, selon les observations qu'il avait faites sur la version commerciale de l'Enigma achetée par le Biuro Szyfròw. Peut-être que la lettre `A` du clavier était simplement reliée à la lettre `A` de la plaque d'entrée. Il ajusta alors ces équations et des solutions satisfaisantes se présentèrent : le cryptanalyste polonais venait de mettre à jour le câblage interne du rotor rapide, nous étions en décembre 1932. Mais ce succès ne permettait pas encore de reconstruire une machine Enigma, car seul un rotor était maintenant entièrement connu. Par chance, à cette époque-là les Allemands changeaient l'ordre des rotors dans le brouilleur tous les trois mois. Ainsi, Rejewski put de servir de la même technique que précédemment, en même temps que des informations fournies par l'espion allemand, pour découvrir les câblages des autres rotors lorsqu'ils occupaient la position de droite dans le brouilleur.

[200] Dans cette théorie, nous disposons de fonctions mathématiques qui opèrent des permutations entre les éléments d'un ensemble donné, en associant à chacun des éléments de cet ensemble un autre élément de l'ensemble, et ce de manière réversible, à l'instar des substitutions de lettres effectuées par les rotors d'une machine Enigma. Ces fonctions s'appellent des permutations.

Le long travail du Bureau du Chiffre

Bâtiment au Bois de Kabaty à Varsovie, siège du bureau de codes dans les années 30

Une fois les rotors connus, le bureau du chiffre polonais put construire une réplique d'Enigma. Mais cela ne lui permit pas encore de lire les messages allemands, car l'atout d'Enigma réside dans le fait que même en possession d'une machine, un ennemi ne pourrait lire un message crypté sans en connaître la clef. Rejewski et son équipe de cryptanalystes étaient donc maintenant face à un nouveau défi. Utilisant les clefs fournies par Hans Thilo Schmidt, ils avaient pu reconstruire Enigma, et maintenant, utilisant leur réplique, ils avaient à retrouver les messages-clefs quotidiens pour pouvoir déchiffrer les messages comme le faisaient chaque jour des milliers d'opérateurs allemands.

L'équipe du Biuro Szyfròw commença alors à répertorier les structures cycliques qu'engendraient chacune des 105 456 dispositions initiales du brouilleur. Cela lui prit un an pour terminer ce répertoire, mais à l'issue de ce travail, les cryptogrammes allemands étaient en mesure d'être décryptés. Chaque jour, Rejewski collectait le maximum de messages allemands et notait les six premières lettres qui constituaient le message-clef pour ensuite dresser des chaînes comme nous l'avons vu précédemment. Il pouvait alors consulter son répertoire qui contenait toutes les dispositions du brouilleur indexées suivant les sortes de chaînes. Il en déduisait la clef du jour concernant l'agencement et l'orientation des rotors. Il lui restait alors à trouver les connexions du tableau de fiches : il entrait un message crypté dans la machine Enigma avec la disposition correcte du brouilleur et effectuait ensuite une analyse statistique des fréquences de lettres pour retrouver la permutation effectuée par le tableau de connexions.

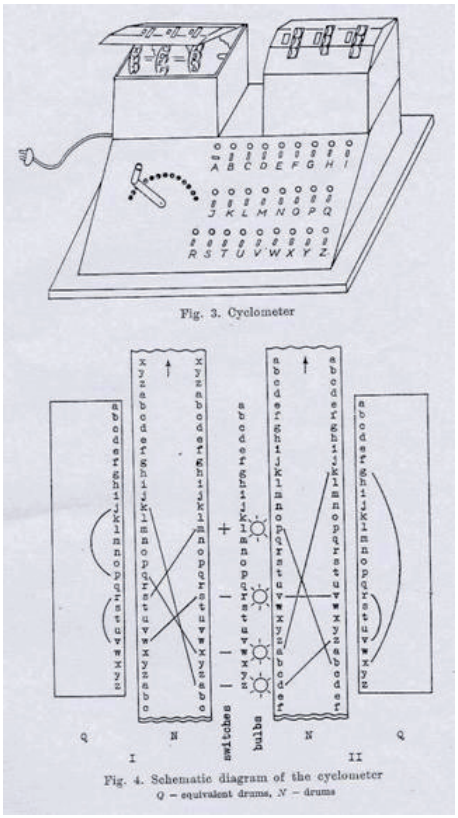


Fig. 3. Cyclometer

Fig. 4. Schematic diagram of the cyclometer
Q – equivalent drums, N – drums

Ainsi, les travaux de Rejewski avaient rendu les communications allemandes transparentes. Mais il ne s'arrêta pas en si bon chemin et se servit de la mécanisation pour automatiser le processus de cryptanalyse en inventant une machine à casser le chiffre d'Enigma : *la Bombe* (également appelé cyclomètre).

Cette machine était capable de vérifier les 17 546 alignements possibles des rotors assez rapidement : en quelques heures, voire une journée. Six machines furent construites afin de vérifier en même temps les six placements possibles des rotors. Mois après mois, l'équipe de Rejewski dut réparer les défaillances des bombes et traiter un flot ininterrompu de cryptages interceptés.

Leurs vies étaient consacrées à la poursuite de la clef du jour. Ce qu'ignoraient les briseurs de codes polonais, c'est que le directeur du Biuro, le major Gwido Langer avait déjà les clefs du jour d'Enigma qu'il tenaient bien cachées dans son bureau !

En effet, Langer, par l'intermédiaire des Français, continuait de recevoir des renseignements procurés par Hans-Thilo Schmidt. À chaque entrevue, celui-ci remettait un ou plusieurs carnets de code. Il en fournit environ pour trente-huit mois au total… Langer jugea plus habile de ne pas révéler à Rejewski l'existence de ces clés afin de se préparer pour l'époque inévitable où il deviendrait impossible pour le transfuge allemand de fournir les codes.

C'est ce qui se produisit en 1938 quand les Allemands renforcèrent la sécurité d'Enigma en ajoutant deux rotors à la disposition des cryptographes. Les opérateurs d'Enigma avaient maintenant le choix des

3 rotors positionnés dans la machine parmi 5, et le nombre de possibilités de dispositions passait de 6 à 60. Rejewski et son équipe se trouvèrent devant un autre problème, c'est qu'il ne connaissait pas le câblage des nouveaux rotors. De plus, le mois suivant, le tableau de connexion passa de 6 à 10 connexions. Au lieu de 12 lettres à apparier, il y en avait maintenant 20. Le cumul de ces deux nouveautés fit passer le nombre de clefs à 159 milliards de milliards. Enigma semblait devenue invulnérable…

Cela tombait plutôt mal, car le contexte politique s'alourdissait. L'Allemagne occupait les Sudètes quand le 27 avril 1939 elle dénonça le pacte de non-agressions avec la Pologne. La rhétorique antipolonaise se faisait de plus en plus virulente. Langer décida alors de mettre les Alliés au courant des avancées polonaises dans le déchiffrage d'Enigma, n'ayant pas les moyens financiers suffisants pour construire une *bombe* 10 fois plus importante. De plus, craignant l'envahissement de la Pologne, il pensa à juste titre faire bénéficier les Alliés du travail de Rejewski et de ses collègues.

Pendant treize ans, Britanniques et Français avaient tenu pour acquis qu'Enigma était intouchable, et voilà donc que l'espoir renaissait. Les révélations polonaises avaient fait apparaître des failles dans le chiffrement d'Enigma, ce qui remonta le moral des Alliés. Certes les avancées polonaises avaient été contrées par les nouveaux rotors, mais Enigma n'était plus tenu pour un chiffre parfait. C'est ainsi qu'en Angleterre, les dirigeants du *Bureau 40* s'activèrent pour rattraper leur retard sur Enigma, recrutèrent des mathématiciens, notamment parmi les meilleurs étudiants des universités de Cambridge et d'Oxford (*Trinity College, King's College...*) et fondèrent la *GC&CS* (*Government Code & Cipher School*) à Bletchley Park dans un grand manoir de style victorien, seul lieu ayant la capacité d'accueillir tous ces cryptographes.

Les scientifiques et mathématiciens britanniques se familiarisèrent avec le chiffre d'Enigma et avec les méthodes polonaises et découvrirent eux-mêmes des raccourcis pour trouver les clefs d'Enigma. Bletchley Park disposait de plus de ressources et de personnel que le Bureau du Chiffre polonais et put donc s'attaquer à la cryptanalyse d'Enigma. Les équipes de cryptanalystes effectuaient les 3/8 pour ne pas être débordées par le flot incessant de cryptogrammes allemands captés par des stations de contrôle sur la côte (Stations Y)[201], et envoyés sans tarder à Bletchley Park. De nouvelles recrues avaient été embauchées

[201] Ces stations, situées sur les côtes anglaises comportaient d'immenses systèmes d'antennes qui étaient capables de capter des signaux venant de Russie et même du Japon. Des équipes d'opérateur travaillaient ici à une tâche pénible consistant à traduire les signaux Morse en lettres, suites et enchaînements de messages codés incompréhensibles. Une seule erreur pouvait rendre un message indécryptable.

grâce à des mots croisés publiés dans le *Daily Telegraph* : quiconque terminait des mots croisés spécialement créés pour l'occasion, en moins de douze minutes, était invité à se présenter à Bletchley pour subir des tests d'entrée.

Langer offrit aux Britanniques et aux Français les deux répliques dont il disposait de la machine Enigma ainsi que les plans des « *bombes* » qui furent transportés jusqu'à Paris par valise diplomatique. Ce fut dans les bagages de Sacha Guitry et de son épouse Yvonne Printemps (les ports étaient surveillés par des espions allemands) que le matériel rejoignit finalement l'Angleterre.

Deux semaines plus tard, le 1er septembre, Hitler envahissait la Pologne…

Au centre de Bletchley Park s'élevait un grand manoir victorien de style gothique-Tudor, construit au XIXe siècle par le financier sir Herbert Leon. Le manoir, avec sa bibliothèque, sa grande salle à manger et sa salle de bal très ornementée, abritait l'administration centrale de toute l'opération Bletchley. Le commandant Alastair Dennitson, directeur de la *GC&CS*, avait un bureau au rez-de-chaussée donnant sur les jardins, une vue qui fut bientôt gâchée par l'érection de nombreuses Huttes. Dans ces constructions de fortune en bois furent logées les différentes activités nécessaires à l'attaque des codes. La Hutte 6 (photo ci-contre) par exemple, était spécialisée dans les communications de l'armée allemande sur Enigma. La Hutte 6 passait ses textes décryptés à la Hutte 3, où un service de renseignements traduisait les messages, rassemblait l'information et essayait de l'exploiter. La Hutte 8 se consacrait à l'Enigma navale et passait ses messages décryptés à la Hutte 4 pour la traduction et la réunion des informations. Au départ, Bletchley Park rassembla une équipe de deux cents personnes, mais au bout de cinq ans, le manoir et les huttes finirent par abriter sept mille hommes et femmes.

Pendant l'automne 1939, les scientifiques et les mathématiciens se familiarisèrent avec la complexité du chiffre Enigma, et ils maîtrisèrent rapidement les méthodes polonaises. Bletchley disposait de plus de personnel et de ressources que le Biuro Szyfrôw polonais, c'est-à-dire qu'on pouvait s'y attaquer au nombre accru de rotors et au fait qu'Enigma était maintenant dix fois plus difficile à percer. Tous les jours, les cryptanalystes anglais accomplissaient le même travail routinier. À minuit, les opérateurs allemands sur Enigma réglaient la machine sur un nouveau code du jour, ce qui ruinait tout ce que Bletchley avait réussi à effectuer la veille. Il fallait recommencer en identifiant d'abord le nouveau code. Cela pouvait prendre plusieurs heures, mais dès que les réglages du jour avaient été trouvés, l'équipe de Bletchley pouvait commencer à déchiffrer les messages allemands qui s'étaient accumulés.

Ayant maîtrisé les techniques polonaises, les cryptanalystes de Bletchley commencèrent à découvrir leurs propres raccourcis pour trouver les clefs d'Enigma. Ils repérèrent par exemple que les opérateurs allemands choisissaient parfois des messages-clefs évidents. Pour chaque message, l'opérateur était supposé utiliser un message-clef différent, dont les trois lettres étaient choisies au hasard. Mais dans la fièvre de la bataille, plutôt que de se donner le mal de chercher une clef au hasard, les opérateurs débordés optaient quelquefois pour les trois lettres se suivant sur le clavier, comme QWE (les claviers étaient en « Qwerty »). Ces messages prévisibles furent baptisés *cillies*. Un autre exemple de cillie était l'usage répété du même message-clef (ce pouvait être les initiales de la petite amie de l'opérateur, du genre des lettres C-I-L, qui sont à l'origine du terme), ou d'un explétif allemand court. Avant d'attaquer Enigma par la voie normale et difficile, les cryptanalystes essayaient systématiquement des cillies et, quelquefois, leurs pressentiments s'avéraient payants.

Les « cillies » n'étaient pas des défauts inhérents à la machine Enigma, mais des faiblesses dans l'utilisation qui en était faite. L'erreur humaine à des niveaux plus élevés compromit également la sécurité du chiffre d'Enigma. Des responsables de l'application des carnets de code devaient décider quels rotors seraient utilisés chaque jour, et dans quelles positions. Ils tentaient d'assurer l'imprévisibilité des ajustements du brouilleur en excluant qu'un rotor reste à la même place deux jours de suite. Ainsi, si nous appelons les rotors 1, 2, 3, 4 et 5, le premier jour on pouvait avoir l'agencement 134, le deuxième jour 215, mais pas 214 puisque le rotor 4 ne doit pas rester à la même place deux jours de suite. Cela peut sembler une stratégie subtile puisque les rotors changent constamment de place, mais en se conformant trop rigidement à cette règle, on facilitait la tâche du cryptanalyste.

Renoncer à certains agencements afin qu'un rotor ne reste pas à la même place réduisait de moitié le nombre des agencements possibles. Les cryptanalystes de Bletchley comprirent ce qui se passait et l'exploitèrent magnifiquement. Ayant identifié l'agencement des rotors pour un jour donné, ils pouvaient immédiatement éliminer la moitié des positions possibles pour le jour suivant. Leur charge en était réduite de moitié.

De même, une règle stipulait que des connexions (sur le tableau de connexions) ne s'effectueraient pas entre deux lettres voisines, ce qui signifie que S pouvait être connecté à n'importe quelle lettre, sauf R et T. La théorie disait que des permutations aussi évidentes devaient absolument être évitées, mais, une fois encore, l'application de cette loi réduisait de manière drastique le nombre des clefs possibles.

Cette recherche constante de raccourcis cryptanalytiques fut rendue nécessaire par l'évolution de la machine Enigma tout au long de la guerre. Les cryptanalystes étaient sans cesse contraints d'innover, de redessiner et sophistiquer les *bombes*, d'élaborer de nouvelles stratégies. Une grande part de leur succès est due à cette combinaison inhabituelle, à l'intérieur de chaque hutte, de mathématiciens, de scientifiques, de linguistes, de champions d'échecs, et de cruciverbistes fanatiques. Un problème apparemment insoluble passait de main en main, jusqu'à ce que quelqu'un disposant des bons outils intellectuels le résolve, ou qu'il parvienne à quelqu'un qui le résolvait partiellement avant de le faire circuler à nouveau. Gordon Welchman, le responsable de la Hutte 6, décrivait son équipe comme « une meute de chiens tentant de trouver une piste ».

Il y eut maints cryptanalystes remarquables, et des trouvailles d'une grande portée, et il faudrait plusieurs gros volumes pour détailler toutes les contributions individuelles. Mais si l'on ne doit évoquer qu'une seule personne, ce sera Alan Turing[202], qui cerna la plus grande faiblesse d'Enigma, et l'exploita

[202] Alan est né à Paddington, de l'officier de carrière Julius Mathison Turing et de sa femme Ethel Sarah Turing (née Stoney). À partir de l'âge d'un an, le jeune Alan est élevé par des amis de la famille Turing. Sa mère rejoint alors son père qui était en fonction dans la colonie des Indes. Ces derniers reviendront au Royaume-Uni à la retraite de Julius en 1926. Très tôt, le jeune Turing montre les signes de son génie. Il est par exemple relaté qu'il apprit seul à lire en trois semaines. De même, il montra une affinité précoce pour les chiffres et les énigmes. Ses parents l'inscrivent à l'école St. Michael's, à l'âge de six ans. La directrice reconnaît rapidement en lui un génie, comme beaucoup de ses professeurs consécutifs au Marlborough College. À

impitoyablement. Grâce à Turing, il devint possible de briser le chiffre d'Enigma même dans les circonstances les plus difficiles.

Alan Turing logea à l'Auberge de la Couronne, à Shenley Brook End. Il se rendait à vélo à Blentchley Park, à 5 kilomètres où il passait une partie de son temps dans les huttes, à travailler comme les autres au percement des codes, et le reste du temps dans le *think-tank*, le réservoir de matière grise, de Bletchley, qui avait été précédemment la resserre de pommes, de poires et de prunes de sir Herbert Leon. C'est là que les cryptanalystes réfléchissaient aux moyens de résoudre de nouveaux problèmes, ou anticipaient sur ceux qui pouvaient surgir dans un futur proche. Turing se concentrait sur le problème posé par une éventuelle modification par les Allemands dans le système de messages-clefs.

Les premiers succès de Bletchley devaient tout aux travaux de Rejewski, qui exploitaient le fait que les opérateurs d'Enigma cryptaient chaque message-clef deux fois de suite ; si le message était YGB, les opérateurs chiffraient donc YGBYGB. Cette répétition était destinée à éviter une erreur pour le destinataire, mais elle constituait un point faible dans la sécurité d'Enigma. Les cryptanalystes anglais comprirent qu'il ne faudrait pas longtemps aux Allemands pour s'en apercevoir, et qu'à ce moment-là les opérateurs

---

Marlborough, il est pour la première fois confronté à des camarades plus âgés que lui, il deviendra l'une de leurs têtes de Turc. À partir de 13 ans, il fréquente l'école de Sherborne, où son premier jour de classe fut couvert par la presse locale en raison de son exploit sportif. En effet, une grève générale avait éclaté au Royaume-Uni et Turing s'était rendu à son école, distante de près de 90 kilomètres, à vélo, s'arrêtant la nuit dans un motel. Sportif accompli, Alan Turing arrivera même 4e à l'arrivée du Marathon de l'Association des Athlètes Amateur (AAA), marathon, dont les meilleurs coureurs sont traditionnellement qualifiés pour les Jeux Olympiques, en 1949, en 2 heures 46 minutes et 3 secondes, un très bon temps à l'époque. Une jambe blessée, Turing cessera de courir sérieusement en 1950. Le penchant naturel de Turing pour les sciences ne lui apporte le respect, ni de ses professeurs, ni des membres de l'administration de Sherborne, dont la définition de la formation mettait plus en valeur les disciplines classiques (littérature, arts, culture physique) que les sciences. Malgré cela, Turing continue de faire des prouesses dignes d'intérêt dans les matières qu'il aime, résolvant des problèmes très ardus pour son âge. Par exemple, en 1928, Turing découvre les travaux d'Albert Einstein, et les comprend alors qu'il a à peine 16 ans, allant même jusqu'à extrapoler la loi du mouvement d'Einstein à partir d'un texte dans lequel elle n'était pas décrite explicitement.

Après les recherches menées à Bletchley Park visant à casser les codes secrets de la machine Enigma utilisée par les Nazis, il rejoint en novembre 1942 les États-unis pour tenter de casser les codes japonais. Il y rencontre Claude Shannon avec qui il s'entretient régulièrement. Il retourne en Angleterre en 1943. Il conçoit également une machine à coder la voix. Il contribue également à de nombreuses autres recherches mathématiques, comme celles qui aboutiront à casser le code généré par le téléscripteur de Fish (machine construite par Lorenz et Siemens en partenariat). Les recherches sur le code de Fish furent utilisées lors de la conception de l'ordinateur Colossus. Cette machine fut conçue par Max Newman et fut construite au laboratoire de recherche des Postes de Dollis Hill par une équipe dirigée par Thomas Flowers en 1943. Turing a également conçu des versions améliorées de la « Bombe » polonaise utilisée pour trouver des clés des messages de la machine Enigma. Ce sont des dispositifs électromécaniques associant plusieurs « machines Enigma » pour éliminer rapidement des ensembles de clés potentielles sur des blocs de communication d'Enigma. Le travail de Turing sur le déchiffrement du code Enigma lors de l'opération Ultra fut tenu secret jusque dans les années 1970 ; même ses plus proches amis n'étaient pas au courant de ces recherches.

L'homosexualité de Turing lui valut d'être persécuté et brisa sa carrière. En 1952, son compagnon aide un complice à cambrioler la maison de Turing, qui porte plainte auprès de la police. L'enquête de police finit par l'accuser d'« indécence manifeste et de perversion sexuelle » (d'après la loi britannique sur la sodomie). Il décide d'assumer son orientation et ne présente pas de défense, ce qui le fait inculper. S'ensuit un procès très médiatisé, où lui est donné le choix entre l'incarcération et un traitement hormonal de réduction de la libido. Il choisit ce dernier, d'une durée d'un an, avec des effets secondaires comme le grossissement de ses seins. Alors qu'il avait été consacré en 1951, en devenant membre de la Royal Society, à partir de 1952 il sera écarté des plus grands projets scientifiques.

En 1954, il meurt d'empoisonnement en mangeant une pomme contenant du cyanure. Beaucoup de gens pensent que cette mort est intentionnelle, et elle fut présentée comme telle (probablement en souvenir de Blanche-Neige). Sa mère, toutefois écarta la thèse du suicide pour soutenir celle de l'accident. Elle affirmait vigoureusement que l'ingestion du poison était accidentelle en raison de la propension de son fils à entreposer des produits chimiques de laboratoire sans aucune précaution.

Certains voient dans le choix du nom et du logo de la société Apple Computer (une pomme croquée aux couleurs du « rainbow flag », le drapeau de la communauté homo-bi-trans) une référence, si ce n'est un hommage à Alan Turing…

d'Enigma seraient amenés à supprimer cette répétition, réduisant à néant les méthodes en cours à Bletchley pour le décryptage. La mission de Turing était de trouver une autre voie pour attaquer Enigma, une voie qui ne serait pas fondée sur la répétition du message-clef.

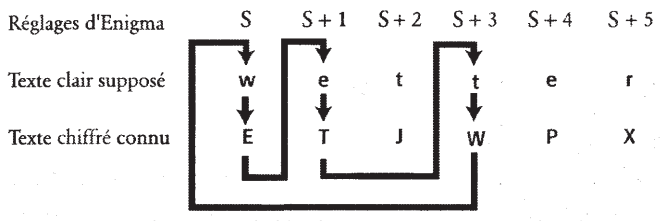
Les semaines passant, une grande bibliothèque se remplissait à Bletchley des messages décryptés accumulés et Turing remarqua qu'un grand nombre d'entre eux se conformaient à une structure stricte. En étudiant de vieux messages décryptés, il pensa que l'on pourrait parfois prédire une partie du contenu d'un message, d'après la date de son envoi et sa source. L'expérience montrait, par exemple, que les Allemands envoyaient un bulletin météo, chiffré par Enigma, chaque jour peu après 6 heures du matin. Ainsi, un message intercepté à 6 h 5 comportait presque sûrement le mot *Wetter*, le mot allemand pour *temps*. Le protocole rigoureux appliqué par toutes les organisations militaires entraînait que le style de ces messages soit parfaitement réglementé, aussi Turing avait une idée de la place du mot Wetter dans le message crypté. Des essais pourraient lui prouver si les six premières lettres d'un texte crypté donné correspondaient aux lettres du texte clair Wetter. On appelle cette méthode, la méthode des *mots probables*. Pour les Anglais, c'était des *cribs*.

Turing avait l'intuition qu'armé de ces cribs, il pourrait vaincre Enigma. Devant un texte crypté, s'il connaissait le groupement de lettres représentant Wetter, disons ETJWPX, il s'agissait d'identifier quels réglages de la machine Enigma transformeraient Wetter en ETJWPX

Le chemin le plus direct serait de prendre une machine Enigma, de taper Wetter et de voir si le texte chiffré exact en sortait. Dans le cas contraire, le cryptanalyste devrait modifier les agencements de la machine, en changeant les connexions de fils, en permutant les brouilleurs, ou en les réorientant, et taper Wetter à nouveau. Si l'on n'obtient toujours pas le texte chiffré exact, on change une nouvelle fois tous ces agencements, et on recommence encore et encore. Le seul problème avec cette approche est que, parmi les 159 milliards de milliards d'ajustements possibles à tester, il est hautement improbable de trouver celui qui transformera Wetter en ETJWPX !

Afin de simplifier le problème, Turing essaya d'appliquer la même stratégie que Rejewski. Il voulait séparer la question des réglages de rotors (quel rotor est à quelle place, et quelles sont leurs orientations respectives) de la question des connexions du tableau. S'il pouvait trouver quelque chose dans le crib qui n'ait rien à voir avec les connexions, il pourrait essayer les 1 054 560 combinaisons possibles des rotors (60 dispositions x 17576 orientations). Ayant établi les positions exactes des rotors, il pourrait ensuite déduire les connexions du tableau.

Il se fixa sur un type particulier de cribs, ceux à l'intérieur desquels on notait des boucles semblables aux chaînes de Rejewski. Les chaînes de Rejewski liaient les lettres dans les messages-clefs. Les boucles de Turing n'avaient rien à voir avec les messages-clefs, puisqu'il travaillait sur l'hypothèse que les Allemands cesseraient bientôt d'en envoyer. À la place, les boucles de Turing connectaient les lettres du texte clair et du texte chiffré dans un mot probable. L'exemple montré sur l'illustration contient une boucle.



Un des mots probables de Turing, montrant une boucle.

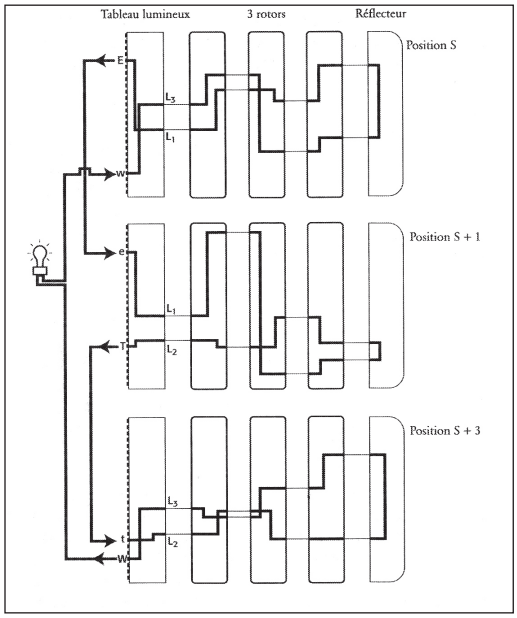
On s'en souvient : les mots probables ne sont que devinés, mais si nous estimons que ce crib est correct, alors nous pouvons lier les lettres w — E, e —T, t —W dans une partie de la boucle. Bien qu'ignorant les réglages initiaux d'Enigma, nous pouvons désigner cette disposition, quelle qu'elle soit, par S. Dans cette première disposition, nous savons que w est crypté E. Après ce cryptage, le premier rotor

tourne d'une place et arrive en position (S+l) et la lettre *e* est cryptée T. Le rotor tourne d'une autre place et crypte une lettre qui ne fait pas partie de la boucle, et nous l'oublions. Le rotor se remet en marche et avance d'une place où nous atteignons de nouveau une lettre qui fait partie de la boucle. Dans cette disposition (S+3), nous savons que la lettre *t* est cryptée W. En résumé, nous savons que :

En position S, Enigma crypte *w* en E
En position S+1, Enigma crypte *e* en T
En position S+3, Enigma crypte *t* en W

Cette boucle semble n'être rien de plus qu'un dessin curieux, mais Turing en examina rigoureusement les implications, et il découvrit qu'elle lui procurait le raccourci qu'il cherchait. Au lieu de travailler sur une seule machine et d'en essayer toutes les dispositions, Turing commença par imaginer trois machines séparées, chacune travaillant sur le chiffrement d'un élément de la boucle. La première machine essaierait de chiffrer *w* en E, la seconde machine essaierait de chiffrer *e* en T et la troisième machine essaierait de chiffrer *t* en W.

Les trois machines auraient des réglages identiques, sauf que la deuxième aurait l'orientation de son brouilleur avancée d'une place par rapport à la première (S+1), et que la troisième serait réglée initialement en (S+3). Pour appliquer ces critères, Turing se représentait un cryptanalyste frénétique, changeant sans arrêt les connexions, essayant toutes les positions des rotors, modifiant les orientations. Tout câblage modifié dans la première machine devait l'être aussi dans les deux autres. Et surtout, quelles que fussent les orientations fixées dans la première machine, elles devaient être décalées d'une place dans la deuxième et de trois places dans la troisième.



Analogie électrique de la boucle du crib (ou mot probable). Trois machines Enigma sont réglées de manière identique, mais la deuxième a son premier rotor avancé d'un cran (disposition S+1) et la troisième a son rotor avancé de deux crans supplémentaires (S+3). Les fils sortant de chaque Enigma sont connectés à ceux entrant dans la suivante. Les trois jeux de rotors cliquettent à l'unisson jusqu'à ce que le circuit soit bouclé et qu'une lampe s'allume. À ce moment-là, la disposition exacte est trouvée. Dans le diagramme ci-dessus, le circuit est bouclé.

On ne voit pas encore très bien l'avantage de cette démarche. Le cryptanalyste doit toujours essayer les 159 milliards de milliards de dispositions possibles et, pour tout arranger, il doit le faire maintenant sur les trois machines simultanément. Mais Turing fit un nouveau pas qui simplifia considérablement les opérations. Il imagina de relier les trois machines par des fils électriques de façon que le circuit électrique reproduise en dur la boucle virtuelle du crib. Les connexions et les rotors changeraient sur la machine, comme décrit ci-dessus, mais le circuit ne serait achevé que lorsque tous les réglages seraient justes pour les trois machines, permettant au courant de passer à travers les trois. Si Turing introduisait dans le circuit une ampoule électrique, elle ne s'allumerait que lorsque les réglages exacts auraient été trouvés. À ce stade, les trois machines avaient toujours à essayer le même nombre colossal d'options pour allumer l'ampoule. Mais tout ceci n'avait été que la préparation du bond logique final de Turing, qui devait rendre la tâche cent millions de millions de fois plus facile d'un seul coup.

Turing avait construit son circuit électrique de manière à annuler l'effet du tableau de connexions, s'autorisant ainsi à ignorer les milliards de branchements du tableau. Si nous regardons la figure ci-contre, sur la première Enigma le courant électrique pénètre dans les rotors et sort à une lettre inconnue, disons L_1. Le courant ensuite passe par le tableau

de connexions et transforme L_1 en *E*. Cette lettre *E* est reliée par un câble à la lettre *E* de la deuxième Enigma, et lorsque le courant passe à travers le deuxième tableau de connexions, elle est transformée à nouveau en L_1. Autrement dit, les deux tableaux s'annulent l'un l'autre. De même, le courant sortant des rotors de la deuxième Enigma pénètre dans le tableau à L_2 avant d'être transformé en *T*. Cette lettre *T* est connectée par un câble à la lettre *T* de la troisième Enigma, et lorsque le courant passe par le troisième tableau de connexions, elle redevient L_2. En clair, les tableaux de connexions s'annulent entre eux au long du circuit, et Turing pouvait donc se dispenser d'en tenir compte

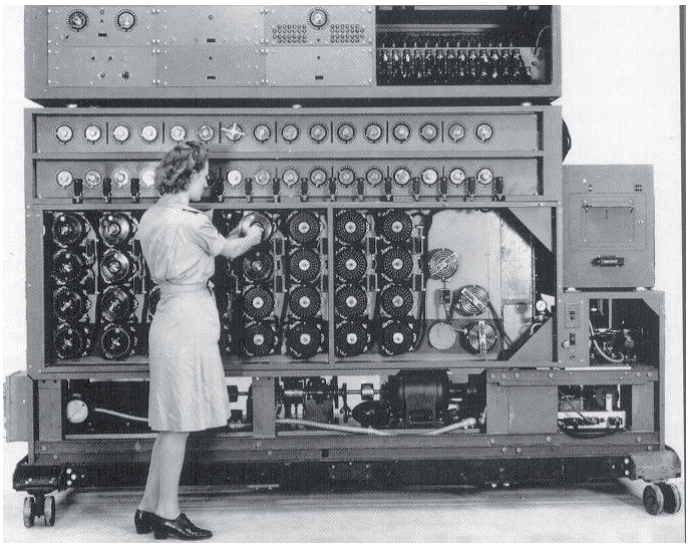
Turing devait simplement lier la lettre issue du premier groupe de rotors, L_1, à la lettre entrant dans le deuxième groupe L_1, et ainsi de suite. Il ne connaissait malheureusement pas l'identité de L_1 et il devait connecter les 26 sorties du premier groupe de rotors aux 26 entrées dans le deuxième, et ainsi de suite. Il y avait maintenant 26 boucles électriques, et chacune était équipée d'une ampoule électrique pour signaler lorsqu'un circuit électrique était bouclé. Les trois groupes de rotors pouvaient alors essayer chacune des 17 576 orientations, avec le deuxième groupe toujours un cran en avance sur le premier, et le troisième deux crans en avance sur le deuxième. Si les rotors changeaient d'orientation toutes les secondes, il ne faudrait que cinq heures pour essayer toutes les orientations.

Il restait deux problèmes. D'abord, il se pouvait que les machines fonctionnent sur un mauvais ajustement du brouilleur, puisque l'Enigma opérait avec trois des cinq rotors disponibles, placés dans n'importe quel ordre, selon soixante dispositions possibles. Ainsi lors que les 17 576 orientations avaient été essayées, si l'ampoule ne s'était pas allumée, il fallait essayer l'une des soixante autres dispositions des rotors et continuer jusqu'à ce que le circuit soit bouclé. Ou alors, le cryptanalyste aurait dû avoir soixante séries de trois Enigma fonctionnant en parallèle.

Le deuxième problème était de trouver les branchements du tableau de connexions, une fois établies la disposition des rotors et leurs orientations. Cela était relativement simple. En se servant d'une Enigma réglée conformément aux positions et aux orientations correctes des rotors, le cryptanalyste tape un texte chiffré et regarde le texte clair qui en sort. Si le résultat est *tewwer*, au lieu de *wetter*, il est clair qu'une connexion permute le *w* et le *t*. Taper d'autres extraits de textes chiffrés révélera d'autres connexions.

La combinaison des mots probables, des boucles et des machines reliées électriquement fournissait un outil remarquable à la cryptanalyse, et seul Turing, avec son expérience unique sur les machines mathématiques, pouvait en être l'auteur. Ses rêveries sur les imaginaires machines de Turing tendaient à répondre à des questions ésotériques sur l'indécidabilité mathématique, mais cette recherche purement académique l'avait préparé à concevoir une machine utilisable, capable de résoudre des problèmes bien réels.

Bletchley réussit à obtenir 100 000 livres pour concrétiser l'idée de Turing sous forme de machines que l'on appela des *bombes*, en référence à la bombe de Rejewski. Chacune des bombes de Turing devait être constituée de douze groupes de rotors reliés électriquement, ce qui leur permettrait de s'attaquer à de plus longues boucles de lettres. L'élément complet mesurait presque deux mètres de haut, deux mètres de long, et un mètre de large. Turing finalisa son projet au début de 1940 et la construction en fut confiée à l'usine British Tabulating Machinery, à Letchworth.



En attendant la livraison des bombes, Turing continua son travail à Bletchley. Son in-

vention fut bientôt connue des autres cryptanalystes du lieu qui saluèrent en lui un décrypteur d'exception. Selon Peter Hilton, un de ses collègues de Bletchley : « *Alan Turing était évidemment un génie, mais un génie amical que l'on pouvait approcher Il était toujours prêt à perdre du temps et à se donner du mal pour expliquer ses idées; mais ce n'était pas un spécialiste étroit, et ses réflexions embrassaient un vaste domaine des sciences* ».

Bien entendu, tout était tenu secret au GC&CS, et personne en dehors de Bletchley n'était au courant de la réalisation de Turing. Ses parents eux-mêmes ignoraient totalement qu'il travaillait sur les codes, à plus forte raison qu'il était le premier cryptanalyste anglais. Il avait dit un jour à sa mère qu'il était impliqué dans la recherche militaire, mais sans autre précision. Elle fut surtout déçue de voir qu'on n'avait pas imposé à son fils une coupe de cheveux plus convenable. Bien que Bletchley fut dirigé par des militaires, ils avaient compris qu'il leur fallait tolérer le laisser-aller et les excentricités de ces intellectuels. Turing prenait rarement la peine de se raser, ses ongles étaient noirs et ses vêtements froissés. Si les militaires fermèrent aussi les yeux sur son homosexualité, nous l'ignorons. Jack Good, un vétéran de Bletchley, déclara : « *Heureusement que les autorités de Bletchley ne savaient pas que Turing était homosexuel, autrement nous aurions perdu la guerre.* »

Le premier prototype de bombe, baptisé *Victory*, arriva à Bletchley le 14 mars 1940. La machine fut mise immédiatement en service, mais ses débuts ne furent guère satisfaisants. Elle se révéla beaucoup plus lente qu'on ne l'attendait, mettant parfois une semaine à trouver une clef. Il fallut un effort concerté pour accroître l'efficacité de la bombe, et un plan modifié fut prêt quelques semaines plus tard. Cela prit encore quatre mois pour construire cette bombe améliorée.

À la même époque, les cryptanalystes durent faire face à la catastrophe qu'ils avaient prévue. Le 10 mai 1940, les Allemands changèrent de protocole pour l'envoi des clefs. Ils ne répétaient plus le message-clef, et par conséquent le nombre de déchiffrements d'Enigma chuta dramatiquement. Cette panne de l'information dura jusqu'au 8 août, date de l'arrivée de la nouvelle bombe. Baptisée *Agnus Dei*, ou de son diminutif *Agnès*, cette machine allait enfin répondre aux espérances de Turing.

Pendant les huit mois suivants, quinze nouvelles bombes furent mises en service, faisant chacune le bruit d'un million d'aiguilles à tricoter. Quand tout allait bien, une bombe pouvait trouver une clef d'Enigma en une heure. Lorsque les connexions du tableau et les positions des rotors (le message-clef) avaient été établies pour un message donné, il était facile d'en déduire la clef du jour. Tous les autres messages envoyés le même jour pouvaient alors être déchiffrés.

Pour autant, le déchiffrement n'était pas devenu une simple formalité. Il y avait bien des obstacles à surmonter avant que les bombes ne commencent à chercher la clef. Il fallait, par exemple, un mot probable. Les décrypteurs devaient fournir des mots probables aux opérateurs, mais il n'était pas garanti qu'ils avaient deviné le sens exact du texte chiffré. Même s'ils avaient le mot juste, il pouvait être à la mauvaise place ; les cryptanalystes pouvaient avoir deviné qu'un message crypté contenait une certaine phrase, mais avoir associé cette phrase à une fausse partie du texte. Il y avait un truc pour voir si un mot probable était à sa place. Dans l'exemple suivant, le cryptanalyste sait que le texte clair est juste, mais il ne sait pas s'il correspond bien aux lettres du texte chiffré.

Texte clair probable	w e t t e r n u 1 1 s e ch s
Texte chiffré connu	IPRENLWKMJJSXCPLEJWQ

Nous avons mentionné plus haut qu'un des traits d'Enigma était de ne jamais chiffrer une lettre par elle-même, ce qui était une conséquence du réflecteur. La lettre *a* ne serait jamais chiffrée *A*, la lettre *b* jamais chiffrée *B* et ainsi de suite. Par conséquent, les lettres ci-dessus sont mal alignées, puisque le premier *e* de *wetter* correspond à un *E* du texte chiffré. Pour trouver le bon alignement, nous allons faire glisser le texte clair et le texte chiffré l'un par rapport à l'autre, afin qu'aucune lettre ne soit appariée avec elle-

même. Si nous déplaçons le texte clair d'une lettre vers la gauche, cela ne convient toujours pas, puisque cette fois le premier *s* de *sechs* répond au *S* du texte chiffré. Si, par contre, nous décalons le texte clair d'une place vers la droite, nous ne voyons plus de chiffrements interdits le texte probable a bien des chances de se trouver à la bonne place et pourra être utilisé comme base de déchiffrement par la bombe.

Texte clair probable	w e t t e r n u l 1 s e c h s
Texte chiffré connu	IPRENLWKMJJSXCPLEJWQ

Les renseignements réunis à Bletchley n'étaient communiqués qu'aux principaux chefs militaires et à quelques membres du Cabinet de guerre. Winston Churchill était très conscient de l'importance des déchiffrements de Bletchley, et le 6 septembre 1941, il rendit visite aux décrypteurs. Rencontrant quelques-uns des cryptanalystes, il fut surpris par la bizarre composition de la troupe qui lui procurait des informations si précieuses ; outre les mathématiciens et les linguistes, il y avait là un expert en porcelaine, un conservateur du musée de Prague, le champion anglais d'échecs et de nombreux bridgeurs. Churchill murmura à sir Stewart Menzies, qui était à la tête de l'Intelligence Service : « *Je vous avais dit de ne pas omettre de retourner une seule pierre, mais je ne m'attendais pas à ce que vous me preniez au pied de la lettre* ». Malgré ce commentaire, cette équipe hétéroclite lui plut, et il qualifia ses membres d'« *oies qui déposent des œufs d'or et qui ne cacardent jamais* ».

Cette visite avait pour but de remonter le moral des décrypteurs en leur montrant que leur travail était apprécié en très haut lieu. Elle mit aussi Turing et ses collègues en position d'en appeler directement à Churchill quand une crise menaça. Pour exploiter au mieux les bombes, Turing avait besoin de personnel supplémentaire, mais ses demandes avaient été bloquées par le commandant Edward Travis, qui avait pris la direction de Bletchley, et qui ne trouvait pas justifié de recruter du monde. Le 21 octobre 1941, les cryptanalystes décidèrent d'ignorer la hiérarchie, et ils écrivirent directement à Churchill.

Churchill n'hésita pas sur la réponse à envoyer. Il adressa immédiatement une note à son officier d'état-major :

À FAIRE AUJOURD'HUI

Assurez-vous qu'ils aient ce qu'ils veulent de toute urgence et tenez-moi informé.

À partir de là, il n'y eut plus de restrictions au recrutement ni à l'achat de matériel. À la fin de 1942, il y avait quarante-neuf bombes, et un nouveau site regroupant des bombes fut créé à Gayhurst Manor au nord de Bletchley.

Cependant, la tâche était lourde, car chaque armée allemande avait son propre réseau de communications et utilisait des machines Enigma spécifiques. Par exemple, les codes utilisés en Afrique du Nord étaient différents de ceux utilisés en Europe. La vraie difficulté se fit jour quand la Kriegsmarine se mit à opérer, en 1942, avec une nouvelle Enigma disposant de 4 rotors à choisir entre 8, et qu'en plus, le réflecteur, fixe dans les machines des autres armées, devint mobile ce qui augmenta encore d'un facteur 26 le nombre de combinaisons possibles.

De plus, les opérateurs de la marine allemande prenaient bien soin de ne pas utiliser de messages stéréotypés ce qui rendait quasi impossible la recherche par mot probable. Pendant toute l'année 1942, la hutte 8 ne déchiffra en moyenne que 3 clés par jour, chacune nécessitant plusieurs semaines de travail !

Le décryptement de l'Enigma navale

Jusqu'au début de l'année 1942, l'Enigma M3 était en service et les cryptanalystes de Bletchley Park étaient en mesure de déchiffrer les cryptogrammes allemands dans un délai convenable. Une chambre spéciale appelée *Submarine Tracking Room* (ci-dessous, la salle des cartes) avait été créée et centralisait toutes les données concernant la localisation et les mouvements des U-Boot. Ce bureau possédait une immense carte de l'Atlantique sur laquelle étaient positionnés des sous-marins et bateaux miniatures indiquant la position des convois anglo-saxons. Grâce à cette immense carte qui s'appuyait non seulement sur ***Ultra***[203] mais aussi sur la reconnaissance aérienne, sur des échos sonars et sur la radiogoniométrie, l'état-major pouvait ordonner à des convois de changer de cap pour contourner une meute de sous-marins.

Ainsi jusqu'en 1942, les informations fournies sur l'emplacement des U-Boot permirent de limiter le nombre de navires torpillés. Pourtant, dès le début de l'année 1942, l'Allemagne entre véritablement dans une industrie de guerre, construit plus de U-Boot, et l'amiral Karl Doenitz, inquiété du peu d'efficacité de ses sous-marins, renforce la sécurité des communications entre eux en complexifiant la machine à crypter.

L'Enigma M3 disparaît donc au profit de l'Enigma M4 dans les sous-marins allemands.

La Submarine Tracking Room affirma en 1942 être incapable de connaître la position des sous-marins allemands, pour la première fois depuis le début de la guerre. Alors qu'en 1941, pendant que *Ultra* était utilisée pour détourner les convois alliés des meutes de U-Boot, seul un convoi sur dix était repéré, ce nombre passa à un sur trois en 1942 pendant le black-out. Par conséquent, le tonnage coulé dans l'Atlantique Nord, qui atteignait 600 000 tonnes durant les six derniers mois de 1941, a été multiplié par plus de quatre dans la deuxième moitié de l'année 1942, atteignant le record de 2 600 000 tonnes ! Et chacun des cinq cents bateaux coulés durant ces six mois entraînait moins de nourriture pour la population, mois de munitions pour les soldats, mois de carburant pour les avions et la perspective de prolonger encore toutes ces misères...

La crainte que l'impuissance des services de renseignements, associée au nombre croissant de sous-marins, ne provoque la perte de plus de navires que l'Amérique ne puisse en produire atteint son paroxysme fin 1942. C'est pourquoi l'OIC (*Operational Intelligence Center*) fit pression sur Bletchley Park pour qu'elle trouve à tout prix le moyen de mettre un terme à ce black-out.

Enigma M4 utilisée dans les U-Boot

[203] Nom de code de la source d'information dûe au décodage d'Enigma.

Dans l'impossibilité de trouver les clefs du jour, Bletchley Park eut alors l'idée de les subtiliser par la force. C'est ainsi que des opérations visant à capturer l'Enigma navale et ses livres de code furent mises sur pied.

Ces attaques devaient être très rapides pour surprendre l'équipage des sous-marins afin qu'ils n'aient pas le temps de détruire les documents secrets et de jeter la machine par-dessus bord. De plus, elles ne devaient absolument pas suggérer aux Allemands que leur code avait été compromis...

U-995, Type VII C, au mémorial naval de Laboe. Seul exenplaire de cette classe de U-Boot restant.

La plus célèbre de ces captures a été celle du U-559[204] forcé de faire surface en octobre 1942 au large de la Méditerranée. C'était la treizième mission de ce bâtiment sous le commandement de Hans Heidtmann. Il avait quitté Messine la veille.

Le courage et l'obstination de Fasson et Grazier, deux marins de la Royal Navy, leur permirent de ramener intacte une Enigma M4, ses carnets de code, et le code météo utilisé par les U-Boot.

Ils n'assistèrent toutefois pas aux formidables conséquences de leur acte puisqu'ils périrent noyés avec le U-559 sans qu'ils n'aient eu le temps d'en sortir. Tous ces documents saisis permirent aux cryptographes de Bletchley Park de briser le chiffre de l'Enigma navale, et en 1943 les pertes des navires alliés baissèrent à nouveau.

À partir de 1943, on assiste à un spectaculaire renversement de situation dans la bataille de l'Atlantique. Non seulement les communications adverses sont à nouveau transparentes, mais les convois bénéficient des dernières technologies de guerre : le radar centésimal en plus de l'habituel *ASDIC*[205], des grenades anti-sous-marines plus puissantes et une protection aérienne plus efficace grâce aux bombardiers *B-24 Liberator* à long rayon d'action. Les U-Boot ne sont plus les chasseurs mais sont devenus des proies. Sur 1170 U-Boot en action pendant la Seconde Guerre mondiale, 780 furent détruits, tuant dans des conditions effroyables 2700 marins. L'échec pour Doenitz est total : ils n'ont pu empêcher les liaisons entre les États-Unis et la Grande-Bretagne.

Les historiens s'accordent pour dire qu'*Ultra* a été un facteur déterminant dans la victoire anglaise de la bataille de l'Atlantique. Sans cette source d'informations, les Allemands auraient conservé une plus grande flotte de sous-marins et davantage de capacité d'intervention. Cela aurait compromis le lien vital avec l'Amérique et les Alliés auraient dû consacrer des moyens humains et financiers considérables à la construction de nouveaux bateaux. Les historiens estiment que les plans alliés auraient été retardés de plusieurs mois et le débarquement repoussé au moins à l'année suivante.

---

[204] Ce bâtiment était de la classe VII C (comme celui de la photo). Avec 654 exemplaires produits entre 1940 et 1945, le type VII classe C était le fer de lance de la Kriegsmarine. Les sous-marins de ce type ont été fabriqués tout au long de la Seconde Guerre mondiale. Le premier U-boot de type VII-C était le U-69, lancé en 1940. Les principales caractéristiques de ce type étaient les suivantes : 871 t en plongée, 67,10 m de long, 6,20 m de large, 9,60 m de haut, 2 moteurs diesel pour un puissance de 3200 ch, 17,7 nœuds en surface, 7,6 nœuds en plongée, profondeur maxi : 230 m, de 44 à 52 hommes d'équipage. Sur les 654 exemplaires produits il en a été perdu 492.

[205] ASDIC (acronyme de *A*nti-*S*ubmarine *D*etection *I*nvestigation *C*ommittee) est l'ancêtre du sonar.

Bien que les avantages de la cryptanalyse d'Enigma se soient énormément fait sentir, et cela, tout au long de la guerre, dans la bataille de l'Atlantique, le décryptage des messages allemands encodés avec Enigma a également permis des prouesses plus ponctuelles lors de certains évènements de la guerre.

La bataille d'Angleterre

Le 8 août 1940, Hitler lance la Luftwaffe contre la Royal Air Force. Le nombre inférieur de chasseurs anglais face aux appareils allemands est alors compensé par les messages quotidiennement interceptés et déchiffrés à Bletchley Park. À cette époque, il existe une ligne directe entre Bletchley et le centre de commandement de l'aviation à Stanmore dont le trafic journalier est de près de deux cents messages, indiquant à quelques heures près la connaissance détaillée des plans et cibles d'attaques allemandes.

Cela permit aux Anglais, en combinant ces informations avec celles obtenues par leurs radars, de faire un usage plus efficace de leurs escadrilles d'aviation, leur évitant du même temps d'être submergés par l'aviation allemande.

Ainsi, le 15 septembre 1940, Hermann Goering ordonna une attaque massive avec 328 bombardiers et 769 chasseurs qui devait constituer le coup final de la bataille d'Angleterre. Prévenu par Bletchley Park, le commandement suprême de l'armée de l'air mit sur pied un comité d'accueil réunissant tous les appareils encore en état de combattre, et put déjouer l'offensive allemande. Deux jours plus tard, Bletchley décrypta l'ordre d'abandonner l'opération *Seelöwe*[206] et de mettre fin à la bataille d'Angleterre.

L'Afrique du Nord

L'implication de Bletchley Park dans la guerre en Afrique du Nord débuta dès 1941 lorsque le général Rommel ayant envahi la Libye et commençant son offensive vers l'Égypte utilisait la machine Enigma pour crypter les communications de ses unités.

En septembre 1941, Bletchley Park fit une avancée majeure en parvenant à décrypter la version d'Enigma utilisée par l'Afrikakorps de Rommel. Ce fut un atout de grande importance sur le théâtre des opérations, car la bataille était incertaine et le front avança et recula jusqu'à six fois pendant la campagne. Pour être plus efficace, Bletchley Park détacha même un de ses centres au Caire. Le décryptement des communications allemandes fournit aux Britanniques des informations sur les navires de l'Axe ravitaillant l'Afrikakorps en munitions et en carburant. Cela permit en partie aux Alliés de couler quarante-sept navires de ravitaillement, donc de paralyser temporairement l'Afrikakorps.

La nomination du général Montgomery à la tête de la 8ème Armée britannique qui accumulait plus de trois fois plus de matériel que l'ennemi précipita encore la retraite de l'armée allemande jusqu'en Tunisie. Rommel s'était alors plaint auprès d'Hitler que son armée était épuisée, et les tentatives de ravitaillement trop sporadiques et totalement inadéquates.

Les armes de la terreur : V1[207] ***et V2***[208]

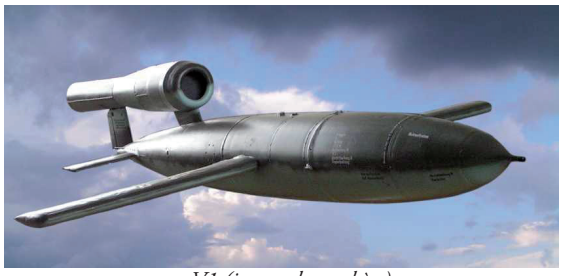
En Allemagne, à Peenemünde, des scientifiques allemands faisaient des recherches secrètes sur des combustibles liquides qui permettraient d'envoyer des bombes volantes sur des cibles déterminées à l'avance. Malgré les quelques témoignages reçus par le gouvernement anglais sur l'activité de la base de

[206] L'Opération Seelöwe (otarie ou lion de mer en français) était un plan d'invasion allemand du Royaume-Uni au début de la Seconde Guerre mondiale.

[207] Le V1 (de l'allemand Vergeltungswaffe ou arme de représailles) était une bombe volante et le premier missile de croisière de l'histoire de l'aéronautique. Elle a été utilisée du 13 juin 1944 au 29 mars 1945 par l'Allemagne nazie contre le Royaume-Uni durant la Seconde Guerre mondiale. Deux jours après le dernier V1, les V2 étaient lancés à leur tour.

[208] Le premier vol réussi d'un V2 eut lieu en octobre 1942 ; la fusée atteignit une altitude de 85 km et une vitesse de Mach 5. Le premier essai avait eu lieu peu avant la guerre sur un modèle réduit, baptisé A5, qui avait atteint 13 000 mètres d'altitude avant que son moteur explose.

Peenemünde, les autorités britanniques se refusaient à croire que de telles performances étaient possibles dans un futur proche et ne considéra pas la menace au sérieux.



V1 (image de synthèse)

Encore une fois, l'aide du décryptage d'Enigma fut précieuse puisqu'elle permit de mettre en lumière les projets des Allemands et de connaître leur avancement, ce qui, cette fois-ci, alerta les autorités anglaises. Ces dernières envoyèrent des avions de reconnaissance patrouiller sur la côte Baltique, qui confirmèrent l'existence de cette base secrète. En raison de la menace sérieuse que ces armes représentaient pour la Grande-Bretagne, des raids aériens massifs furent organisés sur Peenemünde en août 1943, ce qui retarda les expérimentations et productions des V1 et V2 d'au moins un mois, et obligea les Allemands à déplacer leurs usines de production.

V2 au musée de Peenemünde

De plus, en avril 1943, Hitler se préparait à construire des rampes de lancement sur les côtes françaises. *Ultra* intercepta les ordres d'Hitler visant à établir un quartier général près d'Amiens pour contrôler les opérations de lancement des fusées V1, ce qui confirma aux Alliés qu'il leur fallait lancer au plus vite les opérations de débarquement avant que les rampes de lancement ne soient prêtes.

Opération Overlord : le débarquement en Normandie

L'aide apportée par *Ultra* pour les opérations du débarquement s'est notamment fait ressentir dans la campagne d'intoxication menée par les Alliés visant à persuader les Allemands que le débarquement aurait lieu dans le Pas-de-Calais, connue sous le nom d'*Operation Fortitude*. En effet, connaissant les craintes des Allemands d'un débarquement dans le Pas de Calais grâce à *Ultra*, les Alliés ont tout fait pour entretenir cette crainte et tromper les Allemands quant au véritable lieu du débarquement : la Normandie.

Par exemple, un QG imaginaire entouré de chars gonflables et d'engins factices est mis sur pied dans le Kent, en face du Pas de Calais, pour duper la reconnaissance aérienne allemande.

De plus, un concours de circonstances a permis aux Alliés grâce à *Ultra* d'en savoir plus long sur la disposition des armées allemandes dans le nord-ouest de la France. En effet, un désaccord entre Hitler et ses généraux a fourni des détails de première importance sur l'organisation de la défense allemande le long des plages normandes. Rommel est convaincu que la seule façon de battre les Alliés sera de les arrêter sur le rivage avant qu'ils ne puissent consolider leur tête de pont. Aussi demande-t-il que les divisions de Panzer tiennent position le plus près possible des côtes. Son supérieur hiérarchique, le vieux maréchal Von Rundstedt est pour sa part d'un avis diamétralement opposé. Il estime qu'un groupe de divisions blindées doit se tenir largement en retrait du front afin d'être engagé dans une contre-offensive décisive qui rejettera les assaillants à la mer. Quoi qu'il en soit, tout au long du printemps 1944, la discussion fit rage, ce qui assura à Bletchley Park de nombreux messages compromettants, révélant notamment que trois divisions de Panzer sous les ordres de Rommel seront sur la côte, que deux divisions seront placées au nord de la Seine et que quatre autres sont en réserve près de Paris sous le commandement personnel d'Hitler.

Grâce à *Ultra*, le décor du théâtre des opérations de Normandie est donc à peu près révélé. C'était alors aux soldats de faire leurs preuves.

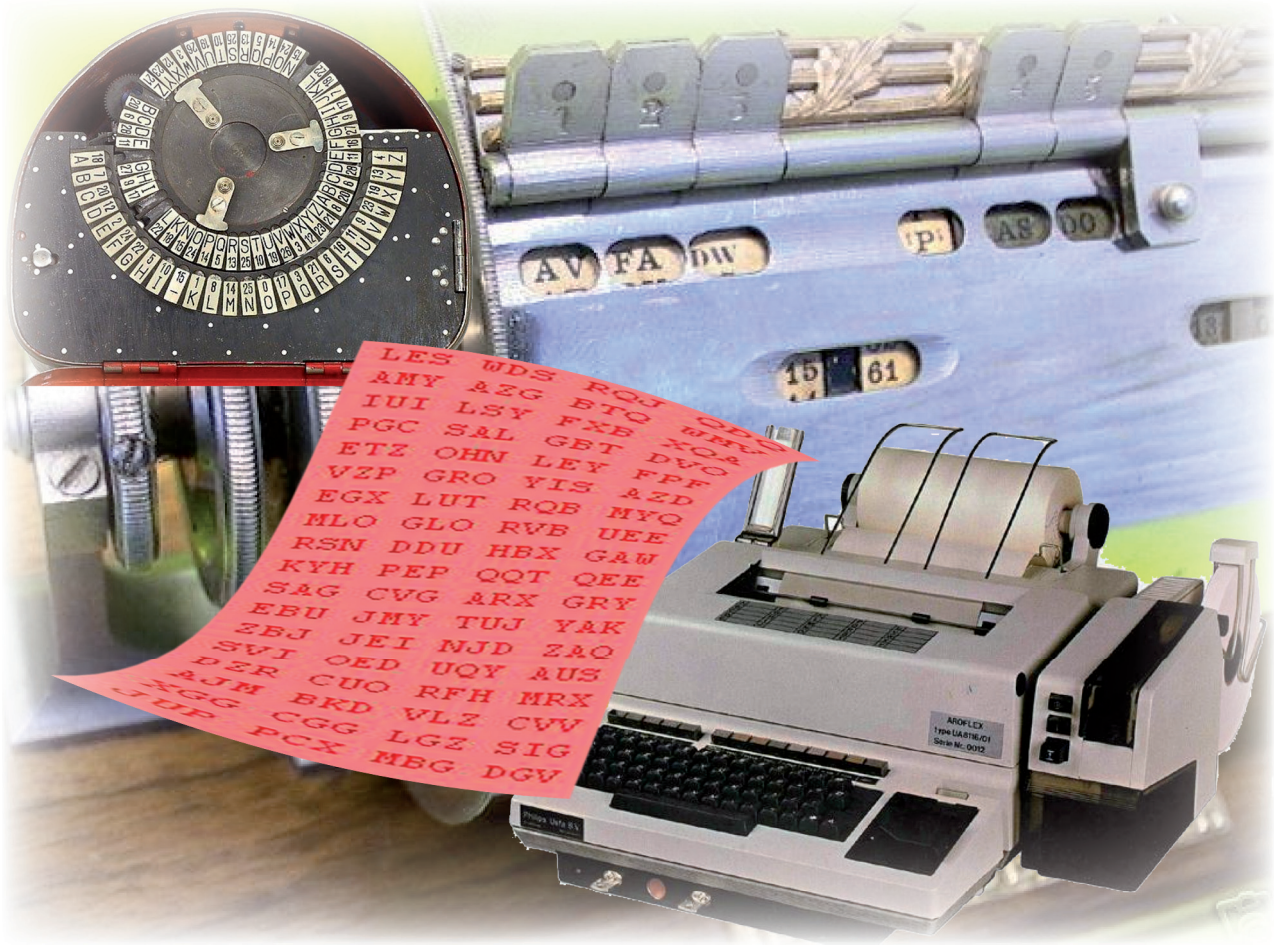
Le secret du décryptage d'Enigma fut gardé pendant trente ans, et ce n'est qu'en 1970/72 que l'on commença à en parler. Le voile ne fut totalement levé qu'en 1974 avec la parution d'un livre : *The Ultra Secret*, écrit par F.W. Winterbotham qui avait été responsable des renseignements distribués par *Ultra*.

Quelques années après la fin des hostilités (en 1952), le matériel avait été transféré à Cheltenham, nouveau centre d'écoutes dont nous avons parlé dans le chapitre consacré au réseau Échelon.

Rejewski n'avait pas su que ses travaux avaient été à la base du déchiffrement d'Enigma ayant été relégué au traitement de chiffres minables dans une unité mineure à Boxmoor…

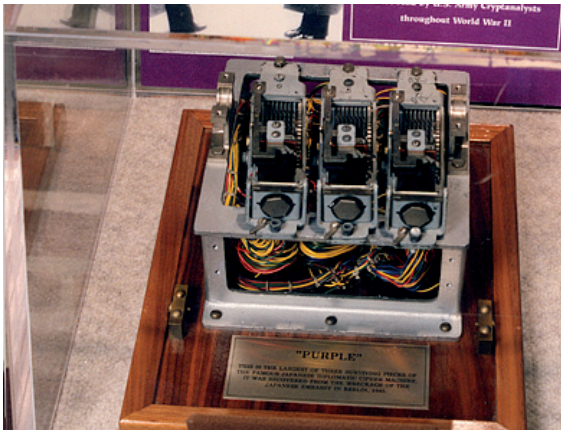
Quant à Alan Turing, son homosexualité ayant été prise pour prétexte en 1952, le gouvernement anglais lui retira sa carte des services de sécurité et il fut évincé des recherches sur l'élaboration d'un calculateur programmable. Enfin, Alastair Denniston, le premier directeur de Bletchley, décédé en 1961, ne reçut la reconnaissance de son vivant. C'est seulement à la sortie du livre de Winterbotham que sa fille put lire un hommage d'un ancien collègue de son père : « V*otre père était un grand homme, envers qui toutes personnes de langue anglaise auront une dette, pour toujours. Que si peu sachent exactement ce qu'il fit est le côté triste des choses…* ».

Autres machines mécaniques, électromécaniques et électroniques à crypter les textes



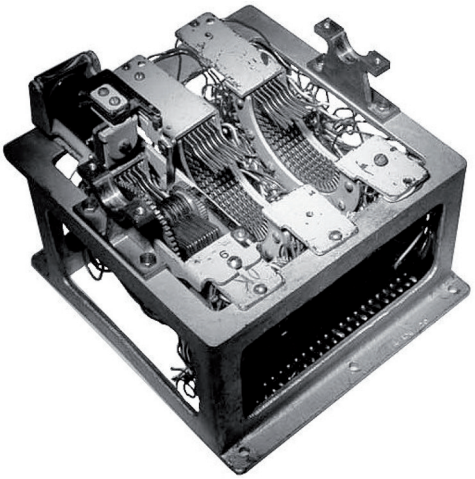
Autres machines à crypter

Le **Code 97** ou code **PURPLE** fut l'une des méthodes de chiffrement utilisées par les Japonais pendant la Seconde Guerre mondiale. Le 97 provient de son nom original en japonais : 97-shiki O-bun In-ji-ki (九七式欧文印字機) qui signifie approximativement « machine à écrire de type 97 pour les caractères européens » ou encore Angooki Taipu B (暗号機B型), soit « machine de chiffrement de type B ». La machine prenait en entrée des caractères européens et produisait une sortie chiffrée



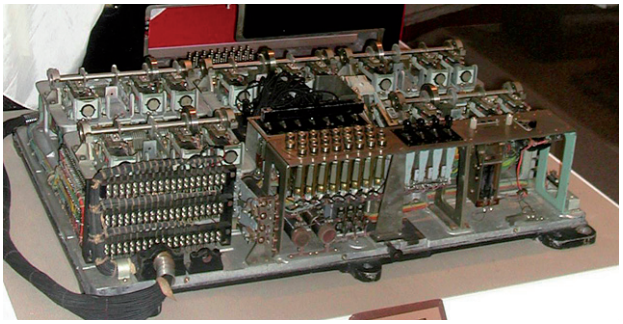
Le 97 fait allusion à l'année 2597 du calendrier japonais, soit 1937. Moins connue qu'Enigma, la machine utilisée pour appliquer ce chiffrement avait des similitudes avec Enigma de par la présence de plusieurs rotors et d'une table de connexions. Elle était surtout destinée à une utilisation diplomatique pour les liaisons entre l'Allemagne et le Japon. Les premières utilisations commencèrent juste avant la guerre.

La machine PURPLE était une amélioration d'une précédente version nommée « Machine M » ainsi que de la « Machine RED ». Ces chiffrements avaient été développés par le capitaine de la marine japonaise Risaburo Ito. Sous couvert du nom de code « Magic », les opérations de déchiffrement occupèrent les Américains dès 1938. Une bonne partie de la cryptanalyse avait été effectuée avant même l'entrée en guerre des États-Unis. Les Japonais (tout comme les Allemands) pensaient que leur chiffrement était impossible à casser, mais William Friedman et Frank Rowlett de l'US Army Signals Intelligence Service réussirent à découvrir des faiblesses, avec en particulier la présence de clés faibles qui rendaient le chiffrement vulnérable.



Les 3 relais d'avancement des rotors ont ici été enlevés pour montrer les pièces internes

Le 7 décembre 1941, l'arrêt des relations diplomatiques par les Japonais, peu avant l'attaque sur Pearl Harbor, était déjà connue des services du chiffre avant même que l'ambassadeur nippon ne l'annonce lui-même. Cet épisode sera à l'origine d'une polémique après-guerre quant aux responsabilités liées au désastre de Pearl Harbor.



JADE était le nom de code donné par les cryptanalystes américains à l'une des machines de chiffrement japonaise de la Seconde Guerre mondiale. Destinée aux messages importants, elle fut utilisée par la marine impériale dès la fin de 1942 jusqu'en 1944. Similaire à CORAL, la principale différence venait de la capacité de JADE à chiffrer des katakana[209] avec un alphabet de 50 symboles. Les cryptanalystes américains en viendront facilement à bout en reconstituant le réseau de connexions au sein de la machine.

[209] Les katakana sont des signes correspondant à des symboles. Ils sont utilisés dans le système d'écriture japonais pour transcrire les mots étrangers, les noms propres étrangers, les noms scientifiques de plantes, animaux, etc.

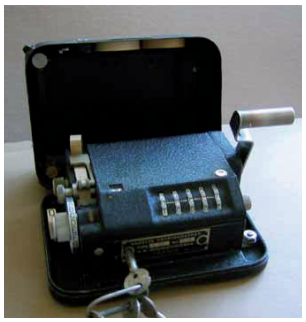
Un exemplaire de la machine fut capturé à Saipan en juin 1944, l'opérateur fut abattu juste avant qu'il ne la détruise. Les Japonais doutant de cette machine qui avait de surcroît des problèmes techniques, décidèrent d'abandonner son utilisation quelques semaines après.

La machine ressemblait à une centrale téléphonique miniature avec 5 circuits comprenant chacune 25 connexions. Les trois premiers circuits agissaient comme des rotors en modifiant les contacts. À chaque symbole chiffré, le premier circuit passait au contact suivant. Le deuxième circuit sélectionnait le contact suivant que lorsque le premier circuit avait fait un parcours complet. Le troisième circuit en faisait de même en fonction de l'état du deuxième circuit. La configuration de ces trois connecteurs était fixe et on ne pouvait pas modifier l'ordre des connexions ce qui représentait une sérieuse limitation. Les deux derniers circuits étaient configurés par l'opérateur.

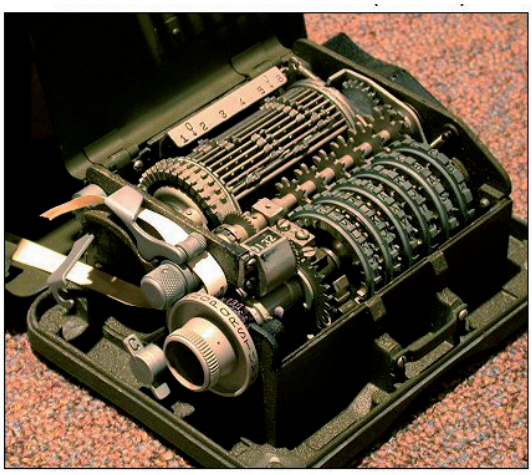
Le clavier de JADE comportait une touche majuscule et 25 autres touches. La machine utilisait deux dispositifs séparés pour chiffrer, l'un pour les majuscules, l'autre pour les minuscules.

B-21 Hagelin

Boris Caesar Wilhelm Hagelin (1892-1983) propose à l'armée suédoise la machine ***B-21***, qui fut pendant une décennie la machine la plus compacte capable d'imprimer des messages chiffrés. Pendant la Seconde Guerre mondiale, les alliés fabriquèrent une autre machine de Hagelin, la Hagelin C-36 (appelée M-209 aux États-Unis), à 140 000 exemplaires. Après la guerre, Boris Hagelin créa à Zoug, en Suisse, Crypto AG, qui est aujourd'hui encore l'un des principaux fabricants d'équipements cryptographiques.



À la demande du Bureau du chiffre français, cette Société construisit la Machine C-35. Cette machine pouvait être connectée à une imprimante à ruban. En 1952, fut lancée la production de la machine CX 52, également nommée M 209 aux États-Unis (ci-dessous à gauche).



En 1952 la NSA introduisit la machine ***KL-7***, également nommée ***ADONIS***. Cette machine comportait 8 rotors mais le rotor n°4 était fixe. Il n'y a donc que 7 fenêtres sur la façade de la machine. Il y a 36 contacts sur chaque rotor.

Cette machine fut en service jusqu'en 1985 entre autres pour les communications des services de l'OTAN. En effet, pendant la guerre froide, les Américains et les Anglais se rendirent vite compte qu'il

était impossible d'utiliser les machines existantes pour crypter leurs communications, car les Soviétiques en connaissaient pratiquement tous les secrets.

La KL-7 remplaça donc la machine SIGABA des Américains et TYPEX des Anglais afin de faciliter les communications entre ces alliés. Le chiffre produit était assez solide, ce fut testé par les premiers ordinateurs, si les conditions d'utilisation étaient respectées. En effet, un système de bagues coulissantes en plastique pouvait être permuté en plus des rotors pour faire varier la rotation de ceux-ci. De plus, son circuit électrique comprenait quatre tubes électroniques blindés : trois thyratrons[210] et une triode. Cependant, son clavier était très dur et on ne pouvait guère taper qu'une lettre par seconde. Enfin, cette machine présentait de très forts rayonnements compromettants[211] aussi bien électromagnétiques qu'acoustiques.

En 1985, quand fut arrêté l'espion Walker, qui avait vendu pendant plus de 17 ans à l'URSS les clés de la KL-7 utilisée par la Marine américaine, il fut décidé de la retirer du service.

Bien sûr, on trouve d'autres machines, en Russie, par exemple : la ***Fialka M-125*** (à droite) d'usage pendant la guerre froide. Machine à 10 rotors et 30 contacts chacun. Au lieu d'illuminer les ampoules pour montrer les caractères résultants du codage des caractères frappés au clavier, la Fialka imprime les caractères sur le ruban perforé et poinçonne simultanément des trous dans la bande en 5 caractères de niveau ressemblant à ceux d'une bande de machine de télétype de Baudot. La Fialka inclut également un lecteur de ruban perforé pour le décodage en entrant rapidement les caractères qui ont été poinçonnés dans un ruban perforé.

La Fialka incorpore un lecteur de cartes qui permet aux cartes perforées d'être employées pour placer des paramètres internes de codage. Ces cartes ont remplacé les tableaux de connexion des Enigma allemandes.

Cette machine fut top-secret jusqu'en 1990

La machine **NEMA** (Suisse)

Entre 1938 et 1940, l'Allemagne avait fourni au gouvernement suisse des machines Enigma pour ses services diplomatiques. Cette machine était le modèle Enigma-K.

Le manque de confiance sur la sécurité de cette machine, et aussi le fait qu'ils pensaient bien que leurs messages pourraient être décodés par les Allemands, amena Hugo Hadwiger, Heinrich Emil Weber et Paul Glur à construire peur propre machine qu'ils nommèrent NEMA (NEue MAschine). Les premiers exemplaires ne furent disponibles

[210] Un thyratron est un type de tube à gaz utilisé comme interrupteur pour les fortes puissances. Ce tube peut prendre la forme d'une triode, d'une tétrode ou d'une pentode, bien que la plupart soient des triodes. Les gaz utilisés peuvent aller de la vapeur de mercure au xénon ou au néon, en passant par l'hydrogène (surtout dans les applications hautes tensions ou les applications nécessitant des temps de commutation très courts). Contrairement aux tubes électroniques classiques, un thyratron ne peut amplifier un signal linéairement.

[211] On entend par rayonnements compromettants, les rayonnements électromagnétiques produits par la machine qui pourraient être captés et analysés. C'est par exemple le cas pour les périphériques Wifi de nos ordinateurs actuels...

qu'en 1945. Cette machine fut utilisée par l'aviation suisse à partir de 1947. Environ 650 machines furent construites. Ces machines furent retirées du service en 1992.

Machine **BID/60** Singlet

Cette machine de fabrication anglaise a été mise en service en 1952 et utilisée jusqu'en 1980. Elle comportait 10 rotors. Elle fut utilisée en même temps que la KL-7 vue plus haut.

Toutes ces machines étant des dérivés de l'Enigma.

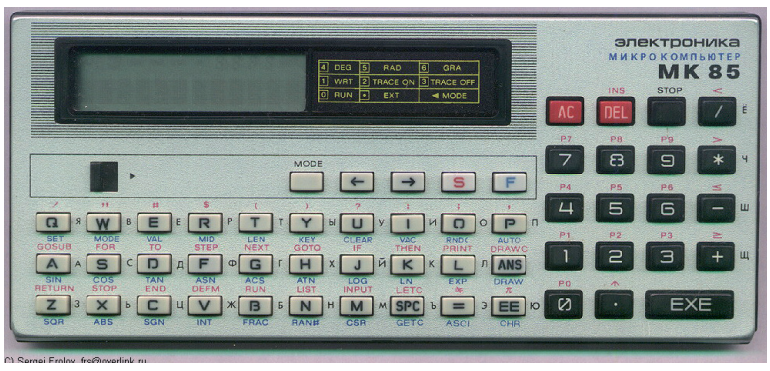
L'arrivée de l'électronique puis des ordinateurs sonna le glas ce de type de matériel.

En 1979, la Société Hagelin commercialisa la **HC-520**, machine de la taille d'une calculette avec un affichage digital LCD.

En 1980, la NSA mettait en service la machine **KL-51**. C'était une machine à crypter hors ligne qui préparait des bandes (cryptées) pour les téléscripteurs. Son fonctionnement était identique dans le système de codage à celui de la KL-7, mais sans rotors, le cryptage étant réalisé par un procédé électronique. Cette machine était désignée sous le nom de **RACE** au Canada et à l'OTAN.

Le **Lektronika MK-85** russe/soviétique est une calculatrice tenue dans la main peut-être la plus avancée pour l'époque. Il y avait des rumeurs au sujet de MK-87 (qui a été censé combiner des dispositifs de calculatrice et de cahier/banque de données).

À la fin des années 80, l'Union Soviétique a développé l'ELEKTRONIKA MK-85, sa calculatrice commerciale la plus avancée. Le MK-85 était un micro-ordinateur programmable en BASIC apparemment basé sur les machines occidentales. Un dispositif cryptographique secret à usage des militaires, nommé **MK-85C** (nom de code ***AZIMUT***) a été basé sur le MK-85 commercial. Il est principalement employé par les forces soviétiques. Le texte à chiffrer est écrit du clavier alphanumérique et peut être édité sur son affichage digital. Le MK-85C a 10^{100} possibilités de clés et peut chiffrer en mode numérique et alphanumérique.



Cette génération de dispositifs cryptographiques, tenus dans la main, peut être vue comme les dernières vraies machines autonomes de chiffrement. À l'ère des ordinateurs toutes les sociétés qui ont développé et ont fabriqué des machines de chiffre ont évolué vers des solutions de chiffrage en temps réel, ainsi que vers des solutions logicielles applicables avec les ordinateurs.

Néanmoins, des dispositifs électroniques de poche de chiffrage sont toujours développés et produits pour des buts spéciaux. La plupart des vieilles machines de chiffre sont maintenant des articles de collectionneurs.

Nous allons terminer ce chapitre en évoquant la machine française **MYOSOTIS**.

L'intervention franco-britannique de Suez, en 1956, avait mis en évidence l'inadéquation de nos moyens de chiffrement, tant nationaux qu'OTAN. Nos alliés britanniques nous firent savoir qu'il ne fallait plus utiliser la B211 qui devait être considérée comme périmée ; en outre, les délais de chiffrement et de déchiffrement étaient apparus largement excessifs. Cela fut un choc considérable pour les militaires. On décida de retirer la B211 des services et d'utiliser à la place la KL-7 qui est alors fournie aux Armées, dans le cadre de l'OTAN.

Sous l'impulsion d'André Muller, les autorités gouvernementales décidèrent de rénover nos moyens de chiffrement. Un plan de modernisation des équipements fut lancé et approuvé en 1957 par la CIC. Des crédits furent débloqués aux Armées.

On acheta d'abord la licence de fabrication de la CX52. Puis on s'orienta vers la conception d'une nouvelle machine et la décision de lancer l'étude d'une machine à chiffrer télégraphique fut prise.

Les trois Armées voulaient chacune en faire une et une véritable guerre des « boutons cryptologiques » commença. La Marine entreprit d'étudier la machine « Ulysse » à laquelle allait collaborer la SEA, la compagnie d'informatique créée par François-Henri Raymond, connue pour les ordinateurs originaux qu'elle fabriquait.

L'Armée de l'Air, avec principalement le Colonel Antoine, se lança dans la conception d'une machine à partir de la KL-7 ; celle-ci est devenue « Violette »et a été étudiée par la SAGEM.

Mais c'est Marius Gaubert, représentant la SEFT à la Sous-Commission « Cryptologie » qui, vers la fin de l'année 1958 ou au tout début de 1959, soumet une idée vraiment originale. Celle-ci consiste à effectuer le calcul du crypto en tirant des alphabets aléatoires[212]. Cette idée est discutée par la Sous-Commission qui, naturellement, la trouve très intéressante. Mais si, sur le plan théorique cette idée est séduisante, encore faut-il démontrer, d'une part, qu'un tel organe de calcul, capable de fonctionner avec la vitesse voulue est réalisable, d'autre part, que l'on sait faire un générateur d'aléa capable de fournir les suites de lettres nécessaires pour constituer les alphabets aléatoires. Ce générateur d'aléa devait offrir un haut niveau de résistance aux attaques cryptographiques connues tout en respectant les exigences du trafic envisagé pour cette machine ! En l'occurrence, il s'agissait d'un générateur pseudo-aléatoire, puisque le destinataire devait pouvoir fabriquer les mêmes alphabets aléatoires pour déchiffrer les messages.

La force de l'idée de Gaubert, c'était de pouvoir effectuer le chiffrement à la volée, sans avoir à mémoriser l'alphabet chiffrant. Marius Gaubert dépose un brevet le 1er août 1960 (brevet nº 834596). L'évolution de l'électronique que l'on pressentait déjà permettait d'espérer que ce principe pouvait être rendu compatible avec les exigences de vitesse des transmissions télégraphiques (50 et 75 bauds). Jean-Pierre Vasseur a immédiatement vu un grand intérêt dans ce brevet, surtout si on pouvait le coupler avec le système de génération de clé auquel il réfléchissait. L'idée de construire un prototype d'évaluation prend corps.

[212] Il semblerait que l'idée de tirer un alphabet aléatoire pour traiter chaque lettre ait germé au CECS parmi les stagiaires, mais on ne savait pas comment la réaliser. L'idée aurait été exposée à M. Gaubert qui a su la mettre en pratique par le mécanisme du chiffrement à la volée !

Par ailleurs, l'OTAN lançait à ce moment un concours pour réaliser une machine cryptographique pour la télégraphie et dont l'échéance de présentation était février 1963.

Le Comité Militaire de l'OTAN avait lancé un appel à candidature pour une machine à chiffrer télégraphique électronique, sur la base de spécifications définies par l'ACSA (*Allied Communications Security Agency*). Il était précisé, entre autres, que la machine devait être sans bande, ni rotor (*tapeless and rotorless*), donc pas de systèmes utilisant des « bandes-clés une fois », ni de machines électromécaniques dérivées de l'Enigma, comme la KL-7.

Elle devait avoir les deux modes de fonctionnement : en ligne ou hors ligne. En outre, l'ensemble de la station de chiffrement devait répondre à des contraintes très sévères concernant le rayonnement et la conduction électromagnétiques des circuits véhiculant des informations claires traitées par la machine (contrainte TEMPEST : *Transcient ElectroMagnetic Pulse Emanation Standard*). Le problème du rayonnement avait été posé au début des années cinquante par une machine à bande aléatoire dont les relais provoquaient un très fort rayonnement dans lequel on pouvait retrouver des informations claires. Il semble que les Américains avaient appris que ce phénomène avait été exploité à Moscou au détriment de leur Ambassade. Le cahier des charges indiquait simplement « aucun rayonnement détectable », sans préciser les conditions de mesure !

La technologie électronique en circuits discrets de l'époque et les transistors, qui venaient d'être inventés (1948), allaient permettre une souplesse et une complexité de conception cryptologique jamais atteinte par la technologie électromécanique antérieure. En outre, une rapidité de traitement supérieure aux vitesses télégraphiques usuelles était envisageable : le sempiternel reproche de lenteur fait au Chiffre allait enfin tomber ! Il est vrai que l'électronique des années cinquante utilisait presque exclusivement des lampes (tubes à vide : diodes triodes, pentodes...). Mais le nombre de circuits nécessaires rendait la réalisation d'une machine à chiffrer à lampes totalement irréaliste. Il était temps de songer à recourir à l'électronique des composants solides, celle des semi-conducteurs, pour réaliser de nouvelles machines.

Il s'agissait non seulement d'améliorer les qualités cryptographiques de ces machines, mais aussi leurs conditions d'utilisation en automatisant plus de fonctions dans un volume plus faible et en les rendant plus maniables pour réduire les erreurs d'exploitation. En outre, l'électronique à semi-conducteur diminuait considérablement le poids, l'encombrement et la consommation, donc l'alimentation. Ceci allait dans le sens d'un élargissement du domaine d'emploi des machines, surtout pour les besoins tactiques, et permettait d'envisager des systèmes embarqués ou portables. Il fallait aussi satisfaire les nouvelles exigences des télécommunications, en particulier l'augmentation de la vitesse de transmission.

Après bien des péripéties dues à la présentation à ce concours de trois autres machines, la KW-7, présentée pas les USA, la ALVIS présentée par le Royaume-Uni et l'ELCROTEL présentée par l'Allemagne, et bien que la machine anglaise, plus chère et moins performante, fut retenue dans un premier temps, 6 mois plus tard Myosotis obtient l'approbation du Comité Militaire pour la protection des informations de toutes classications OTAN. La machine Myosotis est donc approuvée par l'OTAN. C'est un beau succès[213] !

L'aboutissement du projet Myosotis marquait une avance de la Thomson-CSF dans le domaine du Chiffre, non seulement sur le plan national, mais aussi au plan international.

Mais à la suite du choix de Myosotis pour être l'équipement cryptographique des trois armées, SAGEM avait demandé une compensation. Dans le cadre d'un protocole d'accord, suscité par le SCTI, il est décidé que SAGEM participera à la fabrication en série des Myosotis : SAGEM fabriquera le sous-ensemble de commande télégraphique, CSF se réservant le bloc chiffrant.

[213] Mais il faut avouer que ce fut une victoire à la Pyrrhus : la France devait sortir de l'Organisation Militaire du Traité de l'Atlantique Nord en mars 1966, de sorte que la CSF n'eut guère l'occasion de fournir des matériels de chiffrement aux Armées de l'OTAN. Et les services américains étaient en possession de tous les détails de Myosotis !

Enfin, la fabrication de Myosotis est confiée au centre de Cholet, rattaché à Levallois depuis sa création en 1936. L'usine de Cholet commence l'industrialisation de Myosotis en 1964 et sa fabrication en série en 1966. Elle était dotée d'un service d'étude et de développement. Une section de ce service prend en charge ce nouveau matériel avec MM. Candelier et Lamotte qui avaient participé à l'étude et à la réalisation des prototypes à Puteaux et à Levallois.

Au début de la conception de Myosotis, les transistors au silicium ayant des performances insuffisantes n'étaient pas disponibles. C'est pourquoi les transistors au germanium avaient été choisis. Mais à l'époque du lancement de la fabrication des Myosotis à Cholet, les transistors au germanium commençaient à être supplantés par les transistors au silicium. Cependant, l'usine de Cholet ne put prendre en compte cette évolution technologique : les délais de fabrication étaient trop courts et la reprise de la conception des Myosotis dans cette nouvelle technologie juste au moment de l'industrialisation aurait été trop coûteuse. C'est pourquoi la filière germanium fut maintenue pendant plusieurs années par l'usine de Saint-Egrève.

En 1974, mille machines auront été réalisées par Cholet et, au total, ce sont mille cinq cents équipements qui sortiront de l'usine de Cholet.

Signalons que, grâce à l'habilitation OTAN, un ensemble de deux équipements (un pour chaque extrémité de la ligne) ont même été fournis à la Norvège pour protéger une de ses liaisons !

Les trois Armées et le Ministère des Affaires Etrangères se sont équipés de Myosotis. L'Armée de Terre, imitée par les Affaires Etrangères, privilégie le chiffrement en ligne au sein de ses centres de transmissions et ses chiffreurs deviennent des cryptotélégraphistes. Par contre, l'Armée de l'Air, son souci d'économie rejoignant son souci de sécurité, fait exploiter ses Myosotis hors ligne par des sous-officiers régulateurs chiffreurs.

Le projet Myosotis fut la conséquence de la volonté de l'État français de se doter de moyens de chiffrement modernes, sûrs et adaptés à ses besoins. L'importance et la qualité des travaux qui ont abouti à la réalisation de cette machine ont permis de doter la France non seulement d'une doctrine du Chiffre cohérente, mais aussi de structures étatiques et industrielles qui l'ont placée au tout premier rang dans le monde dans le domaine de la cryptographie.

La position de la France s'est ensuite maintenue pendant une trentaine d'années grâce aux développements ultérieurs de nouveaux systèmes cryptographiques, développements dont la vigueur a encore été accentuée par les progrès considérables que l'électronique et les communications ont connus durant cette période. Avec l'introduction progressive de l'informatique dans les divers systèmes d'information, les conditions d'utilisation du Chiffre se sont considérablement modifiées en évoluant vers une intégration dans ces systèmes toujours plus poussée et une automatisation sans cesse accrue.

À partir du début des années quatre-vingt-dix, l'apparition du Chiffre civil et le formidable essor d'Internet ont posé de nouveaux problèmes. Les besoins des civils ainsi que leur façon d'utiliser le Chiffre étaient différents de ceux des gouvernements.

De nombreux systèmes de chiffrement, en majorité d'origine américaine, sont alors apparus sur le marché dans une anarchie d'autant plus complète que les nouveaux utilisateurs du secteur civil n'avaient aucune compétence et aucun repère pour se faire une idée de leur valeur.

Crypter la voix

En France jusque dans les années 60, on utilisait pour les liaisons radiotéléphoniques un mécanisme de protection consistant à renverser la bande de fréquences du signal de la parole (250 à 2750 Hz), via un modulateur à 3000 Hz : après filtrage, la modulation était inversée autour de la fréquence centrale 1500 Hz. C'est ce que l'on appelait le « secret international ». En cas d'interception, ce dispositif rendait la conversation inaudible (ou plutôt difficile à comprendre). Mais ce système, qui en réalité ne contenait aucun secret, était très facilement décryptable. Il suffisait de renverser à nouveau la bande.

Ce système avait donc été ensuite rendu plus compliqué en divisant cette bande en cinq parties à peu près égales et en modifiant l'ordre dans lequel se trouvaient ces cinq morceaux de bande qui pouvaient aussi être inversés. C'était le « secret à découpage de bande », conçu par la compagnie américaine *Western Electric Company*.

Cette transformation du spectre était réalisée, de façon mécanique, au même instant aux deux extrémités de la ligne de transmission. La combinaison qui, à chaque instant, définissait ces permutations et inversions était changée périodiquement (typiquement toutes les vingt secondes) par un système mécanique à base de cames qu'un moteur électrique faisait tourner.

Ce dispositif était complexe et relativement lourd à mettre en œuvre. Cependant, le secret était considéré comme faible, car par une analyse de la continuité des bandes, on pouvait reconstituer le signal clair, au besoin en faisant quelques essais si des incertitudes de continuité apparaissaient.

Bien que des brouilleurs de voix fussent utilisés des deux côtés de l'Atlantique, chaque camp avait les moyens de « casser » le système de brouillage de l'autre en procédant à une analyse fine du spectre audio des conversations. Il n'y avait, de fait, aucune sécurité réelle.

Green Hornet, ou le frelon vert

Le 7 décembre à 11 h 58, heure de Washington (6 h 28 à Hawaii), le Général George Catlett Marshall[214], chef des armées des États-Unis était face à une décision difficile. Les casseurs de codes américains avaient déchiffré le trafic diplomatique japonais et il devenait évident que l'entrée en guerre avec le Japon se précisait. Fort de cette information, on a décidé d'une alerte générale à toutes les forces du Pacifique, y compris Hawaï. Il fallait faire vite, et la seule manière assez rapide était le téléphone. Or, il s'agissait d'informations secrètes très importantes. Le seul système de brouillage en vigueur à l'époque était le brouilleur A-3. C'était un système basé sur la technologie des années 20, et personne ne croyait à son efficacité en matière de brouillage. On savait par ailleurs que la Deutsche Reichspost, l'organisation alle-

[214] George Catlett Marshall (1880-1959), général d'armée américain (*General of the Army*), au cours de la Seconde Guerre mondiale fut l'un des principaux conseillers et stratèges du président Roosevelt pour la conduite du conflit. De 1941 à la fin de la guerre, il participe à toutes les conférences inter-alliés en qualité de conseiller privilégié de Roosevelt. Dirigeant les forces armées américaines engagées en Europe, il s'oppose en 1942 au débarquement en Afrique du Nord, réorganise l'Air Force et planifie le débarquement de Normandie. Il est très déçu de ne pas recevoir le commandement du D-Day mais Roosevelt explique qu'il ne peut se passer de son conseiller. Plus tard, Winston Churchill déclare au sujet de Marshall qu'il était « l'organisateur de la victoire ». En décembre 1944 Marshall est nommé général d'armée, tout comme les trois autres conseillers de Roosevelt William Leahy, Ernest King et Henry Arnold et les deux principaux commandants en chef des opérations Dwight Eisenhower et Douglas MacArthur. Il était franc-maçon.

mande chargée des communications téléphoniques, avait cassé le A-3. Grâce à un poste d'interception situé dans une ancienne pension de jeunesse sur la côte hollandaise, le troisième Reich écoutait et décryptait tous les appels, même codés avec le A-3, y compris ceux de Franklin Roosvelt, de Winston Churchill, et de tous les autres chefs militaires.

Conscient que l'information de la mise en alerte des troupes du Pacifique pouvait être ainsi connue des Japonais, le général Marshall se refusa à utiliser le brouillage A-3, il fit parvenir son message par radiogramme codé. Ce fut une erreur fatale. Lorsque le message parvint à destination, l'attaque de Pearl Harbor était effective. Depuis 7 h 53, les premières bombes nipponnes étaient larguées. En fait, le message parvint à l'ambassadeur américain au Japon environ dix heures après la fin de l'attaque...

Le lourd bilan de l'attaque japonaise mit en relief la situation fâcheuse des communications stratégiques, posant clairement aux chefs militaires et politiques le défi de réaliser des transmissions sûres et rapides. Ce fut le début de la mise en place d'un système crypté de transmission de la voix, mais aussi du système mondial d'écoute développé par la NSA connu plus tard sous le nom d'*Echelon*.

Dès 1936, les Laboratoires Bell avaient commencé d'explorer les techniques pour transformer le signal analogique[215] produit par la voix en signal numérique. C'est la technique dite de l'échantillonnage[216]. Les recherches de Homer Dudley, des Laboratoires Bell, avaient abouti en 1939 à un synthétiseur de voix présenté à New York sous le nom de « vocoder ». Il y avait, à l'époque, environ quatre-vingts brevets déposés pour crypter la voix, mais aucun n'avait de valeur suffisante au niveau sécurité pour en faire un système exploitable au niveau militaire ou diplomatique. La Deuxième Guerre mondiale approchait, et il fallait intensifier les recherches.

SIGSALY

La première machine opérationnelle fut la machine SIGSALY.

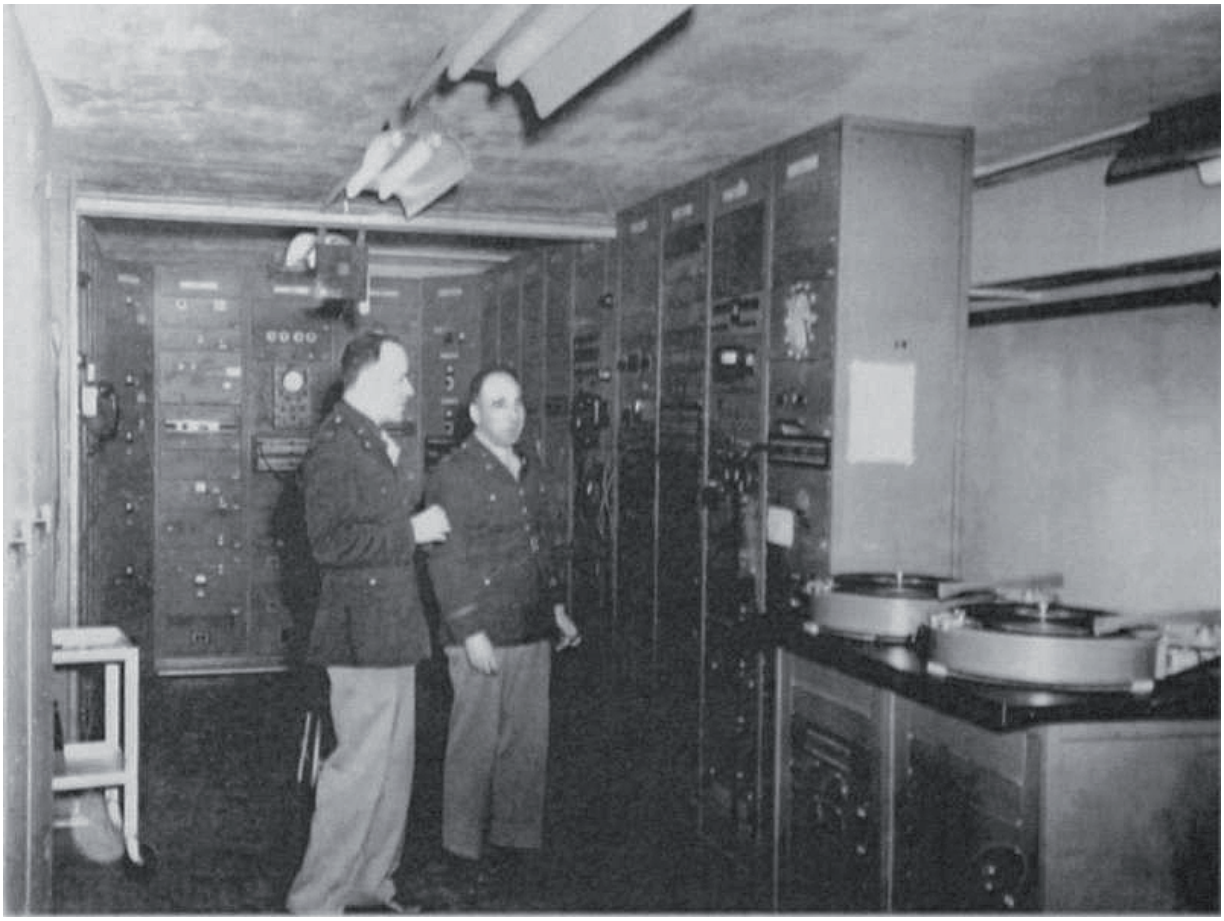
Le nom de SIGSALY n'était pas un acronyme, mais un nom inventé. Un prototype a été développé par les Laboratoires Bell et présenté à l'armée des USA. Le premier nom de cette machine était Green Hornet (Frelon vert), à cause du bourdonnement que provoquait la machine pour brouiller la conversation et la rendre incompréhensible à des oreilles clandestines. Les responsables militaires furent impressionnés et un contrat fut établi pour sa mise en place.

SIGSALY devint de fait le premier système de télécommunications numériques, déployé par l'armée des États-Unis à partir du 15 juillet 1943 pour les communications entre les états-majors alliés US et UK pour pallier l'insécurité des télécommunications analogiques brouillées, restituées en clair en temps réel par l'armée allemande. À partir de cette date, la Deutsche Reichspost a commencé à remarquer que les signaux alliés codés avec le système A-3 avaient considérablement été réduits. L'ingénieur en chef en place à la station d'écoute hollandaise en tira la conclusion qu'un autre système avait été mis en place.

Dès 1942 avait été créé un corps spécialisé, le *805th Signal Service Company*, dont le rôle était de faire fonctionner le futur réseau vocal codé. En juillet 1944, l'école et les services du 805th furent installés au

[215] Un signal est analogique lorsque son information est représentée par la variation d'une grandeur physique.

[216] L'échantillonnage consiste à transformer un signal analogique (continu) en signal numérique (discret), en capturant des valeurs à intervalle de temps régulier (ici *temps* est à prendre au sens large et s'applique à tout signal). C'est une étape nécessaire pour pouvoir enregistrer, analyser et traiter un signal par ordinateur, car celui-ci ne peut traiter que des nombres. Il faut distinguer l'échantillonnage de la quantification, mais ce sont toutes deux des étapes nécessaires à la numérisation d'un signal. La fréquence à laquelle les valeurs sont capturées est la *fréquence d'échantillonnage*, appelée aussi cadence d'échantillonnage, ou taux d'échantillonnage, exprimée en Hz.



La machine SIGSALY en 1943. Remarquer au premier plan les platines avec les disques vinyle servant de clés de codage.

Pentagone à Washington. À cette époque, 193 officiers avaient été formés. L'unité atteindra par la suite 356 personnes. Ce personnel a été réparti dans les 12 stations opérationnelles 24 heures sur 24.

À part Washington, on trouvait des stations à Londres, Alger, en Australie, Hawaï, Oakland, en Californie, à Paris (après la Libération), à Guam, et après la victoire, à Francfort et Berlin.

Il y avait aussi une station flottante sur un navire de 250 tonneaux, de type OL-31, qui servait aux communications du général Douglas MacArthur dans sa campagne du Pacifique. Ce système aurait été utilisé dans le cadre d'une opération aérienne contre le Japon si nécessaire.

Un bel hommage fut rendu à ce système de communication crypté par la Deutsch Reichspost qui fit transmettre un rapport à l'État-major allemand disant : « Il n'y a plus rien à obtenir d'elle, maintenant » en parlant de la station d'interception hollandaise.

Sigsaly fut utilisée jusqu'en 1946, mais son existence est restée secrète jusqu'en 1976, et a servi de support à plus de 3000 conférences secrètes.

Techniquement, le système, basé sur la nouvelle technique vocoder[217] (Voice Operated reCorDER) marque une série de premières technologiques :

[217] Créé par Homer.W. Dudley aux Bell Labs en 1939, le vocoder était initialement un outil d'analyse et de synthèse de la voix. L'analyse procédait par association d'un lot de filtres passe-bande étroits, et le synthétiseur produisait les sons en filtrant une source de bruit selon les données enregistrées lors de l'analyse, au travers de VCA. Révelé au public à l'exposition universelle de New-York en 1939 avec un modèle dénommé « Voder », signalé par V. Bush en 1945 dans le même texte qui introduisait la notion de World Wide Web (memex), le vocoder entra dans le monde de la musique après sa présentation en Allemagne en 1948. Dans ce domaine, il n'est plus utilisé pour sa capacité de synthèse, mais pour moduler une source, typiquement de type « nappe » (cordes, orgue) par les partiels résultant de l'étage d'analyse du vocoder.

– 1. Première téléphonie chiffrée
– 2. Première transmission de voix numérisée
– 3. Première transmission de la parole en codage PCM (Pulse Code Modulation)
– 4. Première utilisation de Companded PCM
– 5. Premiers exemples de modulation FSK (Frequency Shift Keying)
– 6. Première utilisation de FSK-FDM (Frequency Shift Keying - Frequency Division Multiplex) comme méthode de transmission sur support évanescent
– 7. Première utilisation de la technique « eye pattern » pour ajuster l'intervalle d'échantillonnage.

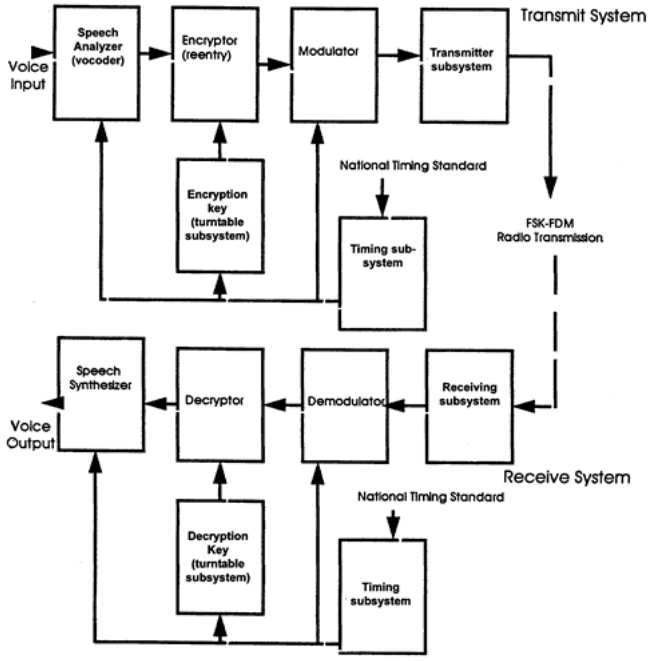


Diagramme du fonctionnement de SIGSALY

La machine était composée d'environ une quarantaine de châssis électroniques supportant des relais, des moteurs synchrones, les tubes à vide redresseurs à vapeur de mercure de taille imposante : diamètre 4 pouces (environ 11 cm) et hauteur 14 pouces (environ 36 cm), une alimentation de forte puissance et un système de refroidissement conséquent. La machine était imposante avec ses 55 tonnes.

C'était la première application du PCM développé par Harry Nyquist[218].

Le PCM

La modulation d'impulsion codée ou MIC, (en anglais Pulse Code Modulation, généralement abrégé en PCM) est une technique d'échantillonnage non comprimé, utilisée notamment pour les disques compacts audio, pour l'enregistrement sur bandes DAT, ainsi que pour les fichiers WAV standards.

Il s'agit d'une représentation numérique d'un signal analogique où la hauteur du signal est prélevée régulièrement à intervalles uniformes de durée T. Chaque échantillon est quantifié sur une série de symboles dans un code numérique, qui est habituellement un code binaire. Le Théorème d'échantillonnage de Nyquist-Shannon[219] stipule que les fréquences plus hautes que la moitié de la fréquence *fs* d'échantillonnage (*fs* = 1/T) ne peuvent pas être reconstruites.

[218] Harry Nyquist (7 février 1889 - 4 avril 1976) a été un important contributeur à la théorie de l'information et à l'automatique. Il est né à Nilsby en Suède. Il émigra vers les États-Unis en 1907 et entra à l'université du Dakota du Nord en 1912. Cinq ans plus tard, il fut reçu comme docteur en physique à l'université de Yale. Après avoir travaillé de 1917 à 1934 chez AT&T, il partit pour les laboratoires Bell. Aux Bell Labs, il fit des recherche sur le bruit thermique appelé également « bruit de Johnson-Nyquist » et sur la stabilité des amplificateurs bouclés (voir Diagramme de Nyquist). Ses travaux théoriques sur la détermination de la bande passante nécessaire à la transmission d'information, publiés dans l'article *Certain factors affecting telegraph speed* posent les bases pour les recherches de Claude Shannon qui amèneront la théorie de l'information. En 1927 Nyquist détermine qu'un signal analogique doit être échantillonné à au moins deux fois la plus haute fréquence le constituant si l'on veut le convertir en un signal numérique correspondant. Ce résultat, connu sous le nom de théorème d'échantillonnage de Nyquist-Shannon, a été publié dans l'article *Certain topics in Telegraph Transmission Theory* (1928). Il prit sa retraite en 1954 et mourut à Harlingen dans le Texas.

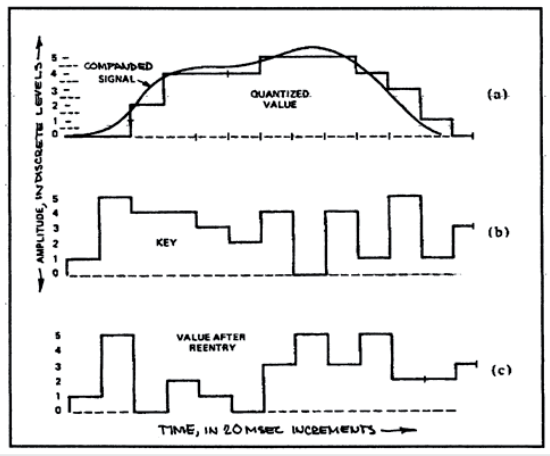
[219] Le théorème de Nyquist-Shannon, nommé d'après Harry Nyquist et Claude Shannon, énonce que la fréquence d'échantillonnage d'un signal doit être égale ou supérieure au double de la fréquence maximale contenue dans ce signal, afin de convertir ce signal d'une forme analogique à une forme numérique. Ce théorème est à la base de la conversion numérique des signaux. La meilleure illustration de l'application de ce théorème est la détermination de la fréquence d'échantillonnage d'un

Plusieurs flux PCM peuvent être multiplexés[220] dans un flux de données global plus grand, grâce à une technique appelée Time-Division Multiplexing ou TDM. Initialement inventée par l'industrie téléphonique, la technologie TDM est aujourd'hui largement utilisée dans les stations de travail audionumériques comme Pro Tools.

Les clés de SIGSALY

Comme dans tout système de chiffrage, la machine SIGSALY disposait de clés. Les valeurs aléatoires nécessaires à la génération des clefs de chiffrement étaient produites par le bruit thermique large bande venant de redresseurs à vapeur de mercure, converties en signaux par modulation FSK et enregistrées sur disques vinyle. Ces disques servaient de support des clefs.

Une série de « masters » a été créée sur des plateaux de cire de 16 pouces de diamètre. Ces disques ont servi à la fabrication des disques vinyle, qui contenaient chacun l'équivalent de 12 minutes de clé de cryptage qui furent distribués dans les différents postes cités plus haut. Les masters étaient détruits ensuite. La technologie évolua rapidement et l'on put créer des disques directement sur acétate soutenu par une couche d'aluminium, sautant l'étape du master. Les clés étaient changées pour chaque conférence et détruites après utilisation.



La ligne (a) représente la quantification numérique de six niveaux du canal de vocoder.

La clé aléatoire est figurée par la ligne (b). Cette information est produite à partir des enregistrements lus sur le sous-ensemble de plateaux tourne-disques. La clé est combinée avec le signal produit en (a) par un processus appelé « reentry ». Ce procédé est mathématiquement décrit comme « addition de deux valeurs modulo 6 ».

La ligne (c) représente le flux de données qui est alors transmis par l'équipement radio de FSK-FDM.

Les bases du procédé de réception et de déchiffrage sont l'inverse du procédé de chiffrage. Les signaux multicanaux sont démodulés, et chaque canal est décrypté en soustrayant modulo 6 la valeur de la clé.

On peut alors reconstruire le signal audio original pour le transformer en discours intelligible.

Ce procédé, compte tenu de la technologie des années 40, était très complexe à mettre en œuvre

Le codage et le décodage s'effectuant en temps réel (voir encadré), le principal problème était la synchronisation parfaite de la machine émettrice et de la machine réceptrice. La fréquence d'échantillonnage de 20 millisecondes employée exigeait l'utilisation de plateaux tourne-disque tournants avec une extrême précision. Le moteur synchrone était piloté par un oscillateur à quartz de 100 kilohertz, la précision atteignait le millionième.

Il fallait que les deux machines soient également synchronisées entre elles, or il n'y avait pas de signal de synchronisation transmis d'une machine à l'autre. Les opérateurs devaient

CD audio, qui est de 44,1 kHz. En effet, l'oreille humaine peut capter les sons jusqu'à 16 kHz, quelquefois jusqu'à 20 kHz. Il convient donc, lors de la conversion, d'échantillonner le signal audio à au moins 40 kHz. 44,1 kHz est la valeur normalisée par l'industrie.

[220] Le multiplexage est une technique qui consiste à faire passer deux ou plusieurs informations à travers un seul support de transmission.

donc se synchroniser avant le début de la transmission. Pour ce faire, la première plage de chaque disque comportait des signaux spéciaux servant à cette synchronisation. Les opérateurs pouvaient ainsi régler avec précision la rotation des tourne-disques. C'était un processus complexe, mais il fonctionnait. Le système plateau tourne-disque-clé était appelé SIGGRUV avec les disques vinyle, puis SIGJINGS quand on employa des disques acétate.

Il y avait une alternative mécanique à la clé enregistrée. Cette clé était fournie par un sous-ensemble appelé AK (Alternative Key). Le sous-ensemble AK était composé d'un grand nombre de commutateurs de progression de relais et autres dispositifs. Ce système utilisait un système de chiffrage habituellement utilisé pour les télétypes.

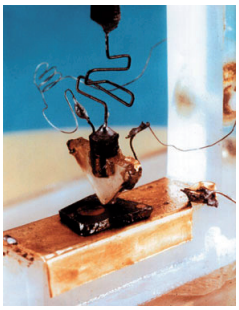
Le système AK était en fait plutôt utilisé pour la maintenance ou pour les communications sans grande valeur stratégique.

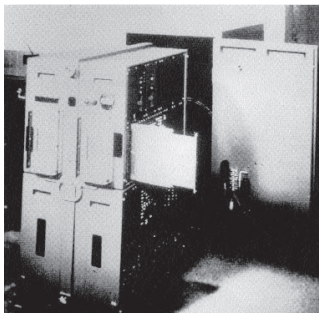
Les autres matériels de codage de la voix

Un des principaux développeurs de matériel de codage de la voix fut un employé de la NSA nommé Thomas E. Tremain.

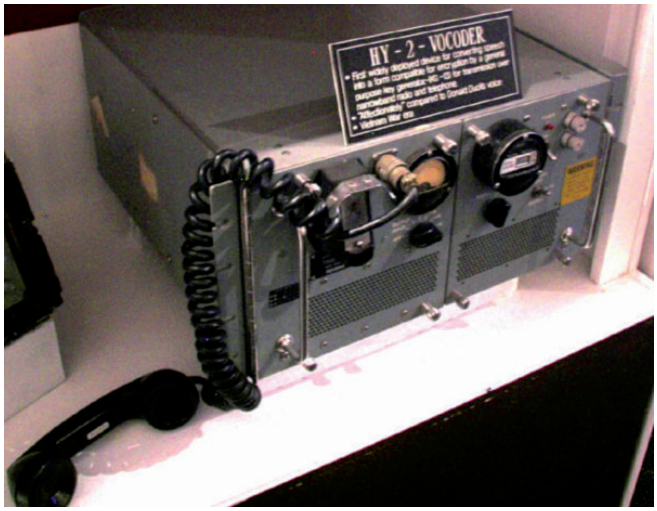
Après SIGSALY, et jusqu'à l'arrivée de T. E. Tremain en 1959, plusieurs générations de codeurs de voix ont été développées. Il y eut le KO-6 (1949) qui était un appareil similaire au SIGSALY mais fonctionnant à une vitesse de 1200 bauds par seconde.

En 1953, fut produit le KY-9 (photo). Cet appareil fonctionnant à 1650 bauds/s employait 12 canaux et était construit avec des transistors faits à la main (ci-contre à gauche). Des 55 tonnes de la machine SIGSALY on était passé à 255 kg.





En 1961, le premier projet développé par T. E. Tremain fut le vocoder HY-2. Cet appareil fonctionnait avec 16 canaux à 2400 b/s. Le système était modulaire et utilisait la technologie « Flyball ». Son poids n'était plus que d'environ 45 kg.



HY-2

Le HY-2 a été largement déployé au Vietnam, mais selon les documents Web de la NSA, le président Johnson a refusé d'utiliser le HY-2 en raison de sa mauvaise qualité du son donnant une voix de « Donald Duck ». Son large déploiement est confirmé par son utilisation dans *AUTOSEVOCOM I*, un réseau mondial de téléphonie sécurisée utilisée par le gouvernement américain dans les années 1960.

Le HY-2 a été la dernière génération de technologie de type vocoder utilisée aux USA.

Entre 1962 et 1964, on commença à faire des essais de numérisation de la voix par ordinateur. C'est entre 1964 et 1968 que l'on vit apparaitre les premiers « vocoders » expérimentaux entièrement numériques.

AUTOSEVOCOM I

Au milieu des années 1960, le Gouvernement des États-Unis a décidé de mettre en œuvre un réseau voix sécurisé.

Une partie de ce système a été déléguée à l'US Army Strategic Communications Command (USASCC), à Fort Huachuca, Arizona. Un sous-groupe de commandement, à savoir la 7ème US Army Signal Command, (Siège social à Fort Ritchie, dans le Maryland) a été chargé de toutes les communications de l'armée US au sein de la zone continentale des États-Unis (CONUS)

Chaque armée aux États-Unis avait un Signal Post Office, qui est chargé du fonctionnement de tous les services téléphoniques, des systèmes radio, centre de communication, etc ...

Il a fallu plusieurs années pour mettre en œuvre AUTOSEVOCOM-1 au sein du CONUS.

L'illustration ci-contre montre l'installation AUTOSEVOCOM I

La technologie « Flyball »

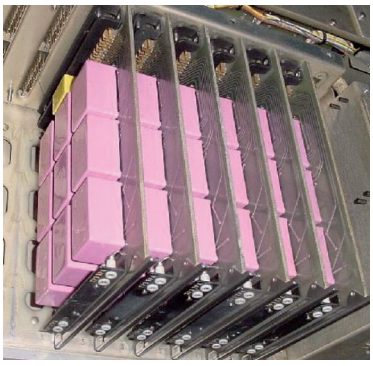
Au fur et à mesure du développement des composants discrets (un composant électronique discret est un composant ne réalisant qu'une fonction simple : diode, transistor, etc.), il devint évident qu'on ne pouvait se contenter de l'utilisation d'une seule face des circuits imprimés.

En même temps, l'industrie de l'électronique développa le concept modulaire (Cordwood Modules). Avec cette technique, les composants sont empilés comme des bâtons de bois et soudés sur une seule face de la carte électronique.

Cette technique, connue sous le nom de « Flyball Modules » a été très utilisée dans les dispositifs de codage de la voix mis au point par la NSA. Les modules étaient enrobés de résine époxy de couleur.

On ne tarda pas à mettre au point des circuits imprimés double face. L'interconnexion entre les deux faces de la carte se faisait par des fils appelés fils « Z ». Leur implantation et leur soudure étaient très délicates, et *The United Shoe Company* mit au point un système d'œillets qui firent des connexions fiables, et ce système fut très prisé pour les circuits imprimés à usage militaire.

La couleur de l'enrobage indiquait la fonction du module, et la tentative d'ouverture d'un module entraînait la destruction de ses composants. Les couleurs des modules étaient : rose, jaune, vert, bleu, rouge, orange et noir. Dans les modèles de vocodeurs KG-13, le noir était un générateur de bruit utilisé comme générateur de clé aléatoire utilisé dans le procédé de cryptage.



On ne connaît pas l'origine du nom « Flyball module » et les techniciens n'employaient que l'expression « module »

Avec l'apparition en 1967 des premiers circuits intégrés à base de silicium, ces modules devinrent obsolètes et furent progressivement abandonnés.

En 1974, la première simulation en temps réel est effectuée à l'aide d'un processeur CSP-30. C'est une date importante dans l'histoire du traitement des signaux, et cela conduisit à la production d'une nouvelle génération de matériels de codage de la voix en temps réel.

STU-III

STU-III est une famille de téléphones sécurisés mis en place en 1987 par la NSA pour l'utilisation par le gouvernement des États-Unis, ses entrepreneurs et ses alliés.

Les STU-III de bureau sont très similaires en apparence aux téléphones de bureau classiques : prise téléphonique murale, et ils peuvent faire des appels vers n'importe quel utilisateur de téléphone ordinaire (par exemple, recevoir des appels, toutefois sans aucune protection spéciale).

Quand un appel est destiné à un autre STU-III correctement mis en place, l'appelant peut demander à son correspondant d'ouvrir la transmission sécurisée (ou, familièrement, à « rendre sécurisé »). Ils doivent alors appuyer sur un bouton sur leurs téléphones et, après un délai de 15 secondes, leur appel est crypté pour empêcher les écoutes.

Il existe des versions portables et militarisées, et la plupart des STU III contiennent un modem interne et un port RS-232 pour les données et la transmission par télécopie.

Les fabricants ont été AT & T (puis transféré à Lucent Technologies), RCA (maintenant - L3 Communications), et Motorola.

Le **CSD 3324E** est un système complet de sécurité des communications de bureau qui fournit la voix, le fax et le chiffrage de données dans un paquet de téléphone. Le CSD 3324E a un mode de cryptage qui a été à l'origine développé pour les canaux faibles à haute fréquence. En conséquence, les communications cryptées sont toujours possibles avec le CSD 3324E, même dans des conditions de mauvaise fiabilité de la ligne. Le chiffrage de niveau élevé de TCC's et le système de gestion principal automatisé protège l'information la plus sensible. Le stockage interne de 400 clefs couplées aux changements principaux automatiques fournit le degré de sécurité le plus complet.

La qualité supérieure de voix est réalisée par deux vocoders intégrés. Le CSD 3324E réduit réellement le bruit et le sifflement dans les lignes téléphoniques de qualité inférieure. Le chiffrage de fax est connecté à la ligne téléphonique à deux fils pour permettre le chiffrage de fax du groupe 3 indépendamment de quelle marque de fax est employée. Une voix et un appel de fax peuvent même être exploités sur la même ligne de raccordement.

Le **CSD 3600** est un dispositif de sécurité compact placé entre le téléphone de base et le combiné. Un seul bouton permet de protéger l'algorithme cryptographique et le chiffrement à clés publiques de haute qualité de *Bell Laboratories*. L'appel peut être décrypté par un dispositif récepteur TCC, un autre CSD 3600, un téléphone cellulaire de sécurité CSD 9300 ou un téléphone de direction de sécurité CSD 4100.

Gestion des Clés

Le CSD 3600 crée et distribue les clés à l'aide du chiffrement à clés publiques[221] négociées. Grâce à la technologie des clés publiques, le chargement manuel et la maintenance des clés n'étant pas nécessaires, la protection des communications est immédiate. Chaque fois que le bouton de sécurité est enfoncé, le CSD 3600 produit une nouvelle clé. Cette clé est unique aux deux CSD 3600 communicants, et ce, pour chaque session. Pour protéger encore plus la communication, des variables aléatoires dérivées de la clé unique sont affichées. En comparant les variables, l'émetteur et le récepteur peuvent détecter si la négociation de clés publiques est trafiquée ou espionnée.

Caractéristiques des Clés

Compatibilité téléphonique universelle. La possibilité d'enclencher les modules sélectionnés à l'arrière du CSD 3600 permet d'établir une compatibilité téléphonique universelle. Les opérateurs peuvent conserver le téléphone de leur choix et utiliser des lignes et commutateurs téléphoniques analogiques et numériques.

Qualité de transmission de la parole. La clarté de la voix durant l'appel chiffré permet d'identifier le locuteur. La supériorité de la transmission vocale provient d'un algorithme sophistiqué d'encodage de la parole mis au point spécialement pour le CSD 3600 par *Bell Laboratories*.

Le CSD 3600 est aussi compact qu'une calculatrice de poche et très léger. Pouvant être aisément transporté dans une serviette, il peut être utilisé à la maison comme en déplacement, même à l'étranger. Le CSD 3600 se branche au combiné du téléphone et non pas au réseau téléphonique. Il peut donc être utilisé aisément dans le monde entier, sans qu'il soit nécessaire de recevoir l'autorisation du réseau mondial.

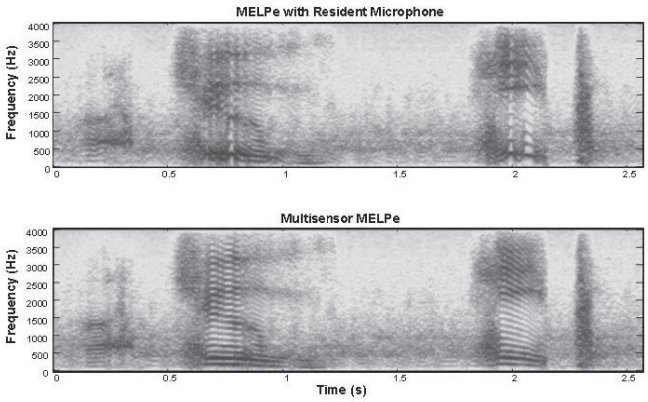
STANAG 4591

À l'heure actuelle (depuis 2002) les codeurs de voix utilisés pour les transmissions de l'OTAN sont des modèles de type « Stanag 4591». Le codage de la voix est fourni par des processeurs à virgule flottante très puissants (Texas Instruments TMS320c54xx, TMS320c55xx). Ils fonctionnent même dans un environnement de « bruits parasites » important, comme ceux que peuvent produire des véhicules militaires en opération.

Les codeurs utilisés sont nommés MELPe (Mixed Excitation Linear Production) le petit « e » en fin de sigle correspond à la dernière version de codeur avec des améliorations importantes des performances

[221] Nous détaillerons le fonctionnement du chiffrement à clé publique/clé privée dans la chapitre traitant de la sécurité des communications.

en milieux bruyants. En 2005, la société française Thalès a développé le dernier MELPe actuellement (en 2007) en cours dévaluation. Les recherches portent notamment sur l'amélioration de l'analyse des spectres sonores et leur numérisation sur des vocables aux consonances proches. Les tests ont été effectués sur plus de 200 heures de paroles par des locuteurs différents, dans 3 laboratoires d'essais dans le monde. Tests supervisés par la NSA et la DARPA (Defense Advanced Research Projects Agency) pour le compte de l'OTAN.



L'illustration ci-dessus montre les spectrogrammes illustrant l'amélioration des formes d'ondes obtenue dans un environnement hautement bruyant. On voit sur le spectrogramme du bas une nette amélioration de la structure harmonique due à l'utilisation d'un Multisensor MELPe.

Snapcell-300 est une percée technologique. Il est actuellement employé par des militaires, des sociétés et des individus dans plus de 30 pays. Le Snapcell-300 pèse seulement 11 grammes et est assez petit pour s'adapter à l'intérieur d'une poche de chemise. Le Snapcell-300 empêche efficacement les écoutes clandestines en utilisant une combinaison des mesures de sécurité multicouche avancées, de l'architecture (PKI) principale publique et du chiffrage d'AES approuvé par le *National Institute of Standards and Technology* des États-Unis (NIST) avec l'approbation du niveau FIPS-140-2.

La plupart des communications sans fil subissent des menaces de sécurité comprenant des attaques dites « homme du milieu »[222] (MITM), des modules de balayage de pointe de fréquence (scanners), le manque d'authenticité entre le combiné et la station de base, et le manque de chiffrage par les réseaux publics fixes qui conduisent la plupart des appels. Une des meilleures manières de protéger l'information sensible contre des oreilles indiscrètes est l'utilisation des dispositifs de haute qualité de chiffrage.

SNAPcell™ fournit la sécurité aux utilisateurs de téléphones mobiles qui craignent de voir compromise leur intimité, leurs secrets commerciaux ou de propriété intellectuelle. À la différence d'autres solutions existantes de GM/M qui exigent d'acheter un combiné cellulaire de sécurité cher, SNAPcell™ est un ultra-petit accessoire compatible avec plus de 25 combinés populaires de *Sony-Ericsson* GM/M. Il se connecte juste dans le combiné et procure la sécurité de la communication au niveau « militaire » tout en

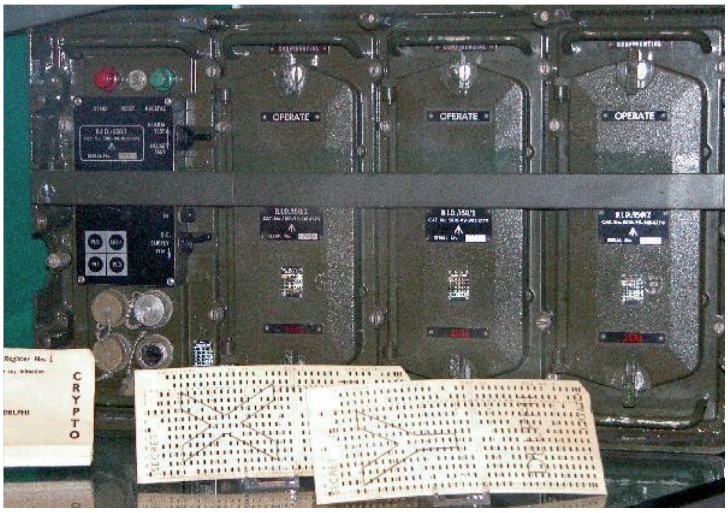
[222] L'attaque de l'homme du milieu (HDM) ou *man in the middle attack* (MITM) en cryptographie, est une attaque dans laquelle l'attaquant est capable de lire, insérer et modifier comme il le souhaite les messages chiffrés entre deux parties, sans que ni l'un ni l'autre ne puisse se douter que la ligne entre eux a été compromise.

assurant une l'excellente qualité de voix ! Les procédures de chiffrage sont complètement transparentes et aucune manipulation particulière n'est exigée pour commencer à employer le degré de sécurité puissant du téléphone mobile ainsi équipé.

Communications radio cryptées

En matière de communication radio cryptée, on peut citer divers matériels utilisés depuis les années soixante.

BID/150



Le système BID/150 a été utilisé pour la première fois en opération par le 15e *Signal Regiment* lors de la crise d'Aden. Les clés de codage étaient fournies sur cartes perforées IBM notées X-Y-Z et introduites à l'arrière de l'appareil. Les cartes n'étaient utilisées que 24 heures et détruites ensuite.

À la fin des années 1960, il a été largement utilisé à partir du niveau bataillon jusqu'au quartier général. Le modèle présenté ici a été utilisé à partir du milieu des années 1960 jusqu'au début des années 1980 (UK Royal Signals Museum de Blandford Forum, Royaume-Uni).

La boîte de DM est l'interface entre le BID/150 et de la radio - C42 ou C45. Elle permet à l'opérateur de sélectionner le mode de travail clair ou sécurisé.

Le mode clair signifie en fonctionnement normal d'un radio VHS analogique

En mode sécurisé le signal analogique est numérisé, puis crypté par combinaison avec la touche numérique générée par le BID/150 ; Le flux numérique est ensuite transmis à l'émetteur de type C42/C45 modifié pour permettre la FM. À la réception le processus est inversé.

Le ***BID 610*** ou ***ALVIS***, est une machine à crypter la voix anglaise introduite dans les années soixante et utilisée par l'armée britannique et également par le ministère canadien des affaires étrangères.

Ce fut la première machine entièrement transistorisée produite par les Anglais. Le niveau de cryptage de la voix permettait son utilisation pour les transmissions « Top secret ».

Photo ci-contre : Un système BID 160 en opération dans un véhicule d'un bataillon danois de communications. Les capots enferment les racks électroniques empêchant les fuites de rayonnements électromagnétiques.

Pour utiliser cet appareil à coder, il fallait paramétrer la clé du jour par un système de fiches et câbles disposés à l'arrière de l'appareil ce qui était fort peu pratique. Par la suite, il fut mis au point des sortes de « clés numériques » sous la forme d'un circuit à enficher dans un

connecteur prévu à cet effet. Ces cartes contenaient en mémoire les réglages pour plusieurs jours.

Il y eut plusieurs matériels fabriqués et utilisés sous le nom générique de BID, Le dernier en date fut le BID 1000 utilisé au Danemark ainsi que dans les services de l'ONU en Belgique entre 1998 et 2000.

Façade d'un module BID 1000

Depuis, on utilise pour crypter les communications radio les systèmes connus sous le nom générique de « *Fascinator* » produits principalement par la firme Motorola.

Fascinator

La série des modules FASCINATOR crypteurs de voix est une ligne des dispositifs cryptographiques qui peuvent être installés dans les systèmes radio numériques existants de *Motorola* et d'autres radios compatibles.

L'installation appropriée de FASCINATOR permet à une radio d'être employée pour les transmissions vocales classifiées. La conception prévoit des transmissions de voix cryptées, tout en maintenant les possibilités de transmissions normales. FASCINATOR se présente sous la forme de huit modules embrochables produisant un cryptage du type DES[223]. Les dispositifs de FASCINATOR sont semi-duplex, 12 dispositifs périodiques de chiffrage fonctionnent en mode synchrone. L'installation de ce dispositif dans les radios compatibles de *Motorola* exigera l'utilisation d'une boîte d'interface de sécurité et un KOI-18 ou un KYK-13 (Le dispositif électronique du transfert KYK-13 est un dispositif conçu par la NSA pour le transfert et le chargement des clefs cryptographiques avec leur mot de contrôle correspondant). Une fois utilisé avec des clefs convenablement classifiées, le système est approuvé pour la transmission de toutes les classifications et catégories de voix.

KYK-13

La clef pour l'équipement de FASCINATOR est fournie sous la forme d'une bande perforée et est normalement empaquetée dans cinq segments, trois copies de chacun, dans les boîtes en plastique.

Crypto période

La crypto période pour l'équipement de FASCINATOR est de 7 jours. Chaque autorité de contrôle de COMSEC[224] établit un temps standard et un jour de la semaine pour la mise en service. L'autorité de contrôle peut autoriser des prolongements de période de secours d'une semaine additionnelle pour des

[223] Le Data Encryption Standard (DES) est une méthode de chiffrement utilisant des clés de 56 bits.

[224] Organisation de contrôle de la sécurité des communications (organismes privés la plupart du temps).

communications mobiles dues aux considérations opérationnelles ou logistiques. Les prolongements de Cryptoperiod au-dessus de 7 jours ou prolongements de secours peuvent être approuvés sur une base de cas par cas par le CMC.

La production ou l'utilisation du matériel de base localement produit pour l'usage individuel avec le FASCINATOR est strictement interdite.

Le module Motorola FASCINATOR est approuvé et approuvé pour l'usage avec le MCX-100, le NX 300, le répéteur portatif, le SABER, les SPECTRA, le SYNTOR X-9000, le SYNTO X-9000 E, l'unité d'interface de console, et les SPECTRA SVMS mobiles.

Radios Saber I-II-III

Radio Spectra

Radio Synto X-9000

Le **DSP 9000** est une famille des systèmes de chiffrage militaires qui fournissent la sécurité à long terme et stratégique pour les canaux à bande étroite finis transmis par communications.

Une interface programmable et la conception de MIL-SPEC rendent le DSP 9000 capable de fixer pratiquement n'importe quelle application à haute fréquence, de VHF ou de fréquence ultra-haute.

Le DSP 9000 utilise la principale technologie de bord dans toute sa conception. Un processeur puissant de signal numérique assure la puissance de calcul énorme qui est employée pour assurer la qualité récupérée exceptionnelle de voix et la sécurité cryptographique. Tous les paramètres audio d'entrée-sortie sont commandés à l'aide d'un logiciel. Ceci permet à un DSP simple 9000 d'être rapidement installé sur une variété de radios sans modifier le matériel.

Les dispositifs exclusifs tels que de demi et pleines versions duplex, choix automatique de chiffrage de voice/data et stockage d'un grand nombre de clefs séparent également clairement le DSP 9000 de ses concurrents. En plus, le DSP 9000 est compatible avec les téléphones sécurisés CSD 3324SE pour permettre la communication de « bureau-à-champ ».

SE-240 – radio pour l'armée suisse

La SE-240 (TRC-3700) garantit la technologie la plus moderne et est compatible à 100% (MELCHIOR)[225] avec les standards (STANAG) de l'OTAN. L'appareil fortement informatisé couvre entre autres un codage linguistique très bon, la plus moderne des transmissions de données high speed ainsi

[225] Moyen d'Elongation pour les Communications HF Interarmées et OTAN en Réseau

qu'une gestion des liaisons et une procédure de saut de fréquence automatique. Outre les caractéristiques de rayonnement habituelles, les systèmes d'antenne garantissent aussi un rayonnement vertical pour « valley-to-valley ».

Le système est complètement compatible avec le système radio VHF PR4G voire la SE-235/435 déjà introduits et permet une interconnexion directe.

Caractéristiques du système

La radio permet un montage et une exploitation automatique et libre de parasites. Il est fait face à la menace « Electronic Warfare » par tout un système.

Le Système 3000 de Thalès consiste en :

1. cryptage des données
2. cryptage de la voix
3. semi-duplex
4. procédé de saut de fréquence intelligent
5. gestion des liens automatique

La gestion des liens automatique permet une prise de liaison automatique avec un rapport signal/bruit optimal. Lors de liaisons point à point, la liaison est maintenue automatiquement.

La gestion inclut cinq fonctions :

1. sélection automatique de la fréquence de travail (AFS)
2. prise de liaison automatique (ALE)
3. régulation de la puissance automatique (APC)
4. gestion des cadences de données automatique (ARM)
5. changement de fréquence automatique (AFC)

Cryptage et nouvelles technologies

Introduction

Les nouvelles technologies, et en particulier l'informatique et le réseau Internet, ont provoqué le développement universel de nouveaux moyens de communication.

Le téléphone, les messages écrits, les images, les transactions financières, tout peut transiter maintenant sur le réseau mondial. L'avantage décisif du moindre coût et de la rapidité est malheureusement contrebalancé par la perte totale de confidentialité des informations, le réseau étant « ouvert », puisqu'accessible à tous.

Il a donc été mis en place des procédures et des procédés de chiffrage afin de protéger au mieux le secret des communications.

La sécurité informatique est un très vaste domaine qui va de la protection des ordinateurs militaires jusqu'aux téléphones portables. La plupart des installations utilisant de l'électronique digitale sont concernées par ce problème, surtout si elles communiquent avec des ordinateurs ou des réseaux externes. La Défense (militaires, ambassades), les banques (transactions électroniques), les entreprises (secrets commerciaux), mais aussi la RATP (faux billets), emploient des spécialistes de la sécurité informatique. De l'avis des spécialistes, le plus gros problème actuellement est dû à l'ignorance par les responsables des dangers encourus et des moyens de protection. Il y a donc un marché de l'emploi énorme pour des agents de sécurité informatique, et leur formation doit inclure la cryptologie.

La cryptologie est seulement, comme nous l'avons dit, un des outils de protection contre les agressions et interceptions indésirables, mais cet outil est essentiel. Il est estimé suffisamment robuste par les spécialistes, du moins tant que les agressions sont faites avec des outils de cryptanalyse connus. Ceci n'est plus vrai lorsque l'agresseur a accès à des paramètres physiques du système (champs électromagnétique ou thermique, informations sur les composants électroniques utilisés). Casser une clef par des méthodes mathématiques est certes possible si l'on dispose de très gros moyens de calcul, mais les temps de calcul sont aussi fortement diminués si l'on dispose d'informations annexes.

Rappelons par ailleurs que de nombreux problèmes relevant de la cryptologie sont loin d'être parfaitement résolus. Un de ces problèmes est de mettre au point une signature pour authentifier de façon discrète les documents (les documents graphiques par exemple) ; une des méthodes utilisées consiste à mettre cette « signature » en filigrane dans une image. Un autre problème est celui de la confiance, c'est-à-dire de savoir si une information a bien été postée par celui qui s'en revendique l'auteur.

Nous verrons dans les pages qui suivent que le problème récurrent de la transmission des « clés de chiffrage » a été résolu, mais également que les capacités croissantes de calcul des ordinateurs a provoqué l'encadrement du cryptage afin de s'adapter aux besoins de sécurité des nations.

Nous allons donc dans ce chapitre étudier l'évolution et le fonctionnement des techniques de cryptages numériques.

Les aventures d'Alice et Bob

Les personnages **Alice** et **Bob** sont des figures classiques en cryptologie. Ces noms sont utilisés au lieu de « personne A » et « personne B » ; Alice et Bob cherchent dans la plupart des cas à communiquer de manière sécurisée.

D'autres prénoms sont utilisés pour décrire d'autres rôles, comme **Oscar** (l'adversaire, opponent en anglais) ou **Eve** (une « écouteuse » ou eavesdropper). Ces personnages font souvent partie des démonstrations d'attaques et d'explications sur les protocoles. Selon la langue, on peut trouver d'autres prénoms (Bernard ou Carole en français, par exemple).

Utilisateurs légitimes :

Alice et Bob (parfois Bernard en français). En général, Alice veut envoyer un message à Bob. Ces noms ont été inventés par Ron Rivest pour son article de 1978 dans le *Communications of the ACM* qui présentait le cryptosystème RSA. (Le rapport technique de 1977 sur RSA n'utilisait pas encore ces noms.).

Carol (ou Carole en français), est une troisième participante aux échanges. Puis, on a souvent **Dave**, un quatrième participant, et ainsi de suite, alphabétiquement.

Adversaires :

Eve, un écouteur externe (de l'anglais eavesdropper), est un attaquant passif. Tandis qu'elle peut écouter les échanges d'Alice et de Bob, elle ne peut pas les modifier.

Mallory, (ou Mallet, pour malicieux), est un attaquant actif. Au contraire d'Eve, Mallory peut modifier les messages, substituer les siens, remettre en jeu d'anciens messages, etc. Rendre un système sûr vis-à-vis de Mallory s'avère un problème plus difficile que pour Eve.

Oscar, un opposant, est habituellement défini comme équivalent à Mallory.

Trudy, une intruse, est plus dangereuse qu'Eve parce que celle-là peut modifier des messages en transit. Bob et Alice devraient idéalement être aptes à détecter de telles modifications, puis soit les ignorer, soit récupérer le message original. Sinon, Trudy peut causer beaucoup de dommages.

Tierces parties :

Isaac, un fournisseur d'accès à Internet («i» de l'anglais *Internet Service Provider*, ISP).

Ivan, un émetteur («i» de l'anglais issuer), pour la cryptographie financière, par exemple.

Justin, du système de justice, plus spécifiquement, un avocat.

Matilda, une marchande, pour la cryptographie financière ou le commerce électronique, par exemple.

Nestor, un tiers de confiance neutre, est une version francophone de Trent.

Plod, est un officier de police, de douanes ou de service de renseignements.

Trent, est un arbitre de confiance («tr» de l'anglais *trusted arbitrator*), est en quelque sorte un tiers parti neutre dont le rôle exact varie avec le protocole dont il est question.

Vanna, voir Peggy.

Victor, voir Peggy.

Walter, un gardien de prison (« w » de l'anglais *warden*), peut surveiller Alice et Bob d'une façon qui dépend du protocole en question.

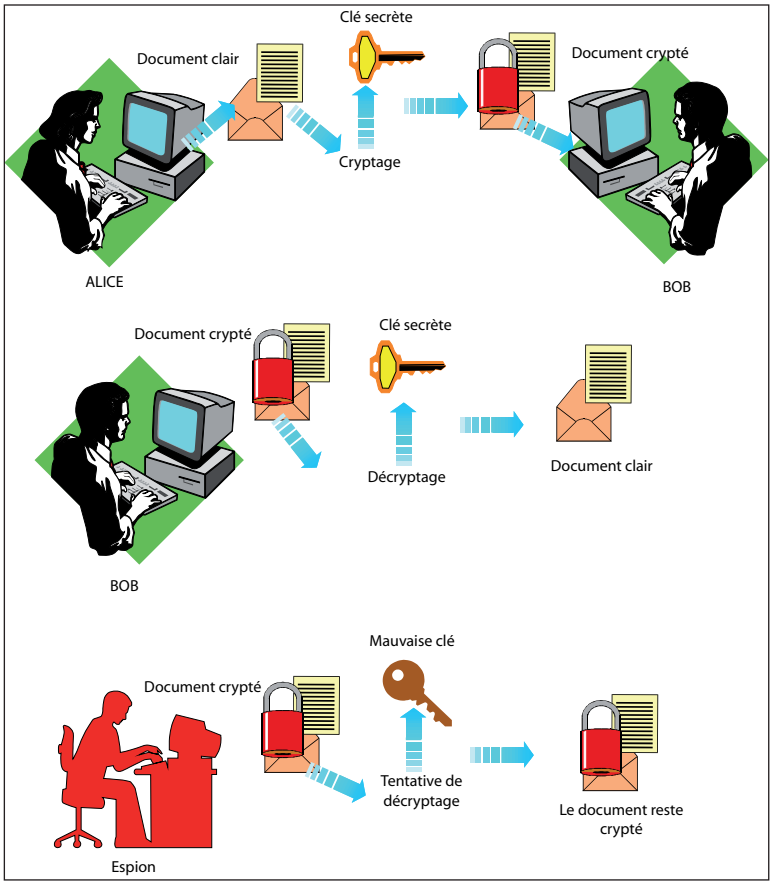
Preuve à divulgation nulle de connaissance[226] **:**

Peggy (ou Pat), un prouveur et Victor, un vérifieur, doivent interagir d'une façon donnée afin de prouver que la transaction voulue a bien eu lieu. On les retrouve souvent dans les preuves à divulgation nulle de connaissance (zero-knowledge). Une autre paire de noms pour ceci est Pat et Vanna (à cause des hôtes de l'émission de télévision américaine *Wheel of Fortune*).

Fonctions recherchées dans la cryptographie numérique :

1 – **la confidentialité** : assurer la confidentialité d'un message, c'est faire en sorte que seuls les destinataires pourront le lire. C'est donc le rendre inintelligible pour les autres.
2 – **l'intégrité** : l'intégrité des données, c'est la non-altération de celles-ci pendant la transmission que l'altération soit volontaire ou le fait du hasard.
3 – **l'authentification** : cette fonction consiste à assurer les correspondants d'un échange de l'identité de chacun d'entre eux. C'est en quelque sorte donner une carte d'identité à l'utilisateur.
4 – **la non-répudiation** : cela consiste à garantir qu'aucun des partenaires ne puisse nier la transaction effectuée.

Les deux types de chiffrement possibles : symétrique et asymétrique



Tout ce que nous avons vu dans les pages précédentes ressort du premier type de chiffrement : ***le chiffrement symétrique.*** Dans ce système, la même clé sert au cryptage et au décryptage. Il faut donc que cette clé soit connue des parties communicantes. Nous avons vu qu'il y a toujours des failles dans ce système et qu'il y a toujours possibilité de casser ce type de cryptage. De plus, la principale difficulté réside dans la transmission des clés, surtout sur Internet ! La communication numérique, dans un premier temps s'était donc pourvue d'outils de chiffrement adaptés basés sur le chiffrement numérique symétrique.

Figure ci-contre :
Principe général du chiffrement symétrique

[226] Une preuve à divulgation nulle de connaissance est un concept utilisé en cryptologie dans le cadre de l'authentification et de l'identification. Cette expression désigne un protocole sécurisé dans lequel une entité nommée « fournisseur de preuve », prouve mathématiquement à une autre entité, le « vérificateur », qu'une proposition est vraie sans toutefois révéler une autre information que la véracité de la proposition. En pratique, ce schéma se présente souvent sous la forme d'un protocole de type « stimulation/réponse » (*challenge-response*). Le vérificateur et le fournisseur de preuve s'échangent des informations et le vérificateur contrôle si la réponse finale est positive ou négative. Les anglophones utilisent l'abréviation ZKIP pour *Zero Knowledge Interactive proof.*

Les principaux outils de chiffrement symétrique

Kerberos

Kerberos est un protocole d'identification réseau créé au *Massachusetts Institute of Technology*[227] (MIT). Kerberos utilise un système de tickets au lieu de mots de passe en texte clair. Ce principe renforce la sécurité du système et empêche que des personnes non autorisées interceptent les mots de passe des utilisateurs.

Kerberos est disponible en *open source*[228] (téléchargeable depuis le site Internet du MIT). Cependant, certains éditeurs, dont Microsoft, proposent des versions commerciales (et donc payantes) de ce système. Ces logiciels respectent de manière générale les principes de fonctionnement du code source original qui est maintenu par le MIT. Kerberos a été conçu dans un esprit de simplicité. Lorsqu'il n'est pas incorporé dans un logiciel commercial, la plupart de ses commandes reprennent la syntaxe des commandes traditionnelles d'Unix[229].

L'ensemble repose sur des clés secrètes (chiffrement symétrique). À l'origine, il fut employé sur des systèmes distribués Unix (Linux). C'est avec Windows 2000 qu'il fit son retour.

Le nom de Kerberos vient du grec Κερβερος, « Cerbère ».

Dans un réseau simple utilisant Kerberos, on distingue plusieurs entités :

- le client (C), il a sa propre clé privée K_C
- le serveur (S), il dispose aussi d'une clé privée K_S
- le serveur de tickets (TGS pour *Ticket Granting Server*), il a une clé privée K_{TGS} et connaît la clé privée K_S du serveur
- le centre de distribution de clés (KDC pour *Key Distribution Center*), il connaît les clés privées K_C et K_{TGS}

Le client veut accéder à un service proposé par le serveur S.

La première étape pour le client consiste à s'identifier auprès du serveur de clés (KDC). Le client a une clé privée K_C, celle-ci est également connue par le serveur de clés. Le client envoie son nom au serveur de clés et lui indique le serveur de tickets qui l'intéresse. Après vérification sur l'identité du client (cette partie dépend des implémentations, certains serveurs utilisent des mots de passe à usage unique), le serveur de clés lui envoie alors un ticket T_{TGS}. Ce ticket autorise le client à faire des requêtes auprès du serveur de tickets TGS.

Ce ticket T_{TGS} est chiffré par le serveur de clés avec la clé du serveur de tickets (K_{TGS}). Il contient notamment des informations sur le client, mais également la clé utilisée pour établir la communication entre le client et le serveur de tickets. Cette clé de session, nous la noterons $K_{C,TGS}$. Le client reçoit également cette clé de session $K_{C,TGS}$, elle a toutefois été chiffrée avec la clé privée K_C du client.

À ce stade, le client possède un ticket T_{TGS} (qu'il ne peut pas déchiffrer) et une clé $K_{C,TGS}$.

---

[227] Le *Massachusetts Institute of Technology*, MIT, (en français : Institut de Technologie de Massachusetts) est une institution de recherche et une université américaine, spécialisée dans les domaines de la science et de la technologie. Située à Cambridge, dans le Massachusetts, à proximité immédiate de Boston, elle est considérée au XXIe siècle comme la meilleure université occidentale en sciences et en technologies.

[228] La désignation Open Source (source ouverte en français) s'applique aux logiciels dont la licence respecte des critères précisément établis par l'*Open Source Initiative*, c'est-à-dire la possibilité de libre redistribution, d'accès au code source, et de travaux dérivés. Par commodité de langage, on parle aussi de logiciels libres.

[229] UNIX™ est le nom d'un système d'exploitation multitâche et multiutilisateur créé en 1969, à usage principalement professionnel, conceptuellement ouvert et fondé sur une approche par laquelle il offre de nombreux petits outils chacun dotés d'une mission spécifique.

Il a donné naissance à une famille de systèmes, dont les plus populaires en 2007 sont *Linux* et *Mac OS X*.

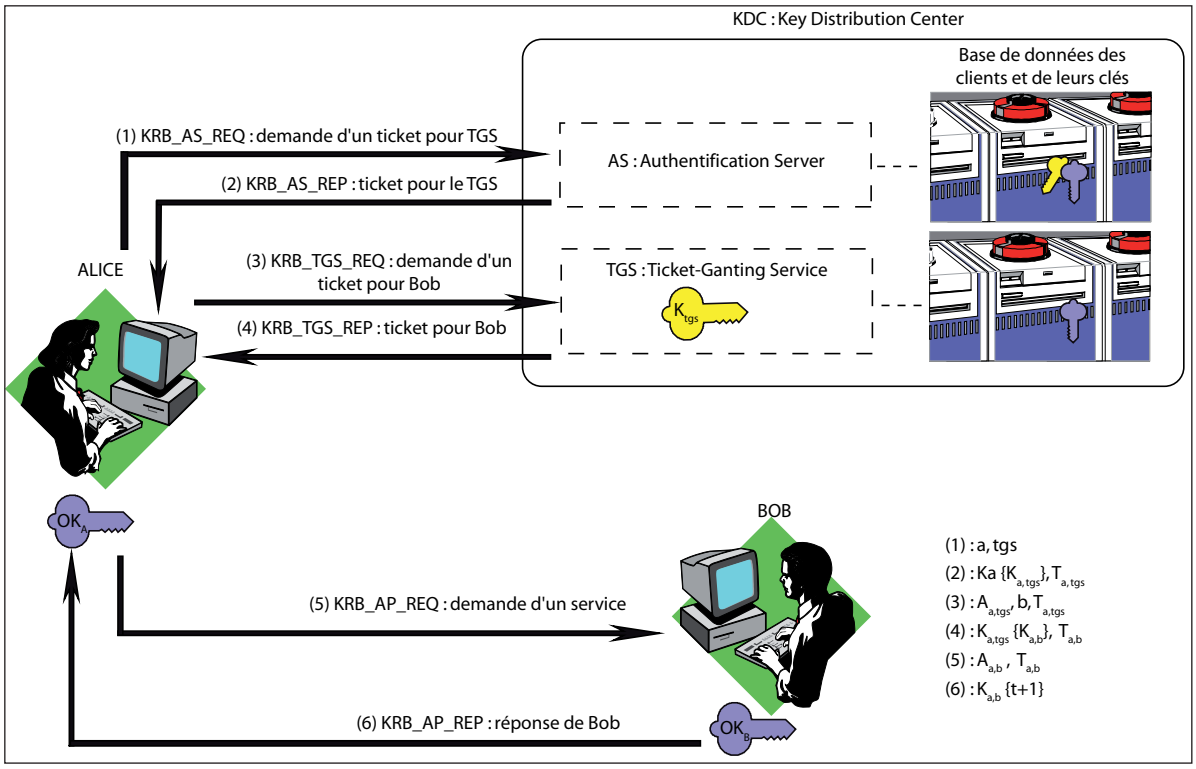
La deuxième étape est l'envoi par le client d'une demande de ticket auprès du serveur de tickets. Cette requête contient un identifiant (des informations sur le client ainsi que la date d'émission) chiffré avec la clé de session $K_{C,TGS}$ (qui est trouvée par le client en déchiffrant les informations reçues depuis le serveur de clés avec sa clé privée). Le client envoie aussi le ticket qui lui avait été transmis par le serveur de clés.

Le serveur de tickets reçoit alors son ticket et il peut le déchiffrer avec sa clé privée K_{TGS}. Il récupère le contenu du ticket (la clé de session) et peut ainsi déchiffrer l'identifiant que lui a envoyé le client et vérifier l'authenticité des requêtes. Le serveur de tickets peut alors émettre un ticket d'accès au serveur. Ce ticket est chiffré grâce à la clé privée du serveur K_S. Le serveur de tickets envoie aussi au client une autre clé de session $K_{C,S}$ pour les communications entre le serveur final et le client. Cette seconde clé de session a été chiffrée à l'aide de la clé $K_{C,TGS}$ connue à la fois par le serveur de tickets et le client.

La troisième étape est le dialogue entre le client et le serveur. Le client reçoit le ticket pour accéder au serveur ainsi que l'information chiffrée contenant la clé de session entre lui et le serveur. Il déchiffre cette dernière grâce à la clé $K_{C,TGS}$. Il génère un nouvel identifiant qu'il chiffre avec $K_{C,S}$ et qu'il envoie au serveur accompagné du ticket.

Le serveur vérifie que le ticket est valide (il le déchiffre avec sa clé privée K_S) et autorise l'accès au service si tout est correct.

Une fois qu'un client s'est identifié, celui-ci obtient un ticket (généralement, un fichier texte - mais son contenu peut aussi être stocké dans une zone de mémoire sécurisée). Le ticket joue le rôle d'une carte d'identité à péremption assez courte, huit heures généralement. Si nécessaire, celui-ci peut être annulé prématurément. Sous les systèmes Kerberos comme celui du MIT, ou de Heimdal, cette procédure est généralement appelée via la commande *kdestroy*.



La sécurité de Kerberos repose sur la sécurité des différentes machines qu'il utilise. Une attaque sur le serveur de clés serait dramatique, car elle pourrait permettre à l'attaquant de s'emparer des clés privées des clients et donc de se faire passer pour eux. Un autre problème qui pourrait survenir sur la machine du client est le vol des tickets. Ils pourraient être utilisés par une tierce personne pour accéder aux services offerts par les serveurs (si la clé entre le client et le serveur est connue).

L'expiration du ticket permet de limiter les problèmes liés au vol des tickets. De plus, les tickets contiennent l'adresse IP du client et le ticket n'est donc pas valable s'il est employé depuis une autre adresse. Pour contrer cela, l'attaquant devrait spoofer[230] l'IP du client. Une attaque sur les identifiants échouera, car Kerberos leur ajoute un élément. Cela évite les attaques par renvoi d'identifiants qui auraient été interceptés. Les serveurs conservent l'historique des communications précédentes et peuvent facilement détecter un envoi frauduleux.

L'avantage de Kerberos est de limiter le nombre d'identifiants et de pouvoir travailler sur un réseau non sécurisé. Les identifications sont uniquement nécessaires pour l'obtention de nouveaux tickets d'accès au serveur de tickets.

DES

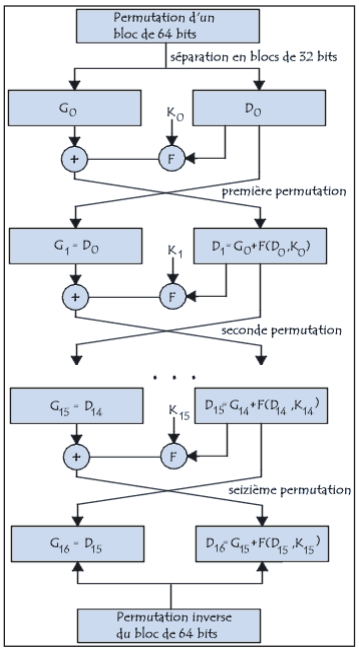
Le *Data Encryption Standard* (DES) est une méthode de chiffrement utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en *Triple DES*, ce qui ne fait rien pour améliorer ses performances. DES a notamment été utilisé dans le système de mots de passe Unix.

Historique

En mai 1973, le *National Bureau of Standards* américain demande la création d'un chiffrement utilisable par les entreprises. À cette époque, IBM dispose déjà d'un algorithme appelé *Lucifer*. Cet algorithme avait été conçu au début des années 1970 par Horst Feistel, selon ce qu'on appelle maintenant un schéma de Feistel[231]. Il fait donc partie de la catégorie des chiffrements à clef secrète, itératif par blocs.

En bonne logique, cet algorithme aurait dû être sélectionné par le NBS. En pratique, ce fut presque le cas : la NSA demanda à ce que Lucifer soit modifié, par ses soins. Ainsi fut créé le DES, qui fut adopté comme standard en novembre 1976.

Cela suscita bien entendu des rumeurs selon lesquelles la NSA aurait volontairement affaibli l'algorithme, dans le but de pouvoir le casser. Étrangement, le DES s'est révélé résistant à plusieurs attaques ne devant apparaître dans la communauté académique que beaucoup plus tard. Encore plus étonnant, *Lucifer*, lui, résistait moins bien.



Algorithme DES

Fonctionnement

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits, représentées par 64 bits (avec un bit de chaque octet servant pour le contrôle de parité). Ce

[230] L'usurpation d'adresse IP (en anglais : IP *spoofing*) est une technique de hacking (étude des failles et vulnérabilités d'un système) consistant à utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité. Elle permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on spoofe l'adresse IP. De manière plus précise, cette technique permet la création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre.

[231] Un réseau de Feistel est une construction utilisée dans les algorithmes de chiffrement par bloc, nommée d'après le cryptologue d'IBM, Horst Feistel. Elle a été utilisée pour la première fois dans *Lucifer* et *DES*. Cette structure offre plusieurs avantages, le chiffrement et le déchiffrement ont une architecture similaire voire identique dans certains cas. L'implémentation matérielle est aussi plus facile avec un tel système même si les choses ont passablement changé depuis la fin des années 1970. Un réseau de Feistel repose sur des principes simples dont des permutations, des substitutions, des échanges de blocs de données et une fonction prenant en entrée une clé intermédiaire à chaque étage. Il est vraisemblable que Feistel ne soit pas le seul inventeur de cette architecture. Durant une conférence, Don Coppersmith a laissé entendre que Bill Notz et Lynn Smith (de l'équipe d'IBM travaillant sur DES) avaient été en grande partie à l'origine du réseau de Feistel tel que nous le connaissons.

système de chiffrement symétrique fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel.

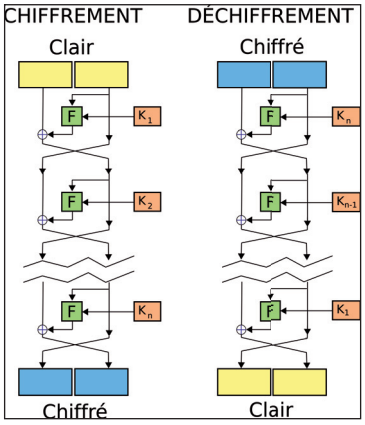


Schéma de Feistel

D'une manière générale, on peut dire que DES fonctionne en trois étapes :

- permutation initiale et fixe d'un bloc (sans aucune incidence sur le niveau de sécurité).
- le résultat est soumis à 16 itérations d'une transformation, ces itérations[232] dépendent à chaque ronde d'une autre clé partielle de 48 bits. Cette clé de ronde intermédiaire est calculée à partir de la clé initiale de l'utilisateur (grâce à un réseau de tables de substitution et d'opérateurs XOR)[233]. Lors de chaque ronde, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel. Le bloc de 32 bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 63) subira une transformation.
- le dernier résultat de la dernière ronde est transformé par la fonction inverse de la permutation initiale.

DES utilise huit tables de substitution (les S-Boxes) qui furent l'objet de nombreuses controverses quant à leur contenu.

S_5		4 bits au centre de l'entrée															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1100**	**1011**	**1100**	**1101**	**1110**	**1111**
Bits externes	**00**	0010	1100	0100	0001	0111	1100	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1100	0011	1001	1000	0110
	10	0100	0010	0001	1011	1100	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1100	0100	0101	0011

Ci-dessus une S-Box (S5) tirée de l'algorithme DES. La sortie de 4 bits est obtenue à partir de l'entrée de 6 bits. On divise ces 6 bits en deux parties : les deux bits aux extrémités et les quatre bits restants (au centre). Les deux bits indiquent la ligne et les bits centraux donnent la colonne correspondante. Par exemple, avec une entrée « 011011 », on divise en « 0 1101 1 ». Ce qui donne pour la ligne « 01 » et pour la colonne « 1101 ». La sortie de la table est alors « 1001 ».

On soupçonnait une faiblesse volontairement insérée par les concepteurs. Ces rumeurs furent dispersées au début des années 90 par la découverte de la cryptanalyse différentielle qui démontra que les tables étaient bien conçues.

Les attaques sur DES

Plusieurs attaques ont été découvertes sur DES. Elles permettent de diminuer les coûts d'une recherche exhaustive des clés qui se monte à 255 opérations en moyenne. À noter que certaines de ces méthodes ne sont plus efficaces avec des algorithmes de cryptage plus récents du fait de l'introduction d'un effet avalanche.

[232] En mathématiques, une itération désigne l'action de répéter un processus.

[233] La fonction OU exclusif, souvent appelée XOR (eXclusive OR), est un opérateur logique de l'algèbre de Boole. À deux événements, qui peuvent avoir chacun la valeur VRAI ou FAUX, il associe un résultat qui a lui-même la valeur VRAI ou FAUX. Cet opérateur est très utilisé en électronique, en informatique, et aussi en cryptographie du fait de ses propriétés intéressantes. Son symbole est traditionnellement un signe plus dans un cercle : ⊕.

• La ***cryptanalyse différentielle*** découverte par Eli Biham et Adi Shamir en 1991 permet de trouver la clé en utilisant 2^{47} textes clairs. Le principe est de disposer d'un DES implémenté dans une boîte noire hermétique avec une clé secrète à l'intérieur. En fournissant suffisamment de texte en entrée, on peut statistiquement analyser le comportement des sorties selon les entrées et retrouver la clé. Les entrées utilisées pour cette attaque doivent mutuellement présenter une légère différence (par exemple un bit qui change). En regardant comment la différence affecte la sortie, on peut établir des statistiques et en augmentant le nombre d'entrées, on améliore la fiabilité de l'attaque.

• L'***attaque-T*** (Tickling attack) est une variante de la cryptanalyse différentielle. Elle a été découverte lors de la conception du DES par les chercheurs d'IBM et révélée par Don Coppersmith au milieu des années 90. Pendant une vingtaine d'années, le silence a été complet sur cette découverte. À l'époque, elle avait incité les concepteurs de DES à renforcer le contenu des tables de substitution (au lieu de l'affaiblir comme la rumeur le laissait entendre).

• La ***cryptanalyse linéaire*** inventée par Mitsuru Matsui en 1993 est plus efficace, mais moins pratique pour la simple et bonne raison que l'attaquant ne dispose pas de la boîte noire et qu'il ne peut pas soumettre ses propres textes. Cette attaque nécessite 2^{43} couples (tous chiffrés avec la même clé) que l'attaquant a pu récupérer par un moyen ou un autre. Elle consiste à faire une approximation linéaire de DES en le simplifiant. En augmentant le nombre de couples disponibles, on améliore la précision de l'approximation et on peut en extraire la clé.

• Le ***compromis temps-mémoire*** est un concept inventé par Martin Hellman au début des années 80. En partant du principe que le même message va être chiffré plusieurs fois avec des clés différentes, on pourrait calculer une immense table qui contient toutes les versions chiffrées de ce message. Lorsque l'on intercepte un message chiffré, on peut le retrouver dans la table et obtenir la clé qui avait été utilisée pour le coder. Cette attaque n'est bien sûr pas faisable, car nous avons besoin d'une table de l'ordre du milliard de GB. Le génie d'Hellman a été de trouver un moyen pour réduire cette table à environ 1 téraoctet (soit 1 million de fois moins que la table complète), ce qui est faisable de nos jours.

• D'autres attaques sont spécifiques à des implémentations et ne sont pas forcément spécifiques à DES. Dans le cas d'un DES implémenté dans du matériel, on pourrait analyser la consommation électrique et déduire certaines informations sur la clé (une consommation accrue indique des bits actifs). Le même style d'attaque peut aussi être employé sur un ordinateur en calculant le temps mis pour chiffrer avec des textes différents ou en analysant la mémoire utilisée.

• Toutes les autres attaques sur DES visent à réduire le temps de calcul d'une recherche exhaustive en utilisant des machines spécifiquement conçues pour la tâche (grâce à des FPGA[234] en parallèle par exemple)

Une telle machine a été construite en 1998. *Deep Crack*[235] a coûté environ 200 000 dollars et pouvait casser la clé en moins d'une semaine.

Le calcul distribué en utilisant les ordinateurs des particuliers (projet distributed.net) a prouvé son efficacité en cassant une clé en moins de 24 heures. (voir encadré page 566)

circuit FPGA

[234] FPGA (*field-programmable gate array*), réseau de portes programmables in-situ. Un circuit logique programmable, ou réseau logique programmable, est un circuit intégré logique qui peut être reprogrammé après sa fabrication. Il est composé de nombreuses cellules logiques élémentaires librement assemblables.

[235] Deep Crack a été conçu par *Cryptography Research, Inc., Advanced Wireless Technologies* et l'*EFF*. Le principal concepteur a été Paul Kocher, le président de *Cryptography Research. Advanced Wireless Technologies* a construit 1 856 puces spécialisées pour le DES, contenues sur 29 cartes électroniques de 64 puces. Les cartes étaient ensuite insérées dans six boîtiers d'ordinateurs. La recherche était coordonnée par un PC qui assignait une certaine plage de clés à chaque puce. La machine était ainsi capable de tester plus de 90 milliards de clés par seconde, et met environ cinq jours pour tester toutes les clés possibles.

AES

Le standard de chiffrement avancé (*Advanced Encryption Standard* ou *AES*) est un algorithme de chiffrement symétrique, choisi en octobre 2000 par le NIST pour être le nouveau standard de chiffrement pour les organisations gouvernementales des États-Unis.

Histoire

Il est issu d'un appel à candidatures international lancé en janvier 1997 et ayant reçu 15 propositions. Parmi ces 15 algorithmes, 5 furent choisis pour une évaluation plus poussée en avril 1999 : MARS, RC6, Rijndael, Serpent, et Twofish. Au bout de cette évaluation, ce fut finalement le candidat Rijndael, du nom de ses deux concepteurs Joan Daemen et Vincent Rijmen (tous les deux de nationalité belge) qui a été choisi. Ces deux experts en cryptographie étaient déjà les auteurs d'un autre algorithme : Square.

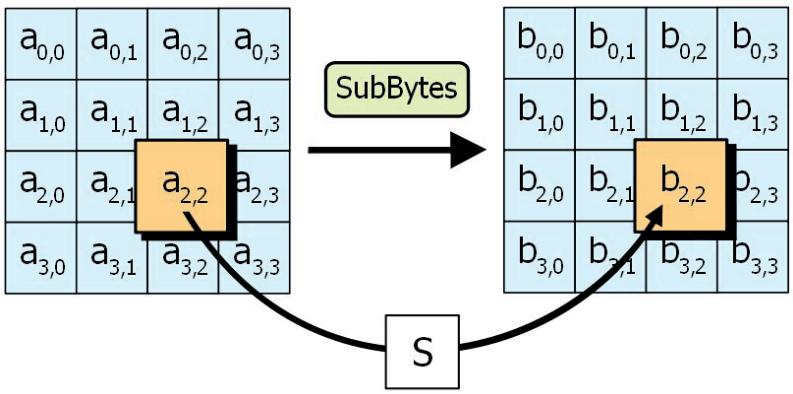
AES est un sous-ensemble de Rijndael : il ne travaille qu'avec des blocs de 128 bits alors que Rijndael offre des tailles de blocs et de clefs qui sont des multiples de 32 (compris entre 128 et 256 bits).

Ce faisant, l'AES remplace le DES (choisi comme standard dans les années 1970) qui de nos jours devenait obsolète, car il utilisait des clefs de 56 bits seulement. L'AES a été adopté par le NIST (*National Institute of Standards and Technology*) en 2001. De plus, son utilisation est très pratique, car il consomme peu de mémoire et n'étant pas basé sur un schéma de Feistel, sa complexité est moindre et il est plus facile à implémenter.

Fonctionnement

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(2^8) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

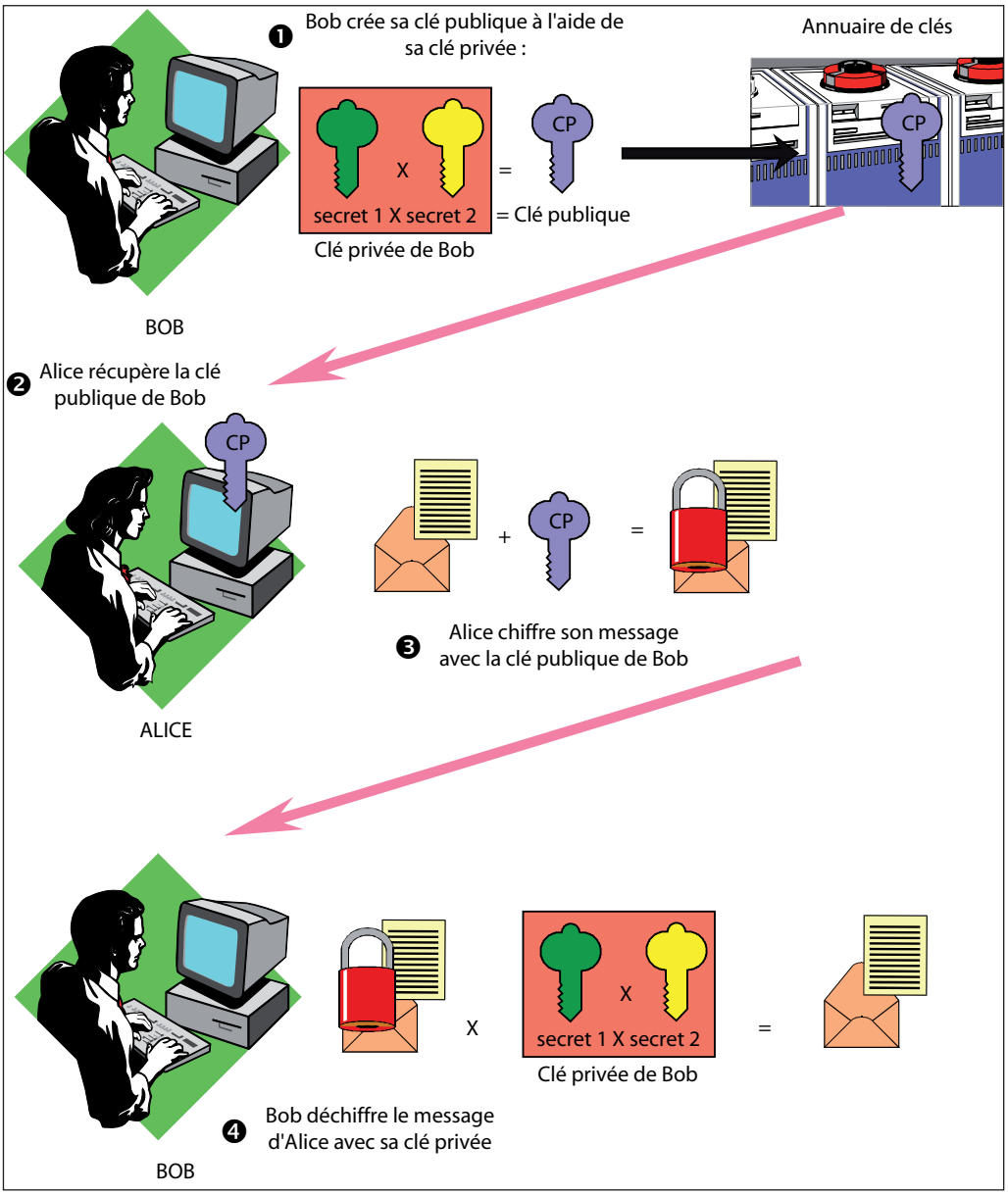
Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.



Principe de base de AES

Le cryptage asymétrique, invention de la clé publique

Cette technique ne repose plus sur le partage d'une même clé secrète, mais sur la possession d'une ***clé privée*** par l'utilisateur et d'une clé associée, dite ***clé publique***, mise à disposition de la communauté. Chaque personne possède sa propre paire de clés. La première reste secrète, alors que la seconde est disponible pour tout le monde.



Lorsque Bob désire envoyer un message à Alice, il utilise la clé publique de cette dernière pour chiffrer le message. Alice utilisera sa clé privée pour le déchiffrer. L'avantage de ce processus est qu'il n'est pas réversible : la clé utilisée pour chiffrer le message ne peut être utilisée pour le déchiffrer.

On doit l'invention de ce système à deux universitaires de l'Université de Stanford, Whitlfield Diffie et Martin Hellman qui firent paraître un article titré : « *De nouvelles voies pour la cryptographie* » en 1976.

Comme souvent dans l'histoire de la cryptographie, les vrais découvreurs ne sont pas toujours ceux que l'on pense. En effet, l'histoire a retenu les noms de Merkle, Hellman et Diffie car ils ont été les premiers à publier leur invention. En fait, on a appris plus tard que les trois premiers inventeurs de l'idée du système à clef publique était James Ellis, Clifford Cocks et Malcom Williamson, qui travaillaient au *Government Communications Headquarters* (GCHQ) de Cheltenham, établissement anglais top secret fondé sur les ruines de Bletchley Park après la Seconde Guerre mondiale.

Merkle, Hellman et Diffie

James Ellis

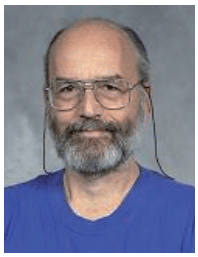
Clifford Cocks

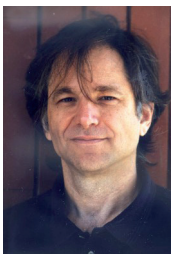
Malcom Williamson

Ellis posa les bases dès 1969. Puis, en 1973, Cocks eut une idée de ce qui serait plus tard connu sous le nom de chiffre asymétrique **RSA**. Il ne put mettre en œuvre son idée, car les ordinateurs de l'époque n'étaient pas encore assez puissants. En 1974, Cocks expose son idée à Williamson. Ce dernier, qui pense que cela est trop beau pour être vrai, reprend tout à zéro pour trouver une faille. Au lieu de cela, il trouve le système d'échange de clef de Diffie-Hellman-Merkle, à peu près en même temps que Martin Hellman. En 1975, Ellis, Cocks et Williamson avaient donc découvert tous les aspects fondamentaux de la cryptographie à clef publique, mais les trois Anglais se turent. Secret militaire oblige.

RSA

RSA, du nom de ses inventeurs : Ron Rivest, Adi Shamir et Léonard Adleman.





Le secret de la clé tient à la difficulté de factoriser un nombre premier très grand.

Le protocole de cryptographie RSA :

D'abord, le destinataire du message va préparer 2 clés :

- une clé publique (qui sera divulgué librement)
- une clé privée (qui sera conservé précieusement)

Ensuite, l'émetteur va préparer son message puis le crypter grâce à la clé publique du destinataire. Il peut alors lui envoyer le message.

Enfin, le récepteur de ce message va pouvoir le déchiffrer à l'aide de sa clé privée, qu'il est le seul à détenir.

Voici le plan des différentes étapes à suivre :

Rappel de quelques notions d'arithmétique :
Un nombre est *premier* s'il admet que 1 et lui-même comme diviseurs entiers positifs.
L'opération *modulo*, consiste à donner le reste de la division euclidienne d'un entier par un autre. Autrement dit :
r = mod(a;b) signifie que r est le reste de la division euclidienne de a par b.
Avec un exemple : mod(27;5) = 2 car 5 * 5 + 2 = 27.
Rappel informatique :
Les caractères saisis au clavier d'un ordinateur sont transformés en *code binaire*.
L'ASCII définit 128 caractères numérotés de 0 à 127 et codés en binaire de 0000000 à 1111111. Sept bits suffisent donc pour représenter un caractère codé en ASCII. Toutefois, les ordinateurs travaillant presque tous sur huit bits (un octet) depuis les années 1970, chaque caractère d'un texte en ASCII est stocké dans un octet dont le 8e bit est 0.
Les caractères de 0 à 31 ainsi que le 127 ne sont pas affichables et correspondent à des directives de terminal. Le caractère 32 est l'espace blanc. Les autres correspondent aux chiffres arabes, aux lettres latines majuscules et minuscules et à quelques symboles de ponctuation.

I) Préparations des clés :

a) Clé publique

1. Trouver deux nombres premiers p et q distincts (p et q doivent restés confidentiels)
2. Calculer n = p × q
3. Calculer f = (p-1)×(q-1)
4. Choisir un nombre e quelconque premier avec f (le PGCD de e avec f doit être égal à 1)

> Notre clé publique est (n; e)

b) Clé privée

1. Trouver d tel que e × d 1 (mod f(n))
2. La relation précédente peut aussi s'écrire : e × d = f(n) × k + 1
3. Les conditions suivantes doivent alors êtres respectées : 1 ≤ d < f(n) et k est un nombre entier.

> Notre clé privée est (p; q; d)

II) Préparations du message :

a) Numérisation

1. Transcrire le message d'un langage alphanumérique en un langage numérique (remplacement des lettres, symboles et caractères en langage décimal).
2. Pour cela, il est possible d'utiliser le code ASCII.

b) Découpage

1. Il faut à présent découper le message numérique en tranche t, comportant un chiffre de moins que le nombre de chiffres de n.

III) Cryptage :

L'émetteur crypte le message pour l'envoyer au destinataire.

1. Il chiffre chacune des tranches t en tranche t' grâce à la relation : te t'(mod n). Cette étape équivaut à verrouiller le cadenas du « coffre » contenant le message.
2. Il envoie ensuite le message crypté contenant les différentes tranches t'.

IV) Décryptage :

Le destinataire reçoit le message crypté et le déchiffre.

1. Il déchiffre chacune des tranches t' en tranche t grâce à la relation : t' d t(mod n). Cette étape équivaut à déverrouiller le cadenas avec la clé privée.

2. Il retrouve alors les tranches t d'origines.
3. À présent, il ne reste plus qu'à rassembler les tranches t puis à les retranscrire en langage d'origine.
4. Le message à bien été transmis et reçu d'une façon confidentielle !

Exemple :

I) Préparations des clés :

Alice veut envoyer le message « SALUT » à Bob, sans que personne ne le sache. Bob doit au préalable construire ses clés publique et privée :

a) Clé publique

1. Il choisit p = 23, q = 41.
2. Ainsi, n = p × q = 23 × 41 = 943, Donc n = 943.
3. (p-1) × (q-1) = 22 × 40 = 880, Donc f = 880.
4. Plusieurs valeurs sont possibles pour e. Disons qu'il choisi e = 19 (le PGCD de e et f doit être égale à 1).

> La clé publique de Bob est (n; e), donc égale à (943; 19)

b) Clé privée

1. Par un calcul, il trouve que d = 139, puisque 19 × 139 1(mod 880).
2. > Pour déterminer d, Bob utilise l'algorithme d'Euclide étendu[236].
3. Par une seconde relation, on a : 19 × d = 880 × k + 1 19 × d = 880 × 3 + 1 19 × d = 2641 d = 2641 / 19 = 139
4. > Pour déterminer le nombre k, Bob entre la fonction (880x + 1) / 19 sur le tableur de sa calculatrice, et regarde pour quelle valeur de x, le résultat est un entier. C'est alors la valeur de k.

> La clé privée de Bob est (p; q; d), donc égal à (23; 41; 139)

II) Préparations du message :

a) Numérisation

1. Elle convertit le message en nombres, en utilisant le code ASCII de façon à transcrire numériquement le message..
2. Le message « SALUT » devient alors 008365768584 en langage décimal.

b) Découpage

1. A présent, elle découpe le message numérique en tranche t, d'un chiffre de moins que le nombre de chiffres de n. n = 943, il y a 3 chiffres, donc chaque tranche t comportera 3 - 1 = 2 chiffres. Ainsi, on a : 83 65 76 85 84.

III) Cryptage :

Alice doit maintenant crypter le message pour l'envoyer à Bob.

1. Pour ce faire, elle utilise la clé publique pour chaque bloc :

$83^{19} \equiv 493 \pmod{943}$.
$65^{19} \equiv 152 \pmod{943}$,
$76^{19} \equiv 540 \pmod{943}$,
$85^{19} \equiv 150 \pmod{943}$,
$84^{19} \equiv 226 \pmod{943}$,

[236] L'algorithme d'Euclide étendu est une variante de l'algorithme d'Euclide qui permet, à partir de deux entiers a et b, de calculer non seulement leur plus grand commun diviseur (PGCD), mais aussi deux entiers u et v tels que au + bv = pgcd(a,b). L'algorithme d'Euclide permet d'obtenir de tels entiers parce qu'à chaque étape de l'algorithme, on n'a que des sommes de multiples de a et b. Quand a et b sont premiers entre eux : u est alors l'inverse pour la multiplication de a modulo b, ce qui est un cas particulièrement utile. Comme l'algorithme d'Euclide, l'algorithme étendu se généralise aux anneaux euclidiens, par exemple aux polynômes à une variable sur un corps.

Le message codé est donc M = 493 152 540 150 226.

2. Alice peut maintenant envoyer le message crypté à Bob (par courrier postal, par courrier électronique, par téléphone, etc).

IV) Décryptage :

Bob reçoit le message sous sa forme chiffrée : M = 493 152 540 150 226.

1. Il utilise donc sa clé privée pour décrypter ce message, et récupérer le véritable contenu. Pour ce faire, il déchiffre le message de la façon suivante :

2. Chacun des blocs de 4 chiffres est élevé à l'exposant d de la clé privée de Bob, ici égale à 139, et congru au message d'origine modulo 943 :

$0493^{139} \equiv 0083 \pmod{943}$,

$0756^{139} \equiv 6576 \pmod{943}$,

$0030^{139} \equiv 8584 \pmod{943}$.

3. Ainsi (Ma)b = 00 83 65 76 85 84.

4. A présent, il ne reste plus qu'à retranscrire le message en langage d'origine : 00 83 65 76 85 84 = « SALUT »

5. Le message a été correctement transféré, et personne n'a pu le lire pendant le transfert !

Points forts et faiblesses :

Avantage :

La méthode de cryptographie RSA est un procédé actuellement très fiable et très utilisé qui regroupe tous les avantages d'un système cryptographique idéal. Il est d'ailleurs considéré comme le plus efficace des systèmes cryptographiques à clé publique.

Sa grande force repose sur la difficulté de décomposer de très grands nombres en produit de facteurs premiers et établi ainsi un lien mathématique pratiquement incassable entre clé privée et clé publique.

Si la taille du nombre n dépasse 1024 bits, alors il est impossible avec les moyens actuels, d'en déterminer les facteurs premiers le composant, et donc, l'information transmise par ce système reste dans une confidentialité absolue. Si la taille de ce nombre atteint 4096 bits, alors il est inespéré qu'il soit factorisé dans un avenir prévisible.

Inconvénient :

La principale faiblesse de ce système est qu'il n'est théoriquement pas impossible de décomposer de grands nombres en produit de facteurs premiers. D'ailleurs, l'évolution des technologies et des puissances de calculs, repoussent toujours plus loin les limites de factorisation.

En effet, une clé de 256 bits peut être factorisée en quelques heures par un ordinateur individuel, et une clé de 512 bits peut être cassée par l'associativité de nombreux ordinateurs (voir encadré page suivante), en un temps raisonnable.

L'actuel record de factorisation, réalisé en 2005, à permis de décomposer entièrement un nombre de 663 bits en produit de facteurs premiers par calcul distribué.

Donc, si la taille des clés reste inférieure à 1024 bits pour l'échange d'un message, sa sécurité ne sera pas totalement assurée.

De plus, si l'on admet que la puissance des ordinateurs double tous les 18 mois (loi de Moore), alors il faudra constamment repousser la taille des clés. Une clé de 2048 bits par exemple, devrait tenir jusqu'en 2079.

Mais il faut également prendre en compte la possibilité que de nouveaux procédés de factorisations soient découverts à l'avenir et permettent ainsi de réduire, si ce n'est d'anéantir, le temps de factorisation nécessaire sur grands nombres.

Enfin, les progrès de la physique vont peut-être sonner le glas de la cryptographie mathématique. Il a été défini, du moins en théorie, un modèle d'ordinateur quantique qui permettrait de factoriser très

rapidement des entiers. Les ordinateurs quantiques n'en sont encore qu'à leurs prémices, mais finiront un jour où l'autre par rendre le système RSA obsolète.

Petits commentaires au sujet de RSA

De nombreuses erreurs dans la gestion imprudente ou maladroite des clés sont à l'origine de décryptages inopinés de messages considérés inviolables, car obtenus avec RSA. L'idée défendue que le noyau mathématique du RSA est inviolable est seulement une conclusion expérimentale tirée de l'échec des tentatives connues d'attaques du RSA. Cette conclusion n'interdit pas que le risque théorique lié au RSA puisse être jugé grand, puisqu'on n'a ni réussi à montrer que la factorisation est difficile, ni même réussi à montrer que le RSA est aussi difficile que la factorisation.

À l'évidence, si une agence de renseignements a découvert quelque chose concernant la factorisation ou s'appliquant directement au RSA sans passer par la factorisation, elle ne rendra pas publique sa découverte et, au contraire, fera tout pour la maintenir secrète le plus longtemps possible. C'est du simple bon sens que de dire cela.

Le calcul distribué, méthode pour casser les clés.

Le principe de base consiste à découper le problème initial en une miriade de sous-problèmes indépendants. Par exemple pour les projets relatifs au décryptage l'algorithme de base consiste à tester toutes les clefs possibles, une par une. Chaque clef peut être testée indépendamment des autres. Si on disposait de deux ordinateurs, sur l'un on testerait les clefs paires (une clef peut être assimilée à un nombre) et sur l'autre les clefs impaires. Cela divise le temps nécessaire pour tester toutes les clefs par deux.

Pour étendre ça à l'échelle d'Internet on construit un système client/serveur et on procède de façon similaire. Prenons l'exemple de DES. Il y a 256 clefs à tester. On commence par en faire des petits paquets, par exemple 228 paquets, (aka blocs), de 228 clefs chacun. Ensuite, sur une machine connectée à Internet en permanence, on installe un logiciel qui va distribuer ces blocs de clefs à la demande, c'est le « serveur ». Chaque participant utilise ensuite un logiciel dit « client » qui va contacter le serveur, demander un paquet de clefs et commencer à tester toutes les clefs contenues dans ce paquet. Une fois toutes les clefs testées, il va recontacter le serveur pour lui indiquer le résultat de sa recherche : « j'ai trouvé la clef solution » ou « j'ai rien trouvé ». La plupart du temps, toutes les clefs étaient mauvaises et il ne lui reste plus qu'à demander un autre paquet de clefs à tester. Le serveur se charge de garder la trace des paquets de clefs déjà testés et garde un ensemble d'informations qui permettent d'établir des statistiques indiquant qui a testé le plus de clefs, qui est le plus rapide, combien d'utilisateurs participent...

Mais lorsque ce logiciel teste toutes les clefs la machine doit être inutilisable !

Non. Cela grâce au multitâche préemptif que tous les OS modernes supportent. Cela inclut Unix et donc bien sûr Linux et FreeBSD, Windows NT, OS/2 et même Windows 95. Le logiciel client va démarrer avec une priorité très faible et ne sera donc exécuté que si aucune autre application n'a de travail à faire. Et c'est souvent le cas. Les applications passent leur temps à attendre soit une entrée au clavier soit que les données arrivent du disque dur. Pendant ces attentes, habituellement, le processeur se tourne les pouces.

Il n'est pas nécessaire de se connecter à Internet très longtemps ni très fréquemment. La quantité de données à transférer varie suivant le projet mais les logiciels clients vous permettent généralement de télécharger du travail pour plusieurs jours voire plus d'une semaine.

Il reste l'aspect mémoire. Les logiciels de décryptage utilisent très peu de mémoire et n'auront donc aucune incidence de ce coté. Les autres projets utilisent généralement plus de mémoire et il peut être préférable de les réserver aux machines les plus puissantes ou bien de les faire tourner lorsque l'ordinateur n'est pas utilisé, sous forme d'économiseur d'écran par exemple.

Il y a de nombreux autres projets utilisant le calcul distribué : factorisation des nombres de Fermat, factorisation des nombres composites, *SETI* : programme de recherche d'intelligence extra-terrestre, *ClimatePrediction*, dont le but est de prédire l'évolution du climat au 21e siècle, *FightAIDS@Home*, un projet qui étudie l'évolution de la résistance du virus du Sida au médicaments, etc.

Dix fois dans l'histoire des services d'espionnage, un système de codage a été considéré cent pour cent sûr et inviolable par ceux qui l'utilisaient, alors qu'au même moment un service ennemi ayant percé de secret du système lisait tranquillement tous les messages qui tombaient entre ses mains. Il suffit de relire les pages précédentes !

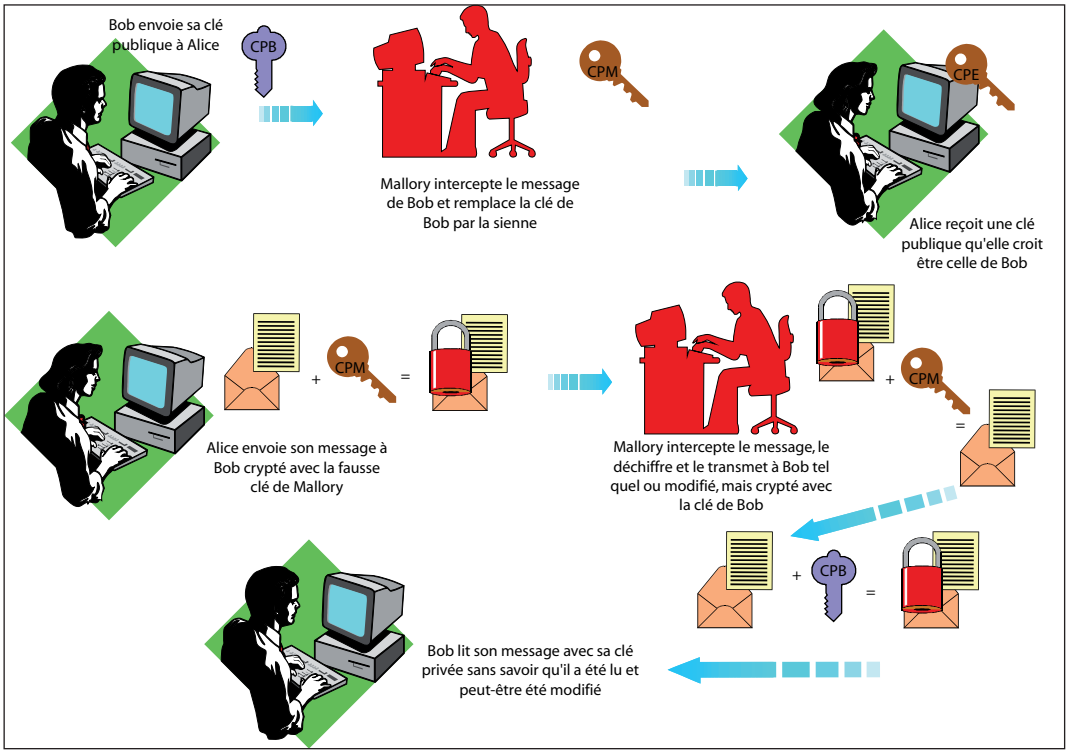
Si nous souhaitons protéger des données pour une longue période de temps, soyons conscients que tout s'appuie, en cryptographie mathématique, sur un état de l'Art qui peut changer rapidement et dont la réalité est peut-être déjà totalement autre que celle présentée au public.

Peter Shor a montré en 1994 qu'avec un ordinateur quantique on peut factoriser efficacement des nombres entiers. Si l'on réussit à construire de telles machines, tout un pan de la cryptographie mathématique sera définitivement compromis. Les ordinateurs quantiques encore aujourd'hui (?) sont de simples fictions théoriques, cependant, là encore, l'avance possible de certains services secrets (ou de la NSA ?...) n'est pas à exclure et, si elle est réellement sensible, alors il se peut que pour eux la factorisation des clés de 1 024 bits ou de 2 048 bits du RSA soit devenue un jeu d'enfant...

Les certificats numériques

Les certificats numériques sont importants en cryptographie à clé publique parce qu'ils garantissent qu'il n'y a pas d'intermédiaire (appelé en cryptologie l'*homme du milieu*[237]) qui espionne les échanges.

Reprenons notre schéma en y incorporant un intermédiaire malveillant.



Les certificats numériques sont délivrés par des « Autorités de certification », ce sont des sociétés privées pour la plupart. La première a vu le jour en 1988, c'était la société *Verisign*.

[237] L'attaque *Man In The Middle* - ou homme du milieu (HDM) - consiste pour un tiers à s'interposer dans une communication sans que les parties concernées n'en aient conscience. Il existe en réalité plusieurs méthodes d'attaque dites Man In The Middle. En cryptographie, il s'agirait ainsi pour l'assaillant de parvenir à lire, adresser et modifier des messages chiffrés entre deux parties de manière transparente pour ces dernières. Pour cela, il devra préalablement écouter le trafic réseau et intercepter les paquets IP. La technique man in the middle peut par conséquent s'appliquer dans un système de chiffrement par clefs publiques, ainsi que dans le protocole d'échange de clefs Diffie-Hellman, lorsque celui-ci est utilisé sans authentification. La paternité de la première mise en œuvre remonterait aux années 90 et serait le fait d'un célèbre pirate, reconverti depuis en expert de la sécurité et auteur : Kevin David Mitnick. Plus précisément, Mitnick aurait utilisé une méthode appelée IP Spoofing afin de s'introduire dans l'ordinateur de Tsutomu Shimomura, un expert de la sécurité en relation avec plusieurs agences gouvernementales américaines.
L'IP Spoofing consiste à forger ses propres paquets IP en modifiant notamment l'adresse IP source. Kevin Mitnick aurait ainsi leurré l'ordinateur de Shimomura en laissant croire que les paquets IP reçus provenaient d'une machine autorisée de la Loyola University de Chicago. À charge de revanche toutefois puisque Shimomura a par la suite collaboré avec le FBI et contribué à sa capture en 1995.

Signature et authentification

Un document signé ne doit pas pouvoir être modifié sans le consentement de son signataire. Pour garantir la fabrication des signatures électroniques, on passe par la confection de résumés électroniques des messages. Pour ce faire, on utilise les fonctions de *hachage*[238]. Depuis le simple chiffrement d'un texte, nous sommes parvenus à une notion plus complexe, celle de signature numérique. En effet, en procédant par cumul des cryptages, associé à une fonction de hachage, nous pouvons assurer les fonctions de confidentialité, d'authentification et d'intégrité des données. Il s'agit là de l'un des principaux avantages offerts par la cryptographie à clé publique. L'utilisation des signatures garantit aussi la *non-répudiation*[239].

PGP

Pretty Good Privacy, est une combinaison des meilleures fonctionnalités de la cryptographie de clé publique et de la cryptographie conventionnelle. PGP est un *système de cryptographie hybride.* Lorsqu'un utilisateur crypte du texte en clair avec PGP, ces données sont d'abord compressées. Cette compression des données permet de réduire le temps de transmission par modem, d'économiser l'espace disque et, surtout, de renforcer la sécurité cryptographique. La plupart des cryptanalystes exploitent les modèles trouvés dans le texte en clair pour casser le chiffrement. La compression réduit ces modèles dans le texte en clair, améliorant par conséquent considérablement la résistance à la cryptanalyse. Toutefois, la compression est impossible sur les fichiers de taille insuffisante ou supportant mal ce processus. PGP crée ensuite une *clé de session* qui est une clé secrète à usage unique. Cette clé correspond à un nombre aléatoire, généré par les déplacements aléatoires de votre souris et les séquences de frappes de touches. Pour crypter le texte en clair, cette clé de session utilise un algorithme de cryptage conventionnel rapide et sécurisé. Une fois les données codées, la clé de session est cryptée vers la clé publique du destinataire. Cette clé de session cryptée par clé publique est transmise avec le texte chiffré au destinataire.

Les protocoles

Il existe bien des protocoles de cryptage que nous utilisons sans le savoir, car ils sont la plupart du temps transparents pour l'utilisateur. Le protocole **SSL** (Secure Socket Layer) ou **TLS** (Transport Layer Security) utilisé sur Internet, quand vous êtes avisé que vous visitez une page sécurisée et que se ferme le petit cadenas en bas à droite de votre écran. Le protocole **SSH** (Secrure Shell) qui transmet votre mot de passe après chiffrement quand vous vous connectez à une entreprise par exemple, ou au site des impôts. Le protocole **CHAP** (Challenge-Handshake Authentification Protocol), qui est celui utilisé quand vous vous connectez directement à votre fournisseur d'accès Internet. Le protocole **EAP** (Extensible Authetification Protocol) utilisé principalement dans les réseaux sans fil.

Les protocoles cryptographiques ne sont pas utilisés uniquement sur des ordinateurs connectés à Internet. Ils interviennent dès que des transactions se font par un réseau. Par exemple, ils sont utilisés depuis longtemps dans les décodeurs de chaînes de télévision cryptées. De la même manière, les protocoles sont au cœur de la téléphonie mobile. Chaque téléphone portable contient une carte SIM qui comporte un numéro unique qui l'identifie. On trouve évidemment des protocoles cryptographiques dans tout le système des cartes bancaires et dans la carte Vitale.

[238] Une fonction de hachage, par exemple MD5, forme un résumé d'un texte en remplissant les deux objectifs suivants : - la moindre modification du message initial entraîne une modification majeure du résumé ; - il n'est pas possible de former un message dont le résumé soit égal à une expression donnée. Le résumé MD5 d'un texte est obtenu en commençant par compléter ce texte avant le le sectionner en blocs de 512 bits. Un procédé itératif modifie ensuite une valeur initiale de 128 bits convenue en fonction de chacun des blocs du texte par application de fonctions complexes (et notamment de valeurs prises par la fonction sinus). La valeur finale est le résumé cherché.

[239] Fait de ne pas pouvoir revenir sur le contenu d'un document ou d'une transaction.

La fiabilité des protocoles repose essentiellement sur la fiabilité des algorithmes de cryptage, et nous savons que cette fiabilité ne dure pas. C'est ce qui pousse les chercheurs a explorer d'autres voies comme par exemple la cryptographie quantique. Nous y reviendrons.

Les attaques révélées sur les divers protocoles

Il est intéressant, tout comme pour les bons vieux cryptogrammes du temps jadis, de connaître l'état des attaques contre les divers procédés de cryptage que nous venons de survoler. En premier lieu, cela permet de mesurer la fiabilité réelle, mais provisoire, et cela donne également la mesure de la confiance que l'on peut accorder à ces techniques.

Une attaque est souvent caractérisée par les données qu'elle nécessite :

- attaque sur texte chiffré seul (*ciphertext-only*) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.
- attaque à texte clair connu (*known-plaintext attack*) : le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
- attaque à texte clair choisi (*chosen-plaintext attack*) : le cryptanalyste possède des messages en clair, il peut générer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.
- attaque à texte chiffré choisi (*chosen-ciphertext attack*) : le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

Résumons rapidement les différents types d'attaques employées par le cryptanalyste :

L'analyse fréquentielle

L'analyse fréquentielle examine les répétitions des lettres du message chiffré afin de trouver la clé. Elle est inefficace contre les chiffrements modernes tels que DES, RSA. Elle est principalement utilisée contre les chiffrements mono-alphabétiques qui substituent chaque lettre par une autre et qui présentent un biais statistique.

L'indice de coïncidence

L'indice de coïncidence permet de calculer la probabilité de répétitions des lettres du message chiffré. Il est souvent couplé avec l'analyse fréquentielle. Cela permet de savoir le type de chiffrement d'un message (chiffrement mono-alphabétique ou polyalphabétique) ainsi que la longueur probable de la clé.

L'attaque par mot probable

L'attaque par mot probable consiste à supposer l'existence d'un mot probable dans le message chiffré. Il est donc possible d'en déduire la clé du message si le mot choisi est correct. Ce type d'attaque a été mené contre la machine Enigma durant la Seconde Guerre mondiale.

L'attaque par dictionnaire

L'attaque par dictionnaire consiste à tester tous les mots d'une liste comme mot clé. Elle est souvent couplée à l'attaque par force brute.

L'attaque par force brute

L'attaque par force brute consiste à tester toutes les solutions possibles de mots de passe ou de clés. C'est le seul moyen de récupérer la clé dans les algorithmes les plus modernes et encore inviolés comme AES[240].

[240] Des attaques existent sur des versions simplifiées d'AES. Niels Ferguson et son équipe ont proposé en 2000 une attaque sur une version à 7 tours de l'AES 128 bits. Une attaque similaire casse un AES de 192 ou 256 bits contenant 8 tours. Un AES de 256 bits peut être cassé s'il est réduit à 9 tours avec une contrainte supplémentaire. En effet, cette dernière attaque repose sur

Attaque par paradoxe des anniversaires

Le paradoxe des anniversaires[241] est un résultat probabiliste qui est utilisé dans les attaques contre les fonctions de hachage. Ce paradoxe permet de donner une borne supérieure de résistance aux collisions d'une telle fonction. Cette limite est de l'ordre de la racine de la taille de la sortie, ce qui signifie que, pour un algorithme comme MD5 (empreinte sur 128 bits), trouver une collision quelconque avec 50% de chance nécessite 264 hachages d'entrées distinctes.

Cryptanalyse moderne

Dès les années 70 apparaissent les méthodes de chiffrement modernes par blocs comme DES. Il sera passablement étudié et attaqué ce qui mènera à des attaques majeures dans le monde de la cryptographie. Les méthodes présentées ci-dessous ne sont pas vraiment génériques et des modifications sont nécessaires pour attaquer un type de chiffrement donné.

Souvent, on ne s'attaque pas à une version complète de l'algorithme de chiffrement, mais une variante avec moins de tours (dans le cas des schémas de type Feistel ou les fonctions de hachage). Cette analyse préliminaire, si elle permet de déceler des vulnérabilités, laisse entrevoir une attaque sur l'algorithme complet.

Cryptanalyse linéaire

La cryptanalyse linéaire, due à Mitsuru Matsui, consiste à faire une approximation linéaire de la structure interne de la méthode de chiffrement. Elle remonte à 1993 et s'avère être l'attaque la plus efficace sur DES. Les algorithmes plus récents sont insensibles à cette attaque.

Cryptanalyse différentielle

La cryptanalyse différentielle est une analyse statistique des changements dans la structure de la méthode de chiffrement après avoir légèrement modifié les entrées. Avec un très grand nombre de perturbations, il est possible d'extraire la clé. Cette attaque date de 1990 (présentée à la conférence Crypto 90). Elle est due à Eli Biham et Adi Shamir. Toutefois, on sait maintenant que les concepteurs de DES connaissaient une variante de cette attaque nommée attaque-T. Les algorithmes récents (AES, IDEA[242],

---

le principe des « related-keys » (clés apparentées). Dans une telle attaque, la clé demeure secrète mais l'attaquant peut spécifier des transformations sur la clé et chiffrer des textes à sa guise. Il peut donc légèrement modifier la clé et regarder comment la sortie de l'AES se comporte. Certains groupes ont affirmé avoir cassé l'AES complet mais après vérification par la communauté scientifique, il s'avérait que toutes ces méthodes étaient erronées. Cependant, plusieurs chercheurs ont mis en évidence des possibilités d'attaques algébriques, notamment l'attaque XL et une version améliorée, la XSL. Ces attaques ont été le sujet de nombreuses controverses et leur efficacité n'a pas encore été pleinement démontrée, le XSL fait appel à une analyse heuristique dont la réussite n'est pas systématique. De plus, elles sont impraticables car le XSL demande au moins 287 opérations voire 2100 dans certains cas. Le principe est d'établir les équations (quadratiques / booléennes) qui lient les entrées aux sorties et de résoudre ce système qui ne comporte pas moins de 8.000 inconnues et 1.600 équations pour 128 bits. La solution de ce système reste pour l'instant impossible à déterminer. En l'absence d'une preuve formelle sur l'efficacité d'attaques similaires au XSL, l'AES est donc considéré comme sûr. On peut toutefois parier que dans les années à venir, les avancées en cryptanalyse et la relative simplicité de la structure d'AES devraient ouvrir des brèches dans l'algorithme. Si pareille découverte venait à se produire, des méthodes similaires à AES, comme Camellia, pourraient rapidement devenir obsolètes.

[241] Le paradoxe des anniversaires, dû à Richard von Mises, est à l'origine, une estimation probabiliste du nombre de personnes que l'on doit réunir pour avoir une chance sur deux que deux personnes de ce groupe aient leur anniversaire le même jour de l'année. Il se trouve que ce nombre est 23, ce qui choque un peu l'intuition. À partir d'un groupe de 57 personnes, la probabilité est supérieure à 99 %. Cependant, il ne s'agit pas d'un paradoxe dans le sens de contradiction logique ; c'est un paradoxe, dans le sens où c'est une vérité mathématique qui contredit l'intuition : la plupart des gens estiment que cette probabilité est très inférieure à 50 %. Les gens pensent en général à la probabilité que 2 personnes soient nées en même temps un jour donné, probabilité qui est en effet très faible. Le paradoxe des anniversaires est utilisé en cryptographie pour élaborer des attaques sur les fonctions de hachage. Une des contraintes imposées sur ces fonctions, pour une utilisation cryptographique, est de produire peu de collisions, autrement dit, de rarement prendre la même valeur sur des entrées différentes.

[242] IDEA est un algorithme de chiffrement symétrique par blocs utilisé pour chiffrer et déchiffrer des données. Il manipule des blocs de texte en clair de 64 bits. Une clé de chiffrement longue de 128 bits (qui doit être choisie aléatoirement) est utilisée

etc.) sont conçus pour résister à ce type d'attaque. Les attaques différentielles sont aussi possibles sur les fonctions de hachage, moyennant des modifications dans la conduite de l'attaque. Une telle attaque a été menée contre MD5.

Cryptanalyse différentielle tronquée

Comme son nom l'indique, une telle cryptanalyse s'intéresse à des différences qui n'affectent qu'une partie des variables considérées.

Cryptanalyse différentielle d'ordre supérieur

La cryptanalyse différentielle originale est une différentielle de premier ordre. En introduisant l'équivalent des dérivées dans les fonctions cryptographiques, on peut mener une cryptanalyse avec des degrés supérieurs. Ce sont des « différences de différences de ... ».

Cryptanalyse par différentielles impossibles

Au lieu de chercher les différences probables, on inverse le problème et l'on cherche les différences qui ne se produiront pas. La cryptanalyse différentielle impossible ou cryptanalyse par différentielles impossibles est une technique basée sur la cryptanalyse différentielle (1990), elle a été proposée en 1999 par Eli Biham, Adi Shamir et Alex Biryukov dans le cadre de la cryptanalyse de Skipjack[243]. Le concept en lui-même est apparu quelques années auparavant lors d'attaques différentielles, mais il n'y avait pas de méthodologie formellement définie.

Le principe original de la cryptanalyse différentielle est de perturber les entrées du chiffrement et observer le comportement de ces modifications dans la structure de chiffrement pour séparer les bonnes clés des mauvaises. La cryptanalyse différentielle impossible inverse le problème en cherchant des propagations qui ne se produiront assurément pas. Si une clé candidate produit un comportement considéré comme impossible alors la clé peut être écartée.

Dans leur papier, Shamir et Biryukov font une analogie avec un crible : l'attaque trie les clés et élimine celles qui sont en contradiction avec les observations. Ils font remarquer que le principe n'est pas complètement nouveau. En effet, la cryptanalyse d'Enigma durant la Seconde Guerre mondiale était basée sur certaines caractéristiques impossibles comme une lettre qui se chiffre en elle-même.

L'attaque boomerang

L'attaque boomerang est une version améliorée de la cryptanalyse différentielle inventée par David Wagner[244]. Elle consiste à attaquer les deux moitiés d'un algorithme de chiffrement par bloc et part du principe que certaines propriétés, après perturbations des entrées, ne se propagent pas à travers toute la structure.

---

pour le chiffrement des données, et on a besoin de la même clé secrète pour les déchiffrer. Comme tous les algorithmes de chiffrement par blocs, IDEA utilise à la fois la confusion et la diffusion. L'algorithme est basé sur le mélange d'opérations de différents groupes algébriques. Il y a trois groupes algébriques dont les opérations sont mélangées, et toutes ces opérations sont facilement réalisables à la fois en logiciel et en matériel.

[243] Skipjack fut conçu par la NSA durant les années 1980 dans le cadre d'un projet du gouvernement américain relatif à une puce contenant des primitives cryptographiques, le Clipper chip. Elle était notamment destinée aux appareils électroniques vendus au grand public. La clé de chiffrement devait être fournie au gouvernement qui devenait ainsi capable d'écouter les communications si nécessaire. Skipjack était l'algorithme employé pour le chiffrement au sein du Clipper chip, la puce était conçue pour résister aux modifications externes et permettait au gouvernement d'accéder aux données en clair grâce à un mécanisme nommé *Law Enforcement Access Field* (LEAF). Le chiffrement de bloc était à l'origine secret. Cette attitude du gouvernement (qui va à l'encontre de ce qui se fait habituellement en cryptologie où la transparence est primordiale) alimentait la suspicion de la communauté scientifique à son égard. Devant les doutes des cryptologues, l'algorithme fut déclassifié le 24 juin 1998.

[244] David Wagner , cryptologue et informaticien américain né en 1974. Professeur de mathématiques et d'informatique à Berkeley en Californie. Il est l'auteur de l'Attaque boomerang dans le cadre de la cryptographie symétrique. Les recherches de David Wagner portent sur la sécurité dans les réseaux et les primitives cryptographiques. Il est aussi l'auteur d'outils destinés à vérifier la robustesse de programmes écrits en C et détecter les vulnérabilités présentes dans le code.

L'attaque rectangle

L'attaque rectangle est une extension de l'attaque boomerang, elle a été inventée en 2001 par Eli Biham et son équipe pour attaquer leur chiffrement Serpent[245], candidat pour le standard AES.

Cryptanalyse différentielle-linéaire

Introduite par Martin Hellman et Langford, la cryptanalyse différentielle-linéaire combine les deux principes. L'attaque différentielle produit une approximation linéaire de l'algorithme. Avec cette attaque, Hellman et Langford ont pu attaquer un DES de 8 rondes avec seulement 512 textes en clair et quelques secondes sur un PC de l'époque. Cette méthode a également été employée pour trouver des clés faibles dans IDEA. Ce type de cryptanalyse a été amélioré par Eli Biham en 2002.

Cryptanalyse X^2

La cryptanalyse X^2, concept dû à Serge Vaudenay, permet d'obtenir des résultats similaires à des attaques linéaires ou différentielles. L'analyse statistique associée permet de s'affranchir des défauts de ces dernières en évitant d'avoir à connaître le fonctionnement exact du chiffrement.

Cryptanalyse quadratique

La cryptanalyse quadratique est une invention récente de Nicolas Courtois et Josef Pieprzyk. Cette attaque (nommée attaque XSL) vise en particulier AES et les autres chiffrements basés sur Rijndael. L'attaque XSL est le sujet de beaucoup de controverses quant à sa véritable efficacité de par sa nature heuristique. Elle consiste à résoudre un système d'équations de très grande taille.

Cryptanalyse modulo n

Suggérée par Bruce Schneier, David Wagner et John Kelsey en 1999, cette technique consiste à exploiter les différences de fonctionnement (selon une congruence[246] variable) des algorithmes qui utilisent des rotations binaires.

Attaques par canaux auxiliaires

On distingue plusieurs attaques qui appartiennent à ce genre. Elles consistent à exploiter des propriétés inattendues d'un algorithme lors de sa mise en œuvre. En effet, une sécurité « mathématique » ne garantit pas forcément une sécurité lors de l'utilisation en « pratique ». Dans ce domaine, les attaques sont nombreuses et portent sur différents paramètres :

- temps mis pour effectuer certaines opérations (attaque temporelle)
- le bruit généré par un ordinateur qui chiffre, le processeur émet du bruit qui varie selon sa consommation et les opérations effectuées (cryptanalyse acoustique)
- la consommation électrique (analyse de consommation)
- introduction volontaire d'erreurs dans le système pour provoquer certains comportements révélateurs (attaque par faute)

Une attaque basée sur les temps de réponse a été menée par Serge Vaudenay sur TLS/SSL, ce qui a forcé les concepteurs du standard à faire une mise à jour critique. Les constructeurs de puces de chiffrement visent à aplanir la courbe de consommation électrique pour dissimuler les opérations sous-jacentes.

Compromis temps/mémoire

Ce concept a été introduit par Martin Hellman en 1980. Il a été amélioré en 1993 par Philippe Oechslin avec le concept de table arc-en-ciel, qui lui a permis par exemple d'attaquer les mots de passe

[245] Serpent est un algorithme de chiffrement par bloc finaliste pour le concours AES. Il obtiendra finalement la 2e place (59 votes contre 86 votes pour Rijndael). Serpent a été conçu par Ross Anderson, Eli Biham et Lars Knudsen.

[246] Derrière le terme de congruence se cachent des notions semblables mais de niveaux d'abstraction différents. Historiquement, le terme de congruence naît sous la plume de Gauss pour l'ensemble des entiers relatifs.
En arithmétique modulaire, on dit que deux entiers relatifs sont congrus modulo p s'ils ont même reste dans la division euclidienne par p. On peut aussi dire qu'ils sont congrus modulo p si leur différence est un multiple de p.
La relation de congruence est notée par trois traits horizontaux(≡), suivi du modulo entre crochets.
Exemple : *12* est congru à *2* modulo *5* (*12* ≡ *2 [5]*) car *12* et *2* ont le même reste après division euclidienne par *5*.

de sessions *Windows*, lorsqu'ils sont stockés au format *LanManager*, comme c'est encore le cas le plus souvent. Il s'agit d'un compromis entre une attaque par force brute et l'utilisation de dictionnaires. Une recherche exhaustive nécessite en effet beaucoup de temps alors qu'un dictionnaire de tous les mots de passe possibles nécessiterait énormément de place. Grâce à des procédés algorithmiques, on cherche à trouver un juste milieu entre ces deux principes, en construisant des tables de taille gérable.

Attaques sur les modes opératoires

Les chiffrements par bloc comme DES ou AES ne peuvent chiffrer qu'un bloc de taille donnée (128 bits dans le cas d'AES). Pour chiffrer des données plus longues, on utilise des modes opératoires. Un mode opératoire est la manière de chaîner plusieurs blocs ensemble pour obtenir un chiffrement par flux. Par exemple, on peut découper les données en blocs de 128 bits et les chiffrer séparément. C'est le mode ECB qui est vulnérable puisque la présence de deux blocs chiffrés identiques indique que les deux blocs respectifs dans le message original sont également identiques. D'autres modes évitent ce problème mais ne sont pas totalement exempts de vulnérabilités. On utilise alors des vecteurs d'initialisation qui permettent d'éviter la répétition de séquences identiques entre plusieurs messages chiffrés.

Les chiffrements par flot (par exemple RC4[247]) utilisent aussi un vecteur d'initialisation pour les mêmes raisons. Une telle attaque a été récemment menée à ce propos sur le chiffrement des documents de la suite Office de Microsoft, qui emploie RC4. Le vecteur d'initialisation y est toujours le même pour un document donné ; un grand nombre d'informations peuvent donc être récupérées en comparant le résultat du chiffrement d'un document après légère modification.

Attaque par rencontre au milieu

Chiffrer deux fois avec le même algorithme, mais via deux clés différentes est une ouverture à une attaque de type rencontre au milieu. Contrairement à ce que l'on peut penser de prime abord, le chiffrement obtenu n'est pas équivalent à un chiffrement avec une clé deux fois plus longue (on ne passe pas de 256 à 512 dans le cas de DES). Il suffit en effet d'essayer toutes les clés pour déchiffrer la première étape. On obtient un résultat, toujours chiffré, qui se trouve entre les deux blocs de chiffrement. Ce résultat est soumis à son tour à une recherche exhaustive avec toutes les clés possibles. Au final, la complexité est seulement multipliée par deux. Dans le cas de DES, on obtient une résistance de l'ordre de 257, c'est pourquoi on utilise 3DES[248] qui a une complexité finale de 2112 opérations (malgré une clé plus longue de 3*56 bits). Grâce à trois chiffrements, chaque sortie du deuxième bloc de chiffrement doit être essayée avec toutes les clés, ce qui augmente considérablement le nombre de possibilités.

[247] RC4 est un algorithme de chiffrement à flot, conçu en 1987 par Ronald Rivest, l'un des inventeurs du RSA, pour les Laboratoires RSA. Il est supporté par différentes normes, par exemple dans SSL ou encore WEP. Le Wired Equivalent Privacy (abrégé WEP) est un protocole pour sécuriser les réseaux sans-fil de type Wi-Fi. Les réseaux sans-fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique. Cependant, plusieurs faiblesses graves ont été identifiées par les cryptologues. Le WEP est parfois surnommé avec le sobriquet de Weak Encryption Protocol (Faible protocole de chiffrage). Le WEP a donc été supplanté par le WPA en 2003, puis par le WPA2 en 2004 (WPA2 est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance). Malgré ses faiblesses intrinsèques, le WEP fournit un niveau de sécurité minimal qui peut décourager les attaquants les moins expérimentés, quoique l'on puisse trouver aujourd'hui des utilitaires de cracking de réseaux WEP.

[248] Le Triple DES (aussi appelé 3DES) est un algorithme de chiffrement symétrique enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes. Cette utilisation de trois chiffrements DES a été développée par Walter Tuchman (chef du projet DES chez IBM), il existe en effet d'autres manières d'employer trois fois DES mais elles ne sont pas forcément sûres. La version de Tuchman utilise un chiffrement, suivi d'un déchiffrement pour se conclure à nouveau par un chiffrement. Le Triple DES est généralement utilisé avec seulement deux clés différentes.

Attaques sur les systèmes asymétriques

Casser un chiffrement assuré par de la cryptographie asymétrique nécessite d'autres approches. Dans le cas de RSA, c'est la difficulté de la factorisation qui assure la résistance du chiffrement. Pour ElGamal[249], c'est le problème du logarithme discret[250] qui est employé. Toutefois, certaines failles peuvent apparaître selon l'utilisation que l'on fait de ces algorithmes. RSA est vulnérable si des exposants de faible magnitude sont utilisés (attaques de Don Coppersmith[251] et Wiener). Sous des conditions particulières, un surchiffrement avec RSA peut être attaqué. Le standard PKCS assure une utilisation plus robuste de RSA, même si les premières ébauches du standard étaient sensibles à des attaques par des canaux auxiliaires (Bleichenbacher).

Attaque temporelle

En cryptanalyse, une attaque temporelle consiste à estimer et analyser le temps mis pour effectuer certaines opérations cryptographiques dans le but de découvrir des informations secrètes. Certaines opérations peuvent prendre plus de temps que d'autres et l'étude de ces informations temporelles peut être précieuse pour le cryptanalyste. La mise en œuvre de ce genre d'attaque est intimement liée au matériel ou au logiciel attaqué. Des attaques temporelles peuvent aussi se faire à distance, via un réseau. L'observation des délais dans un système est en général soumise à des perturbations aléatoires. Ceci est d'autant plus vrai que l'observation se fait via un réseau. La plupart des attaques temporelles demandent que l'adversaire connaisse les détails de l'implémentation. Cependant, ces attaques peuvent aussi servir à identifier les algorithmes employés et faire de l'ingénierie inverse.

Autres propriétés analysées

Certaines propriétés observées dans les algorithmes de chiffrement ne mènent pas forcément à des attaques mais permettent de déceler des faiblesses dans la conception, problèmes qui peuvent en cacher d'autres plus importants.

Les clés faibles

Certains algorithmes sont susceptibles d'avoir des clés dites faibles. Si une telle clé est utilisée pour chiffrer un message une première fois et que l'on rechiffre le résultat, toujours avec la même clé, alors on obtient le message en clair. Plus formellement, $E_k(E_{k(m)})=m$. DES possède 4 clés de ce genre. Il y a aussi des clés dites semi-faibles. Dans ce cas, $E_{k1}(E_{k2(m)})=m$.

Biais statistique

On peut chercher si la structure de chiffrement produit des biais statistiques. En général, un algorithme de chiffrement est censé produire un résultat proche d'un générateur de nombres aléatoires uniformément distribués, de manière à donner le moins d'information possible et maximiser l'entropie. Si un biais est observé (par exemple, on observe plus de bits à '1' que de bits à '0') alors des analyses supplémentaires peuvent parfois permettre de concevoir une attaque. Citons entre autres des attaques sur RC6 dont les permutations s'écartent sensiblement des caractéristiques normalement observées dans les générateurs de nombres pseudo-aléatoires.

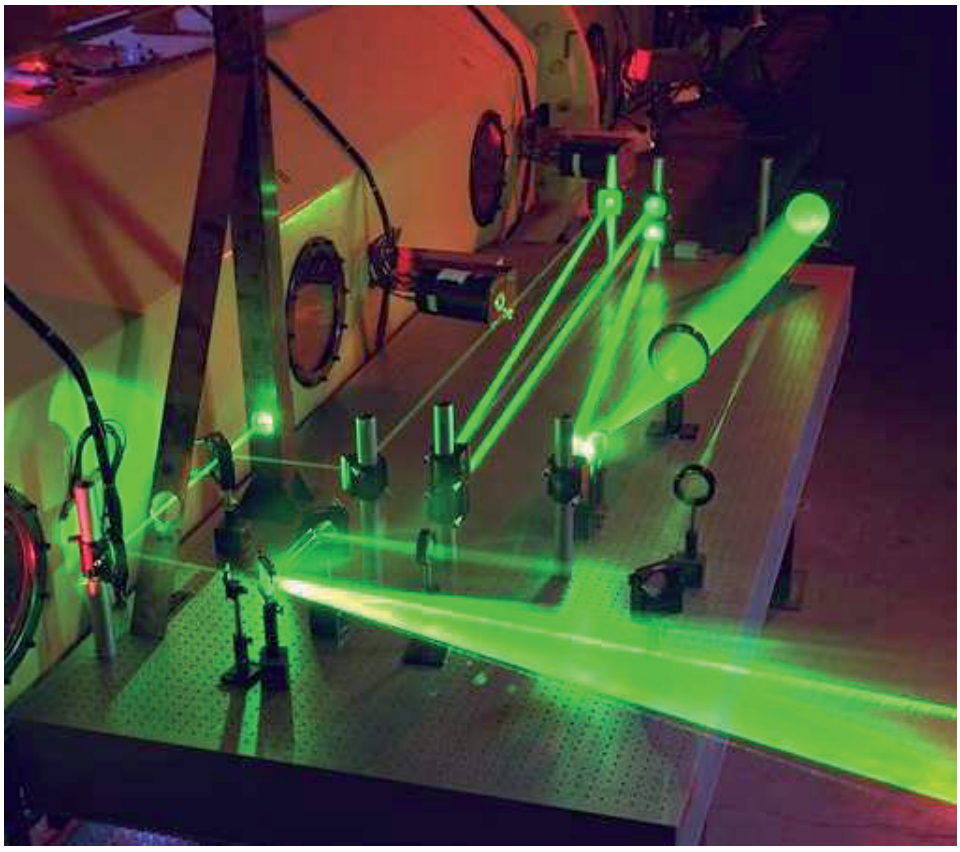
---

[249] L'algorithme ElGamal est un algorithme de cryptographie asymétrique basé sur les logarithmes discrets. Il a été créé par Taher Elgamal. Cet algorithme est utilisé par le logiciel libre GNU Privacy Guard, de récentes versions de PGP, et d'autres systèmes de chiffrement, et n'a jamais été sous la protection d'un brevet contrairement à RSA. Il peut être utilisé pour le chiffrement et la signature électronique. L'algorithme DSA du NIST est basé sur ElGamal.

[250] En algèbre générale et dans ses applications d'arithmétique modulaire, le logarithme discret est défini en théorie des groupes, par analogie avec le logarithme ordinaire.

[251] Don Coppersmith est un mathématicien et cryptologue américain. En 1972, il obtient un bachelor en mathématiques au Massachusetts Institute of Technology, suivi d'un master en 1975 et d'un doctorat en mathématiques à l'Université de Harvard en 1977.

La cryptographie quantique



La cryptographie quantique, une idée lumineuse

Les systèmes mis en place à l'heure actuelle pour protéger les communications des oreilles ou des regards indiscrets seront vulnérables à plus ou moins brève échéance, la puissance de calcul d'un simple ordinateur de bureau augmentant chaque jour. De plus les progrès mathématiques aidant, rien de prouve qu'on ne trouvera pas un algorithme suffisamment efficace, à terme, pour factoriser des grands nombres. Du reste, nous ne savons pas si ce n'est déjà le cas. En août 1999, un ordinateur a pu casser une clé de 512 bits d'un code RSA !

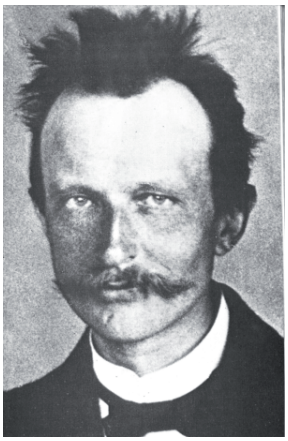
Il faudrait donc aller plus loin et imaginer un système dont les propriétés physiques seraient telles qu'il serait indéchiffrable, mais surtout « inécoutable » : on ne pourrait intercepter ou copier un message à l'insu des interlocuteurs... Certes, un tel système ne résoudrait pas tout, mais il découragerait pour un moment les éventuels curieux. Le temps des physiciens reviendrait-il ? Car n'oublions pas que les mathématiciens qui ont développé les procédés de codage actuels ne l'ont fait qu'en s'appuyant sur des procédés de transmissions inventés par des physiciens.

Cette technique pour rendre les communications inviolables existe. Non seulement en laboratoire, mais même au plan commercial, même s'il y a encore beaucoup de limites techniques à leur développement universel : c'est la cryptographie quantique.

Nous allons faire un petit tour dans ce monde en essayant de ne pas surcharger nos explications de mathématiques et nous ferons l'état des travaux et du développement industriel de ce procédé.

L'histoire a commencé en... 1900.

La physique quantique



Max Planck né le 23 avril 1858 à Kiel, est issu d'une famille nombreuse et bourgeoise. Ses arrière-grand-père et grand-père paternels sont professeurs de théologie, son père professeur de droit (il participa à la rédaction du Code civil allemand), tandis que sa mère est issue d'une famille de pasteurs.

En 1878, il soutient sa thèse de doctorat sur « le second principe de la thermodynamique » et la notion d'entropie[252] en perpétuelle augmentation. Ses professeurs ne sont guère convaincus. Il passe néanmoins son habilitation l'année suivante (1881) sur « les états d'équilibre des corps isotropes aux différentes

[252] En thermodynamique, l'entropie est une fonction d'état introduite en 1865 par Rudolf Clausius dans le cadre du second principe, d'après les travaux de Carnot. Clausius a montré que le rapport Q/T (où Q est la quantité de chaleur échangée par un système à la température T) correspond, en thermodynamique classique, à la variation d'une fonction d'état qu'il a appelée entropie, S et dont l'unité est le joule par kelvin (J/K). La thermodynamique statistique a ensuite fourni un nouvel éclairage à cette grandeur physique abstraite : elle mesure le degré de désordre d'un système au niveau microscopique. Plus l'entropie du système est élevée, moins ses éléments sont ordonnés, liés entre eux, capables de produire des effets mécaniques, et plus grande est la part de l'énergie inutilisée ou utilisée de façon incohérente. Boltzmann a formulé une expression mathématique de l'entropie statistique en fonction du nombre d'états microscopiques Ω définissant l'état d'équilibre d'un système donné au niveau macroscopique : formule de Boltzmann S = k Ln Ω. Cette nouvelle définition de l'entropie n'est pas contradictoire avec celle de Clausius. Les deux expressions de l'entropie résultent simplement de deux points de vue différents, selon que l'on considère le système thermodynamique au niveau macroscopique ou au niveau microscopique. Dans une période récente le concept entropie a été généralisé et a pénétré dans de nombreux domaines, tels que par exemple : l'entropie de Shannon dans le cadre de la théorie de l'information en informatique ; l'entropie topologique, ainsi que l'entropie métrique de Kolmogorov-Sinaï, dans le cadre de la théorie des systèmes dynamiques en mathématiques.

températures », aboutissant aux mêmes résultats que ceux obtenus auparavant par l'américain Josiah Willard Gibbs, dont les travaux étaient restés confidentiels.

Jusqu'en 1885, il recherche un poste d'enseignant en physique théorique, discipline peu à la mode à l'époque. Il obtiendra enfin un poste de professeur adjoint à Kiel en 1885.

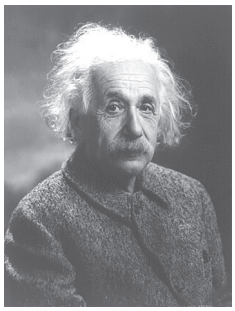
À la mort de Kirchhoff, et sur recommandation de Helmholtz, il est appelé à l'université de Berlin comme professeur adjoint puis titulaire en 1892. Un poste qu'il gardera pour environ quarante ans.

À Berlin, il poursuit des travaux en thermodynamique, en électromagnétisme et en physique statistique. Planck rejette, dans un premier temps, le modèle atomiste des gaz de Maxwell et Boltzmann. Pour lui, la théorie atomique s'effondrera à terme en faveur de l'hypothèse de la matière continue. Il se rallie devant l'évidence à l'atomisme à partir des années 1890.

À cette même époque, Lord Kelvin identifie le rayonnement du corps noir[253] comme l'un des problèmes à résoudre. Jožef Stefan, Ludwig Boltzmann, Wilhelm Wien s'y attaquent ainsi que Otto Richard Lummer, Ernst Pringsheim, Heinrich Rubens, Ferdinand Kurlbaum, Friedrich Paschen et Lord Rayleigh.

Travaillant à formuler avec exactitude le second principe de la thermodynamique, Planck s'intéresse dès 1894 au rayonnement électromagnétique du corps noir. Il adopte les méthodes statistiques de Boltzmann. En 1899, il introduit les constantes de Planck[254] (h) et de Boltzmann (k) en même temps que la notion des quanta[255]. En octobre 1900, il détermine la loi de répartition spectrale du rayonnement thermique du corps noir, sans en maîtriser l'interprétation physique.

C'est à la fin de 1900 qu'il présente sa découverte à la société de physique de Berlin. C'est la naissance de la théorie des quanta, à l'approfondissement de laquelle il participera peu, laissant Einstein l'étayer solidement. Planck a du mal à accepter sa propre hypothèse, rendant la matière « discontinue ». Il devient, par la suite, l'un des premiers soutiens d'Einstein, bien que ce dernier fut très critique vis-à-vis des théories de Planck avant de reconnaître ses positions novatrices.



Albert Einstein (14 mars 1879 à Ulm, Württemberg, Allemagne - 18 avril 1955 à Princeton, New Jersey, États-Unis) est un physicien allemand, puis apatride (1896), suisse (1899), et enfin helvético-américain (1940).

Il a publié la théorie de la relativité restreinte en 1905 et une théorie de la gravité dite relativité générale en 1915. Il a largement contribué au développement de la mécanique quantique et de la cosmologie. Il a reçu le prix Nobel de physique en 1921 pour son explication de l'effet photoélectrique. Son travail est notamment connu pour l'équation $E=mc^2$ qui quantifie l'énergie disponible dans la matière.

[253] En physique, un corps noir désigne un objet idéal dont le spectre électromagnétique ne dépend que de sa température. En pratique, un tel objet matériel n'existe pas, mais il représente un cas idéalisé servant de référence pour les physiciens. Contrairement à ce que son nom suggère, un corps noir n'apparaît pas forcément noir. En effet l'adjectif « noir » signifie ici que l'objet lui-même absorbe toute la lumière extérieure qui tomberait sur lui, et ne reflète aucune radiation non plus. La seule radiation provenant du corps noir est la radiation thermique, ne dépendant que de la température du corps. Le nom corps noir a été introduit par le physicien Gustav Kirchhoff en 1860. Le modèle du corps noir permit à Max Planck de découvrir la quantification des interactions électromagnétiques, qui fut un des fondements de la physique quantique.

[254] En physique, la constante de Planck, notée h, est une constante utilisée pour décrire la taille des quanta. Elle joue un rôle central dans la mécanique quantique et a été nommée d'après le physicien Max Planck. La constante de Planck relie notamment l'énergie d'un photon à sa fréquence ν (lettre grecque nu) : $E=h\nu$

[255] Un quantum (mot latin signifiant « combien » et qui s'écrit « quanta » au pluriel) représente la plus petite mesure indivisible, que ce soit celle de l'énergie, de la quantité de mouvement ou de la masse. Cette notion est centrale en théorie des quanta, laquelle donnera naissance à la mécanique quantique.

La mécanique quantique

Fille de l'ancienne théorie des quanta, la mécanique quantique constitue le pilier d'un ensemble de théories physiques qu'on regroupe sous l'appellation générale de physique quantique. Cette dénomination s'oppose à celle de physique classique, celle-ci échouant dans sa description du monde microscopique — atomes et particules — ainsi que dans celle de certaines propriétés du rayonnement électromagnétique.

Les principes fondamentaux de la mécanique quantique ont été établis essentiellement entre 1922 et 1927 par Bohr, Dirac, de Broglie, Heisenberg, Jordan, Pauli et Schrödinger. Ils permettent une description complète de la dynamique d'une particule massive non relativiste. Bohr a proposé une interprétation du formalisme, appelée interprétation de Copenhague, fondée sur le principe de correspondance.

Les principes de base ont été complétés par Bose et Fermi afin d'autoriser la description d'un ensemble de particules identiques, ouvrant la voie au développement d'une physique statistique quantique. Enfin, en 1930, le mathématicien Von Neumann a précisé le cadre mathématique rigoureux de la théorie. La théorie quantique des champs est l'une de ses extensions relativistes les plus utilisées au XXIe siècle.

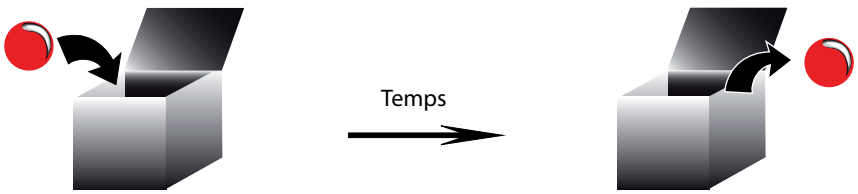
La mécanique quantique a repris et développé l'idée de dualité onde-particule introduite par de Broglie en 1924 consistant à considérer les particules de matière non pas seulement comme des corpuscules ponctuels, mais aussi comme des ondes, possédant une certaine étendue spatiale. Bohr a introduit le concept de « complémentarité » pour résoudre cet apparent paradoxe : tout objet physique est bien à la fois une onde et un corpuscule, mais ces deux aspects, mutuellement exclusifs, ne peuvent être observés simultanément. Si l'on observe une propriété ondulatoire, l'aspect corpusculaire disparaît. Réciproquement, si l'on observe une propriété corpusculaire, l'aspect ondulatoire disparaît.

En 2007, aucune contradiction n'a pu être décelée entre les prédictions de la mécanique quantique et les tests expérimentaux associés. Ce succès a hélas un prix : la théorie repose sur un formalisme mathématique abstrait, qui rend son abord assez difficile. Nous allons, ci-dessous, expliquer, sans mathématiques, le fonctionnement de l'information quantique avant d'en voir les applications en cryptographie.

L'information quantique

En informatique l'information circule sous forme de bit (de l'anglais *binary digit*). Un bit peut prendre deux valeurs : soit 0, soit 1. Pour notre présentation de l'information quantique, nous allons définir, arbitrairement, que le 0 sera une balle rouge et le 1 une balle verte.

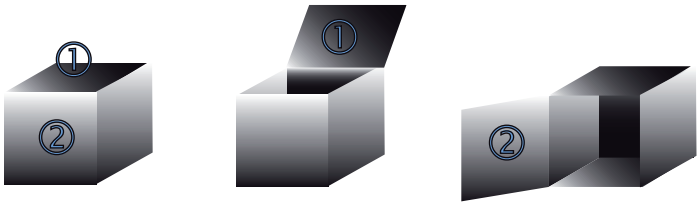
Les bits (balles) sont précieux et nous désirons les protéger au mieux possible. Pour ce faire, nous placerons nos bits dans des boîtes, une balle par boîte. Par exemple, imaginons que nous avons une balle rouge à laquelle nous tenons beaucoup. Nous la plaçons donc dans une boîte afin de la protéger de tout problème, de toute rencontre malheureuse (nous ne voudrions pas, par exemple, que quelqu'un la peigne en vert). Ainsi, on garde notre balle en sécurité jusqu'à ce que, plus tard, nous en ayons besoin et la sortions de la boîte. Évidemment, puisqu'une balle rouge est entrée, une balle rouge sortira avec certitude :



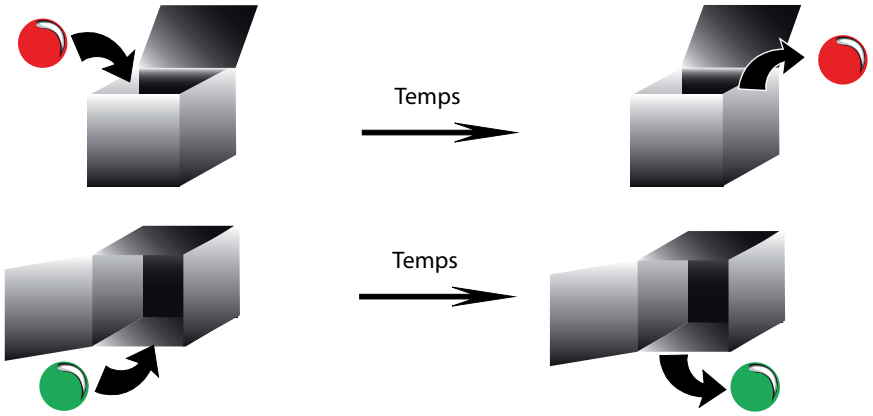
Cette remarque apparemment anodine met en évidence une propriété fondamentale de l'information classique : lire l'information classique n'en change pas la valeur (évidemment !). De ce fait, l'information classique (les balles) peut facilement être copiée. De plus, on peut facilement et efficacement protéger l'information classique contre les erreurs.

Bien sûr, les bits sont vraiment utiles (sans bits, vous ne pourriez lire ce texte !) mais leurs propriétés ne sont pas vraiment surprenantes et excitantes. Considérons plutôt les propriétés de l'information si cette information devait suivre les règles étranges de la mécanique quantique.

Nous nommerons l'unité fondamentale de l'information quantique le bit quantique ou, plus simplement, qubit (de l'anglais *quantum bit*). Comme sa contrepartie classique, un qubit peut prendre deux valeurs que l'on représente à nouveau par des balles rouges ou vertes. Ce ne sont toutefois pas des balles ordinaires : ce sont des ***quballes***[256] ! Ces quballes sont très précieuses et nous désirons les protéger de tout problème potentiel. Ainsi, comme dans le cas des balles classiques, nous placerons les quballes dans des boîtes. Il y a une différence importante ici toutefois : pour prendre en compte les propriétés étranges des quballes, nous aurons besoin de boîtes munies de deux portes.

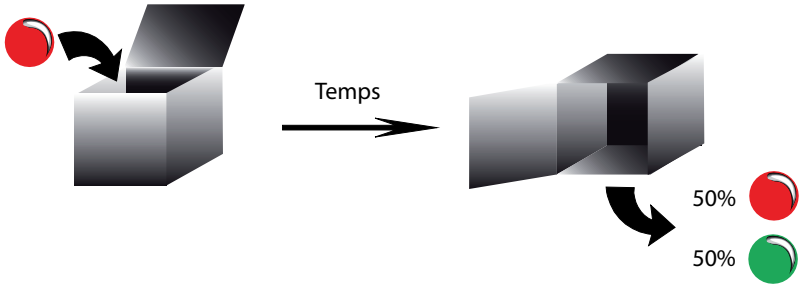


Comme dans le cas classique, si l'on place une quballe rouge dans la boîte par la porte #1 et que, à un temps ultérieur, nous ouvrons cette même porte, nous verrons évidemment une quballe rouge (la même chose tient aussi pour les quballes vertes). De la même façon, si l'on place une quballe rouge (ou verte) par la porte #2 et que l'on ouvre plus tard cette porte, nous verrons une quballe rouge (ou verte).



Étrangeté quantique

Intéressons-nous maintenant à une expérience qui n'était pas possible dans le cas classique où nous n'avions qu'une seule porte. Plaçons premièrement une quballe rouge par la porte #1 et, plutôt que de regarder le contenu de la boîte par cette même porte, nous ouvrons maintenant la porte #2 :



[256] Nous utilisons ce nom pour cette démonstration. Ce n'est en aucun cas une expression « officielle » !

Dans ce cas, nous ne verrons pas nécessairement un quballe rouge. Nous verrons soit rouge, soit vert ! Plus précisément, si nous répétons cette même expérience plusieurs fois, nous observerons que dans 50% des cas le résultat est rouge et dans l'autre 50%, vert. Le résultat est donc complètement aléatoire et ne dépend pas de la couleur initiale de la quballe (rouge ici).

Ce résultat est étrange et il est utile de résumer rapidement ce que nous avons vu jusqu'à présent. Si l'on place une quballe par une porte et, à un temps ultérieur, nous ouvrons cette même porte, nous verrons une quballe de couleur identique. Toutefois, si l'on place une quballe par une porte donnée (disons #1) et ouvrons l'autre (ici #2) le résultat peut être soit vert soit rouge, et ce, peu importe la couleur initiale de la balle. Tout ceci est étrange et demande une explication.

L'interprétation donnée à ce phénomène par les physiciens est que, lorsqu'une quballe est préparée d'une certaine façon (par une certaine porte) avant que l'on regarde par cette même porte, la quballe est comme nous l'avions initialement préparée (même couleur). Ainsi, lorsque l'on regarde par cette même porte, le résultat est celui auquel on est en droit de s'attendre : la couleur initiale. Par contre, si l'on prépare notre quballe par une certaine porte (disons encore #1), avant que l'on regarde par l'autre porte (du point de vue de l'autre porte, ici #2) notre quballe est à la fois rouge et verte ! De ce fait, lorsque l'on ouvre cette porte (ici #2) nous obtenons soit rouge ou vert avec une probabilité 1/2. Les physiciens appellent cette étrange situation (lorsqu'une quballe est simultanément rouge et verte) une ***superposition quantique*** : nous dirons donc que dans ce cas une quballe est dans la superposition des couleurs rouge et verte.

De plus, après avoir ouvert la porte et observé, par exemple, une quballe verte alors la quballe n'est plus dans une étrange superposition d'états, c'est une quballe verte et c'est tout. L'action d'ouvrir la boîte et de regarder la quballe a donc perturbé son état, cela a détruit la superposition ! Il n'y a aucune analogie pour cela avec les balles régulières, classiques.

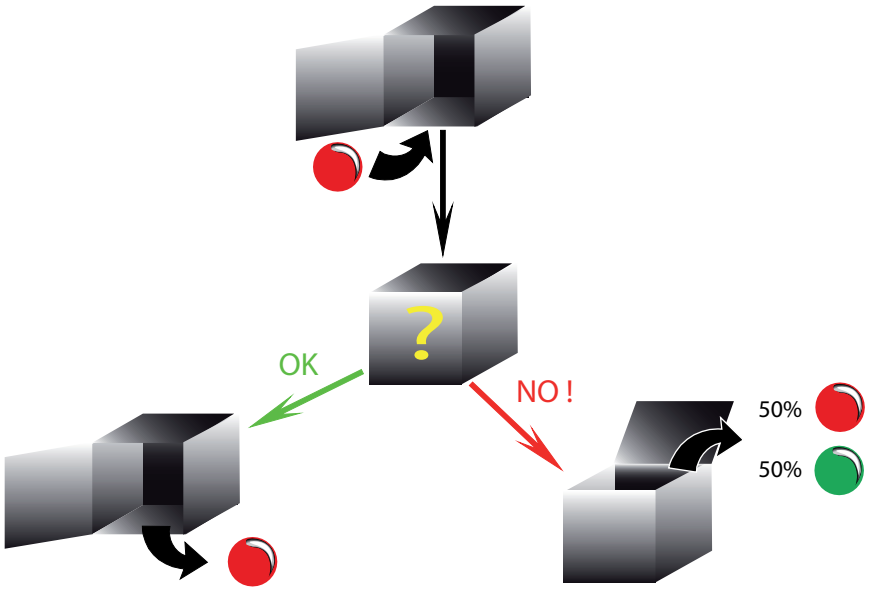
Vous n'êtes probablement pas satisfait de cette « explication » concernant les superpositions d'états et la perturbation résultant d'une mesure. Rien n'a été dit sur le fait que, dans une expérience donnée, nous obtenons une quballe rouge et dans une seconde expérience une quballe verte alors que la préparation et les conditions expérimentales sont les mêmes dans les deux cas. En fait, est-ce que l'on pourrait prédire pour toutes préparations et mesures quelle sera la couleur de la quballe ? Malheureusement, la réponse à ces questions est qu'il n'y a simplement pas d'explication pour cela. Ce comportement étrange des quballes est tout ce que la mécanique quantique nous dit. La théorie quantique ne nous donne aucun outil pour prédire le résultat d'une expérience donnée, elle ne nous donne accès qu'à des probabilités. En d'autres mots, la mécanique quantique nous permet de prédire les statistiques reliées à un grand nombre de mesures mais ne peut rien nous dire de plus à propos d'une mesure particulière. De même, la théorie quantique nous donne peu d'intuition sur la signification d'une superposition d'états et sur ce que cela veut dire pour une balle d'être à la fois rouge et verte.

Ce que l'on sait toutefois est que si l'on applique les règles étranges de la mécanique quantique (les superpositions et les probabilités) pour expliquer ce que l'on observe de la nature, nous obtenons de très bons résultats. En fait, la théorie quantique est la théorie ayant le plus grand succès comparativement à toute autre théorie en physique. Ceci devrait être une raison suffisante pour accepter ces règles étranges et continuer à nous intéresser à leurs conséquences sur l'information et son traitement.

Conséquence : copie interdite

Attardons-nous maintenant à une première conséquence de ces règles étranges : l'impossibilité de copier l'information quantique. Pour ce faire, considérons le jeu suivant : Alice prépare une quballe sans montrer ou dire à Bob comment elle le fait (par quelle porte et avec quelle couleur). Elle donne ensuite la boîte contenant la précieuse quballe à Bob et lui demande d'en faire une copie. Il gagne s'il réussit.

Considérons par exemple le cas où Alice place dans la boîte une balle verte par la porte #2. Elle donne ensuite la boîte fermée à Bob (celui-ci reçoit donc la boîte marquée d'un point d'interrogation) :



Pour faire une copie, Bob doit évidemment connaître l'état (couleur) de la quballe. Afin d'obtenir cette information, il doit ouvrir la boîte et regarder à l'intérieur. S'il ouvre la porte #2, il voit une quballe verte et il peut dès lors en faire une copie conforme : il gagne la partie. Toutefois, si le malheureux ouvre plutôt la porte #1, il verra avec probabilité 1/2 une quballe de la mauvaise couleur et produira une copie incorrecte. Il y a donc une certaine probabilité pour que l'opération de copie échoue.

Ce résultat est plus frappant lorsque l'on réalise que, sans l'aide d'Alice, Bob ne peut savoir s'il a fait une copie conforme à l'originale ou non, et ce, simplement car il n'a aucune façon de savoir s'il a ouvert la bonne porte. Puisque l'on ne peut copier ce que l'on ne connaît pas, on doit en conclure qu'il est impossible de copier l'information quantique avec une grande probabilité de succès.

Pour certaines applications (comme la protection de l'information quantique contre les erreurs, la correction quantique d'erreurs, où nous aimerions faire plusieurs copies d'un qubit pour le protéger) cette propriété est très gênante. Dans d'autres circonstances, comme la cryptographie quantique, cela s'avère très utile.

Opérations quantiques

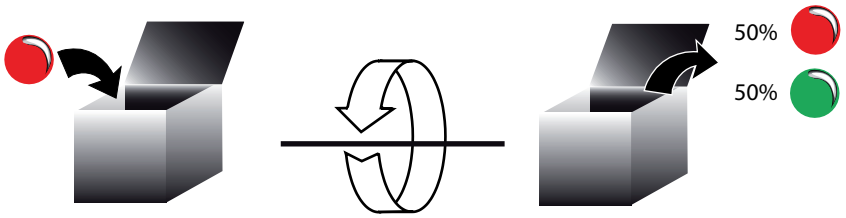
Comme nous le savons, les bits sont tout ce qui compte pour un ordinateur. Les bits encodent l'information sur votre disque dur, l'unité centrale (CPU) de votre ordinateur traite des bits lorsqu'il exécute des logiciels et ce sont aussi des bits qui sont traités par votre carte graphique ou votre imprimante.

Imaginez maintenant un ordinateur qui n'utilise pas des bits, mais des qubits : un ordinateur quantique. Est-ce qu'une telle bête serait utile ? Est-ce qu'elle pourrait être plus puissante qu'un ordinateur utilisant des bits réguliers ? La réponse à ces deux questions est affirmative. Avant de présenter pourquoi tel est le cas, expliquons d'abord comment il est possible de manipuler des qubits ou, en d'autres mots, comment on peut appliquer des opérations logiques sur ceux-ci.

Le but de toute opération logique, est de changer la valeur des qubits d'une façon contrôlée. Une opération intéressante à réaliser avec des qubits est de créer des superpositions d'états. Comment faire cela ? Comme vu précédemment, nous savons que si l'on prépare une quballe par la porte #1, avant d'ouvrir quelques portes que ce soit, la quballe est, du point de vue de la porte #2, dans une superposition d'états :

si l'on ouvrait la porte #2, nous verrions rouge ou vert avec une probabilité égale. Nous savons donc comment préparer des superpositions d'états.

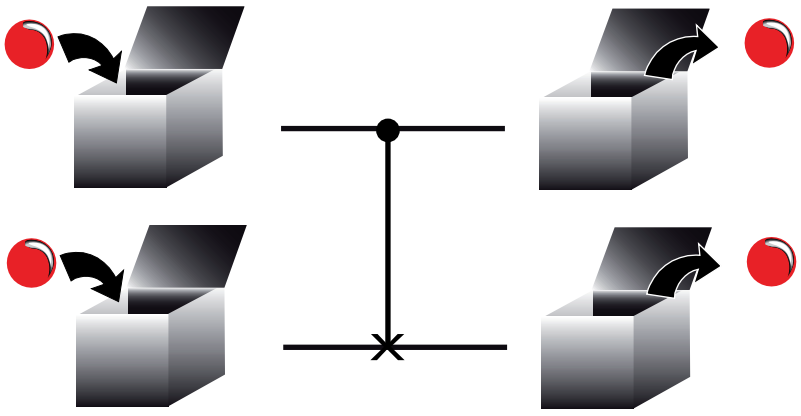
Mais imaginons que nous ayons accès seulement à la porte située au-dessus de la boîte. Comment procéder alors ? Une solution simple est de préparer la quballe par la porte #1 (qui est initialement au-dessus) puis effectuer une rotation de la boîte de façon à ce que la porte #2 soit maintenant au-dessus (une rotation de 90°). Nous avons alors une superposition d'états du point de vue de la porte du dessus :



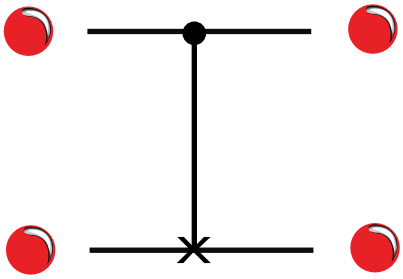
Dans l'image ci-dessus, la quballe à gauche représente l'état initial et celle de droite l'état final. Le diagramme entre ces dernières représente l'opération appliquée sur la quballe initiale. Il s'agit ici d'une rotation qui est représentée par la flèche circulaire.

Cette rotation peut sembler bien superflue, mais ce n'est pas le cas : en pratique, et pour des raisons qui dépassent le cadre de ce texte d'introduction, nous aurions accès seulement « à la porte du haut » dans un ordinateur quantique réel. Cette rotation est donc similaire à ce qui serait vraiment utilisé par un tel ordinateur et c'est ce que nous utiliserons dans ce texte pour préparer des superpositions d'états.

Décrivons maintenant une opérations logiques, ou porte logique, qui est très utile dans la manipulation de l'information quantique : le Non-Controlé (ou *CNOT* de l'anglais *controlled-not*). Contrairement à la rotation que nous venons de voir, cette porte agit sur deux quballes :



De la même façon que ci-dessus, les quballes sur la gauche représentent l'état initial et ceux à la droite le résultat de l'application du CNOT. On représente graphiquement le CNOT par une ligne verticale débutant par un cercle pour se terminer par un x. Puisque nous ne considérerons que la porte du haut par la suite, nous pouvons tout aussi bien omettre de dessiner la boîte. On représentera donc le CNOT comme ceci :



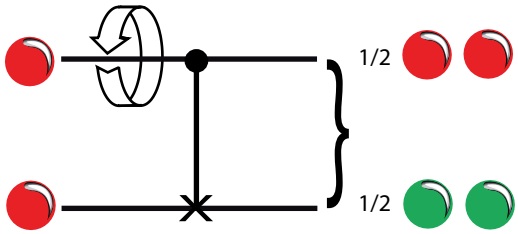
En utilisant cette notation, l'action du Non-Controlé sur les quatre arrangements de couleurs possibles de 2 quballes est résumée par le tableau suivant :

Entrée	Sortie

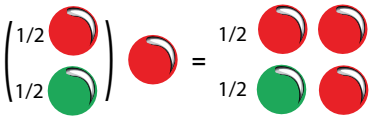
L'action du CNOT est donc d'inverser la couleur de la seconde quballe (ligne du bas dans le diagramme et quballes de droite dans chacune des colonnes du tableau) seulement si la première est verte.

Circuits quantiques

Il est utile de placer plusieurs portes quantiques une à la suite de l'autre afin de réaliser des opérations logiques plus complexes. Considérons par exemple le circuit suivant avec 2 balles rouges comme état initial :



La première étape est une rotation de 90° et a pour effet de créer une superposition d'états pour la première quballe. Suite à cette rotation, les deux quballes sont alors dans l'état :



La première quballe est donc simultanément rouge et verte tandis que la seconde est rouge avec certitude (mais après tout, nous n'avons pas encore appliqué d'opérations sur cette quballe).

Maintenant, appliquons un CNOT sur ce nouvel état à deux quballes. Comme on peut le vérifier à partir de la table de vérité correspondante à cette opération, la combinaison rouge-rouge reste inchangée tandis que vert-rouge devient vert-vert. L'état est donc :

Le résultat de ce circuit sur l'état rouge-rouge est une superposition d'états très spéciale, une superposition de deux quballes plutôt que d'une seule comme vu jusqu'à maintenant. Pour cette superposition, les quballes sont simultanément toutes deux rouges et toutes deux vertes ! Ce résultat est plutôt étrange, mais c'est ce que l'on obtient en appliquant les lois de la mécanique quantique.

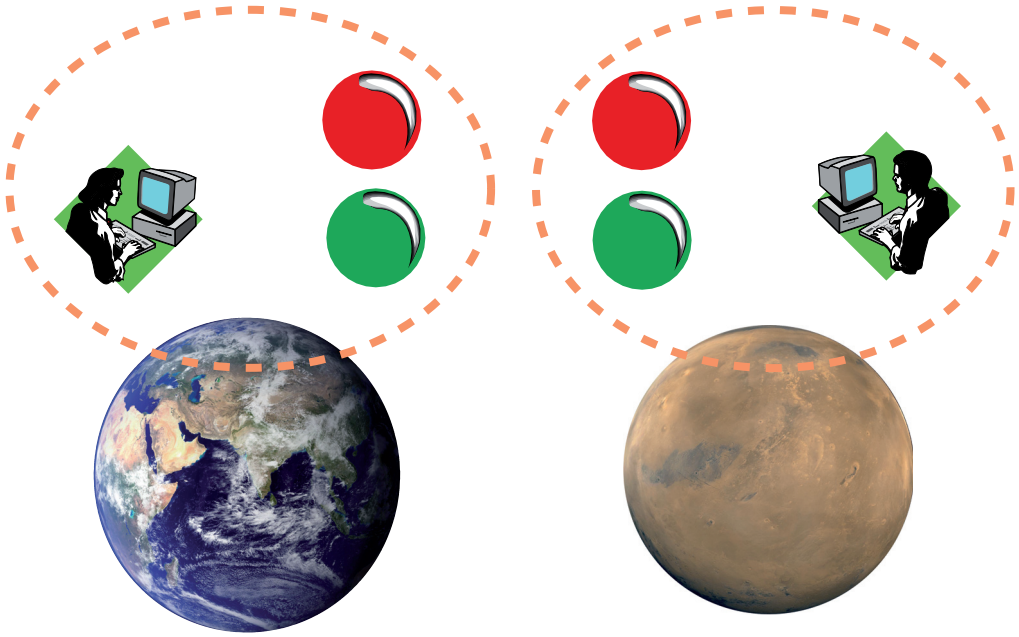
Maintenant, quels sont les résultats possibles lors d'une mesure ? Suivant ce que l'on a appris plus tôt, nous savons que les résultats possibles sont soit deux balles rouges ou deux balles vertes. Ceci veut dire que si l'on ne regarde qu'une seule quballe, nous connaissons immédiatement la couleur de l'autre : ce sera la même couleur que celle observée.

Que les quballes soient de la même couleur après l'application du circuit ci-dessus est vraiment surprenant. En fait, cette situation est tellement spéciale et intéressante que l'on a un nom particulier pour désigner cette situation; on dit que les quballes sont ***enchevêtrées***.

Enchevêtrement, Intrication quantique

Intéressons-nous davantage à l'état à deux quballes préparées à la dernière section afin de comprendre ce qu'il y a de si particulier.

Imaginons que deux quballes, initialement rouges, sont partagées entre Alice et Bob : Alice a la première et Bob la seconde. Ensemble, ils appliquent le circuit décrit à la section précédente. Comme nous le savons, leurs quballes sont maintenant dans une superposition rouge-rouge et verte-verte. Après cette préparation, Alice reste dans son laboratoire sur la Terre tandis que Bob part pour une croisière vers Mars.



Lorsque Bob est arrivé à destination, Alice décide de mesurer sa quballe et elle obtient le résultat rouge. De la discussion précédente, il est clair que, immédiatement, la quballe de Bob est rouge elle aussi : si Bob mesurait sa quballe, il obtiendrait rouge avec certitude. Que s'est-il passé ici ? Une action par Alice sur la Terre a eu une conséquence immédiate sur Mars. Il semble donc qu'un signal soit parti de la balle d'Alice pour se rendre instantanément vers la quballe de Bob afin de l'informer sur la couleur qu'elle doit prendre à partir de ce moment. Ceci est vraiment très étrange, car selon la théorie de la relativité restreinte développée par Einstein en 1905, aucune information ne peut se propager à une vitesse supérieure à la vitesse de la lumière (si le signal est allé instantanément de la Terre vers Mars, il allait certainement plus rapidement que la vitesse de la lumière).

Ce résultat est tellement intrigant qu'en 1935, Einstein, Podolsky et Rosen ont argumenté, en utilisant un scénario similaire dans le principe, que si la mécanique quantique prédit des résultats aussi étranges, elle doit certainement être incomplète et ne peut décrire correctement la nature. Ceci est maintenant connu sous le nom du *paradoxe EPR*[257].

[257] Le paradoxe EPR permet la transmission d'informations plus vite que la vitesse de la lumière. L'enchevêtrement des particules permet, dans certaines circonstances, que deux particules conservent un lien causal, peu importe la distance les séparant : ce qui advient à l'une advient nécessairement à l'autre avec une simultanéité parfaite. Cela veut dire que si on mesure les propriétés d'une des deux particules, on peut connaître automatiquement les propriétés de sa jumelle éloignée, ce qui

Heureusement pour les ordinateurs quantiques et malheureusement pour Einstein et ses collaborateurs, des expériences ont montré que l'enchevêtrement est un phénomène bien réel et présente le comportement étrange décrit ici. Il semble donc que la mécanique quantique est une bonne description de la nature. Il est important de mentionner que la relativité restreinte n'est pas violée dans le scénario présenté ci-dessus parce qu'il n'y a pas d'échange d'informations entre les quballes : il n'y a aucun moyen pour Alice et Bob d'utiliser seulement leurs deux quballes enchevêtrées pour échanger de l'information.

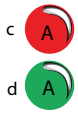
Même s'il n'est possible d'échanger de l'information en utilisant seulement des paires de quballes enchevêtrées (nous appellerons aussi cela une paire EPR), ces états sont certainement utiles. Comme nous le verrons plus loin, ce sont les paires EPR qui rendent les ordinateurs quantiques puissants. Les paires EPR rendent aussi possible la téléportation quantique.

Téléportation quantique

Imaginons qu'Alice veuille donner une quballe bien particulière à Bob (qui est encore sur Mars). Malheureusement, quelqu'un d'autre a préparé cette quballe et elle ne connaît pas les détails de cette préparation. De ce fait, elle ne peut pas simplement dire à Bob comment préparer une quballe identique seulement en parlant avec lui sur le téléphone interplanétaire. De même, cette quballe est très précieuse et Alice n'a aucune confiance dans le service de poste interplanétaire (évidemment, le vrai problème avec cette option est que les officiers des douanes insisteront pour ouvrir la boîte détruisant ainsi l'état de la quballe...).

Heureusement, ils ont toujours en leur possession une paire EPR préparée lors de leur dernière rencontre. Utilisant cette paire, Alice pourra faire parvenir sa précieuse quballe à Bob grâce à la ***téléportation quantique***[258]. Décrivons maintenant comment cela est possible.

Nous verrons comment ces règles étranges de la théorie quantique peuvent s'avérer utiles en mettant à profit tout ce que nous avons vu jusqu'à présent. Il s'agit de la partie la plus technique de ce texte, nous procéderons donc étape par étape. Premièrement, la quballe d'Alice peut être dans n'importe quel état : elle peut être rouge, verte ou les deux. Afin d'être aussi général que possible, nous la représenterons par la superposition suivante :

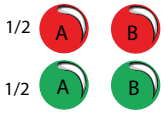


Ceci est très général. Par exemple, le cas où c=1 et d=0 représente une quballe rouge. A l'opposé, c=0 et d=1 représente une quballe verte. L'autre possibilité déjà rencontrée est c=d=1/2, ce qui représente une superposition de rouge et vert. Nous insistons sur le fait que cette quballe appartient à Alice en ajoutant l'indice A sur celle-ci (un B signifie plutôt que la quballe appartient à Bob).

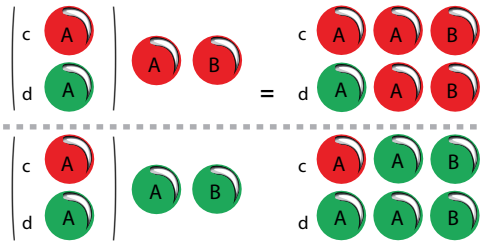
implique que les particules gardent un lien de communication instantané. Or, cela semble contredire la relativité restreinte d'Einstein qui dit qu'aucune communication ne peut dépasser la vitesse de la lumière. C'est pourquoi Einstein appelait ce phénomène « action fantôme à distance ».

[258] La première démonstration expérimentale de l'intrication fut effectuée à l'université d'Innsbruck (en Autriche) en 1997, par le groupe de Anton Zeilinger. Leur configuration permit de téléporter l'état quantique de polarisation à travers une table optique. Une expérience ayant eu lieu quelque temps plus tôt à Rome, par le groupe de De Martini, avait montré le principe de la téléportation, mais en impliquant seulement deux particules, au lieu de trois : une transportant l'information à téléporter, et deux particules intriquées, qui fournissent le canal quantique et doivent être indépendantes de celle transportant l'état. En 2004, un autre groupe de recherche à l'université d'Innsbruck et un groupe au NIST démontra la téléportation d'atomes : l'état quantique électronique d'un ion de Calcium fut téléporté vers un autre, l'ensemble des ions étant contenu dans un piège à ions linéaire. Le 2 juillet 2006, des physiciens à l'Université de Genève ont à nouveau réussi à réaliser une opération de téléportation quantique, en utilisant les propriétés d'intrication des photons, au sein de fibres optiques longues de 800 mètres appartenant à Swisscom.

De même, comme nous l'avons déjà dit, Alice et Bob doivent se partager une paire EPR :



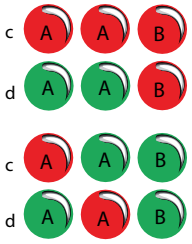
Les indices nous apprennent que la première quballe appartient à Alice et la seconde à Bob. Un aspect nouveau de cet exemple est que l'on ne traite pas seulement d'une ou deux quballes, mais bien de trois (la quballe qu'Alice aimerait faire parvenir à Bob et les deux quballes de la paire EPR).



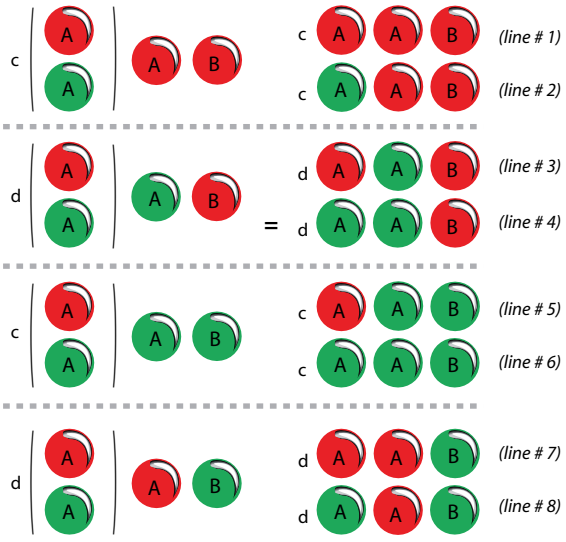
Écrivons donc l'état décrivant complètement l'état du système. Nous avons vu comment faire cela à la section « *Circuits Quantiques* ». Il y a deux possibilités pour la première quballe et deux pour la paire EPR. Il y a donc 2x2=4 possibilités pour les trois quballes (schéma à droite) :

Les facteurs 1/2 de la paire EPR n'ont pas été explicitement écrits et la ligne horizontale n'est qu'un guide pour les yeux. La description complète du système est donc que les trois quballes sont dans une superposition de 4 configurations différentes de couleurs.

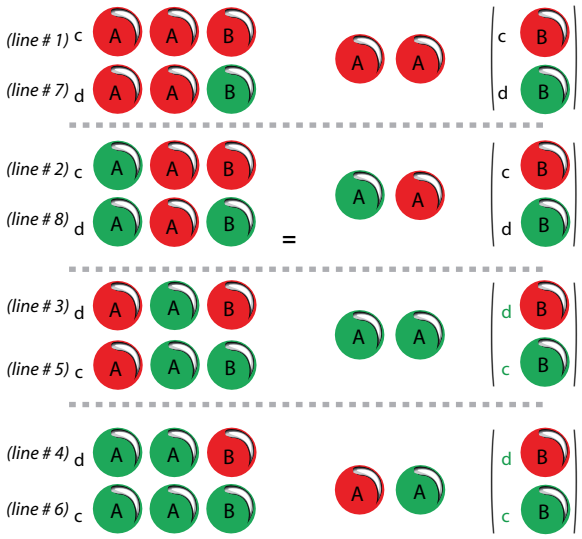
Alice fait maintenant un Non-Controlé sur ses quballes. En appliquant les règles données par la « Table de Vérité » de cette opération (inverse la couleur de la seconde quballe seulement si la première est verte), le résultat est :



Évidemment, seulement la seconde quballe d'Alice à été affectée par cette opération (quballe du centre). Ceci fait, Alice applique maintenant une rotation de 90° sur sa première quballe (la plus à gauche dans chaque ligne). La représentation de l'état sera maintenant un peu plus lourde puisque, comme nous l'avons déjà vu, une telle rotation amène une quballe dans une couleur spécifique vers une superposition des deux couleurs possibles. Nous avions une superposition de 4 configurations, nous aurons maintenant une superposition de 2X4=8 états puisque la première quballe (la plus à gauche) est maintenant soit rouge ou verte :



Heureusement, nous avons presque terminé ! Une observation essentielle ici pour compléter la téléportation est que cette superposition de huit configurations différentes de couleurs a une structure bien particulière : il y a deux configurations (lignes) où les quballes d'Alice sont toutes deux rouges (la première et la septième), deux lignes où elles sont respectivement vertes et rouges (lignes 2 et 8), deux où elles sont respectivement rouge et verte (ligne 3 et 5) et finalement deux où les deux quballes d'Alice sont vertes (lignes 4 et 6). Afin de rendre cette structure plus explicite, réarrangeons les lignes de la superposition de façon à rendre ces paires de lignes voisines :



Du membre de droite de l'égalité ci-haut, il apparaît que, correspondant à chacune des quatre configurations de couleurs des deux quballes d'Alice, correspond une superposition de la quballe de Bob. Quand les deux quballes d'Alice sont rouge-rouge ou verte-rouge alors la quballe de Bob est exactement dans l'état de la quballe qu'Alice voulait lui faire parvenir ! Toutefois, lorsque les quballes d'Alice sont soit rouge-verte ou verte-verte, la quballe de Bob est presque correcte : seulement les coefficients 'c' et 'd' sont interchangés (on insiste sur cela dans la figure en écrivant ces coefficients d'une couleur différente). Cette correspondance entre les quballes d'Alice et Bob est une manifestation que ces trois quballes sont maintenant enchevêtrées.

Afin de compléter la procédure, Alice mesure ces quballes. Il y a quatre résultats possibles : les quatre configurations possibles des deux quballes telles que présentées à la figure précédente. Évidemment, puisque les quballes d'Alice sont enchevêtrées avec celle de Bob, la quballe de Bob après la mesure va être dans l'état associé au résultat d'Alice (voir l'image).

Comme nous l'avons déjà mentionné, dans deux des résultats possibles de la mesure, la quballe de Bob est exactement dans l'état qu'Alice voulait lui faire parvenir ! Malheureusement, pour les deux autres résultats possibles, l'état n'est pas le bon : les coefficients sont interchangés. Afin de régler cette situation, Alice doit dire à Bob quelles couleurs elle a obtenues lors de la mesure. Bob sait alors si les coefficients sont les bons ou non. S'ils sont les bons, la procédure est terminée. S'ils sont inversés, alors il peut échanger une quballe rouge par une verte et une verte par une rouge (un peu de la même façon qu'un Non-Controlé échange une quballe rouge pour une verte). La téléportation est alors complétée : Alice a réussi à « donner » à Bob une quballe dans l'état exact qu'elle désirait sans jamais avoir à lui envoyer cette quballe particulière. Voilà pourquoi cette procédure est nommée téléportation.

Il est important de mentionner que pour compléter le transfert, Alice doit appeler Bob par le téléphone interplanétaire et lui dire les résultats de ses mesures. Sans cet appel, Bob n'aurait aucune façon de savoir si sa quballe est dans le bon état ou non. De ce fait, toute la procédure serait inutile. Évidemment, parler sur le téléphone interplanétaire prend beaucoup de temps (rappelons-nous que l'information ne peut voyager à une vitesse plus grande que celle de la lumière) ceci veut dire que la téléportation en entier ne peut être réalisé instantanément. Einstein serait satisfait de cette conclusion puisqu"elle signifie que la téléportation quantique ne viole pas la relativité restreinte.

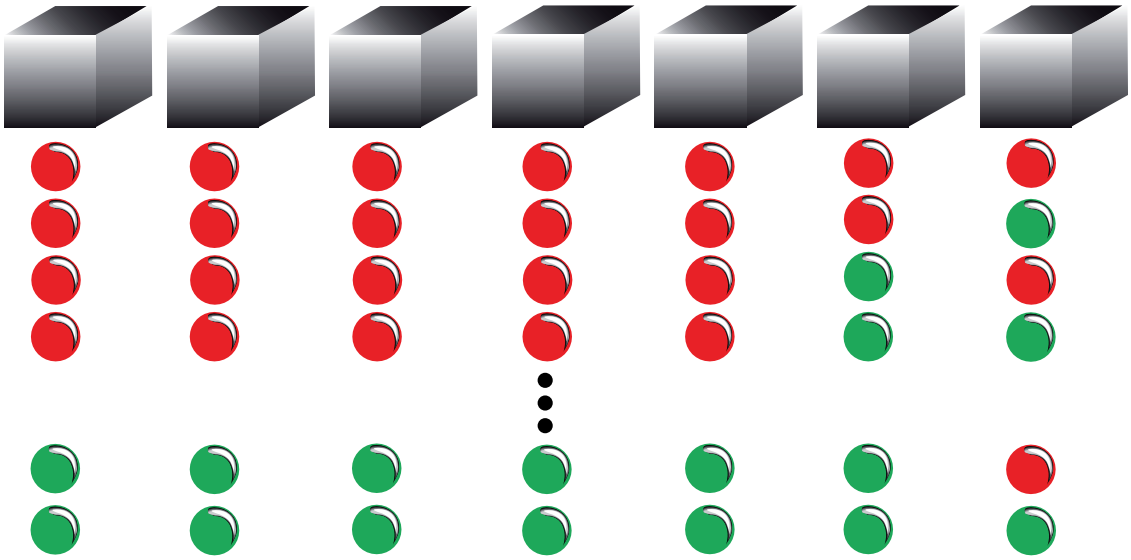
La téléportation quantique n'est pas seulement un rêve de théoricien, mais a été réalisée expérimentalement, utilisant des photons et des spins nucléaires plutôt que des balles toutefois.

L'application de cette technique à des objets plus gros, comme des humains, est par contre encore bien loin si jamais cela devient réalité...

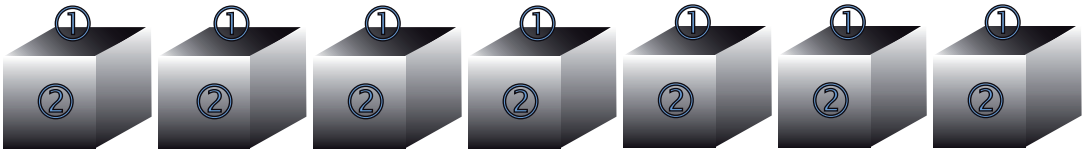
Ordinateurs classiques et ordinateurs quantiques

Une chose que nous avons apprise jusqu'à présent est comment les quballes sont différentes des balles ordinaires, comment l'information quantique est différente de l'information classique. Une des motivations pour étudier ces différences était de savoir si un ordinateur suivant les règles de la mécanique quantique pourrait être utile et peut-être même plus puissant qu'un ordinateur régulier, classique. Il est maintenant temps de répondre à cette question, mais, tout d'abord, regardons le cas classique qui nous est déjà familier.

Imaginons un ordinateur classique (comme un PC) mais ayant seulement 7 bits (ce qui est beaucoup moins que les milliards de bits dans les CPUs modernes !). Encore une fois, on représente ces 7 bits par des balles. Il y a plusieurs configurations de couleurs pour ces 7 balles :



Il y a un total de 2x2x2x2x2x2x2 = 128 arrangements pour 7 bits. Puisque chaque bit ne peut être que rouge ou vert (et non pas simultanément les deux couleurs) alors l'état de cet ordinateur classique est très simple à décrire : chacune de ces 128 configurations de couleurs est mutuellement exclusive et tout ce qui est nécessaire pour représenter complètement l'état de l'ordinateur est 7 bits (évidemment, nous avons un ordinateur à 7 bits alors ceci n'est pas bien difficile à comprendre !). Il s'agit d'une observation bien simple, mais elle sera utile pour bien comprendre la différence avec le cas quantique.



Imaginons un ordinateur quantique à 7 qubits. Comme dans le cas classique, il y a 128 configurations possibles de 7 quballes. Ici toutefois la description n'est plus simple du tout. Dans le cas quantique, on ne peut dire qu'une quballe particulière est soit rouge soit verte puisque, selon la porte que l'on ouvrira, elle a le potentiel d'être rouge ou verte. De plus, puisque les quballes peuvent être enchevêtrées avec les autres quballes, ouvrir une porte a un impact sur ce que l'on obtiendra lorsque l'on ouvrira les autres portes. Rappelons-nous que pour une paire EPR, si l'on ouvre une boîte et observons une quballe rouge, alors on sait, avant même d'avoir ouvert l'autre boîte, que l'on observera une quballe rouge ; notre première mesure a eu une influence sur le résultat de la mesure subséquente. Une description complète des 7 quballes doit donc tenir compte de ces subtilités supplémentaires qui sont inexistantes pour le cas classique.

Pour bien comprendre la différence entre ordinateurs classique et quantique, il est utile de représenter les quballes par des balles régulières. Comme nous venons de le voir, dans le cas quantique, 7 balles régulières ne seront pas suffisantes pour une description complète du système. Puisque toutes les configurations de couleurs pour les quballes peuvent être en superposition d'états, nous aurons besoin de 128 balles régulières, c'est-à-dire autant que le nombre de configurations possibles.

On a donc besoin d'un nombre exponentiellement plus grand (2 à la 7 plutôt que 7) de balles que dans le cas classique ! Comme on le constate à partir du tableau suivant, cela fait une différence énorme :

# de quballes	# de balles classiques requises pour une description complète
10	1020
20	1 048 580
50	1 073 470 000
300	Plus que le nombre d'atomes dans l'univers visible !

Comme on le constate à partir de ce tableau, le nombre de balles classiques requises pour décrire correctement l'information quantique est énorme. Par exemple, pour 300 quballes (un nombre bien petit comparativement aux milliards de transistors dans un PC moderne) le nombre de balles classiques requises est plus grand que le nombre d'atomes dans l'univers visible ! Ceci signifie que si l'on prenait toute la matière contenue dans l'univers visible, nous n'aurions toujours pas assez de ressources pour décrire complètement l'état de ces 300 quballes ! Évidemment, ceci implique que la simulation classique de simplement 300 quballes, sans mentionner un nombre plus grand de quballes, est sans espoir...

Puisqu'un ordinateur classique n'est pas capable de simuler efficacement un ordinateur quantique et puisqu'un ordinateur quantique est capable de simuler efficacement un autre ordinateur quantique, alors un ordinateur quantique doit être plus puissant que sa contrepartie classique. C'est la conclusion à laquelle Richard Feynman est arrivé au début des années 1980 et qui a stimulé l'intérêt dans ce domaine.

Nous avons vu que l'information quantique se comporte étrangement, et ce, en particulier lorsque l'on fait une préparation par une porte et que l'on observe à partir d'une autre porte obtenant alors un

résultat aléatoire. En utilisant cette notation, nous avons obtenu quelques résultats important comme le théorème anticlonage et des applications utiles comme la téléportation quantique.

Toutefois, comme il est devenu évident lors de la discussion reliée à la téléportation quantique, cette notation est un peu lourde lorsque l'on a à traiter un grand nombre de balles. Mais maintenant que l'on comprend les idées de base concernant l'information quantique, une notation beaucoup plus pratique est de représenter les balles (ou quballes) par quelque chose de beaucoup plus simple : disons des 0 et des 1 ! Après tout, il est plus simple décrire un 0 ou un 1 que de dessiner des balles rouge et vertes.

L'intrication quantique et la transmission de pensée

Nous connaissons tous le cas de ces jumeaux qui achètent, sans se concerter la même cravate. Nous avons aussi tous été confrontés à cette réflexion, quand le téléphone sonne et que nous avons au bout du fil celui ou celle à qui nous pensions à ce moment précis : « justement, je pensais à toi ! » On serait tenté de faire une analogie avec le phénomène d'intrication quantique où deux photons, par exemple, prennent la même polarisation au même moment alors qu'ils sont à une distance suffisante pour qu'on puisse affirmer que rien ne les relie physiquement.

Pour illustrer cet effet EPR, citons Etienne Klein qui est physicien au CEA et enseignant à l'Ecole Centrale. Il y voit l'assise théorique du romantisme : *Deux cœurs qui ont interagi dans le passé ne peuvent plus être considérés de la même manière que s'ils ne s'étaient jamais rencontrés. Marqués à jamais par leur rencontre, ils forment un tout inséparable.*

C'est un fait constaté par tous. Et si la mécanique quantique était l'explication ?

Ordinateur quantique : rêves ou réalité

Cette machine abstraite est en effet affligée de deux défauts majeurs. Tout d'abord, le résultat final n'étant déterminé que par des lois de probabilité, un calcul peut, à priori, donner n'importe quel résultat. Il faut donc inventer des algorithmes qui permettent d'augmenter fortement la probabilité que le système « décohére » dans l'état correspondant à la bonne réponse. Un vrai défi pour les théoriciens. Ensuite, lors du calcul, le système doit éviter le moindre contact avec le monde extérieur, puisque celui-ci en romprait inévitablement l'équilibre. L'ordinateur quantique est donc la machine la plus fragile qu'on puisse imaginer ! Cette fois, le défi concerne les expérimentateurs. Tant que les questions de son utilité et de sa construction n'auront pas été résolues, l'ordinateur quantique restera fantomatique... Les dernières recherches lui permettront-elles de se matérialiser ?

Quelques modèles avancés

Deux équipes américaines, celle du Massachusetts Institute of Technology (MIT) et celle du laboratoire national de Los Alamos (Californie) se sont associées pour réaliser un prototype d'ordinateur quantique. À première vue, ce dernier ne réalise aucune opération exceptionnelle : quelques additions, des reproductions d'opérateurs logiques ET, OU, NON... Des calculs qu'une simple calculatrice de poche pourrait effectuer. Mais la méthode est révolutionnaire. Leur prototype n'est pas une boîte grise, avec

un écran, un clavier et une souris. Non, c'est un tube à essai. Quelques gouttes d'un liquide de teinte marron, des molécules de 2,3-dibromothiophène, toutes identiques, composées d'atomes de carbone, d'hydrogène, de soufre et de brome. Ces molécules sont l'équivalent de nos processeurs. Ce sont elles qui exécutent les calculs. L'orientation des noyaux des atomes d'hydrogène, que l'on peut faire varier à l'aide d'ondes radio dont on module la fréquence et la durée, peut se traduire en autant de 0 et de 1, indispensables à la programmation de tout ordinateur. Les chercheurs du MIT encore ont testé avec succès l'algorithme de Grover qui permet de trouver rapidement parmi plusieurs propositions la seule qui convient. Des scientifiques californiens du centre de Recherche Almaden d'IBM et de l'Université de Stanford ont réussi la mise en facteur du nombre 15 par l'algorithme de Peter Shor — à l'aide d'un ordinateur quantique. L'expérience des chercheurs du SPEC a porté sur un bit quantique constitué d'une boucle de métal supraconducteur (aluminium) interrompue par des jonctions tunnel (ou jonctions Josephson). Ce circuit, baptisé « Quantronium », est à ce jour le q-bits électronique le plus performant. L'avantage du Quantronium est d'être bien découplé du circuit extérieur, tout en restant connecté et donc mesurable à tout moment. Grâce à ce découplage, le temps de cohérence est suffisamment long pour permettre des expériences qui n'avaient jamais été réalisées sur un circuit électronique. L'état quantique du Quantronium a ainsi été piloté par des séquences d'impulsions radiofréquence, comme peut l'être celui d'un atome par des impulsions laser. Plusieurs expériences classiques pour des atomes ont été ainsi effectuées sur le Quantronium. Elles ont démontré son caractère quantique sans ambiguïté, et le temps de cohérence quantique a été déterminé. Ce temps est déjà assez long pour envisager la fabrication de circuits comportant plusieurs bits quantiques couplés sur une même puce, et de réaliser ainsi des portes logiques quantiques.

Applications

1° Décomposition en facteurs de nombres premiers algorithme de Shor

Le premier « craquage » d'une clef de cryptage par cet algorithme utilisable seulement sur un ordinateur quantique. Certes, l'opération peut paraître modeste puisqu'elle ne concernait que la factorisation en nombres premiers du chiffre 15 : soit 3 × 5. La performance est ailleurs, dans la conception même de l'embryon d'ordinateur qui a permis de la réaliser. Isaac Chuang, qui a dirigé ces travaux, avait déjà été à l'origine de plusieurs premières : un prototype à deux q-bits en 1996, une machine à trois q-bits en 1999, à cinq en 2000. Cette fois, une formule à sept q-bits a été nécessaire pour réaliser la factorisation.

Leur support : des atomes de carbone et de fluor inclus dans une solution dopée avec des composés ferreux. Cette soupe, placée au cœur d'une machine à résonance magnétique, a subi toute une série d'impulsions électromagnétiques afin de réaliser pas à pas les étapes de l'algorithme de Shor. Tout en évitant les effets indésirables, comme la décohérence du système, qui fait perdre aux atomes leurs propriétés quantiques. Et en disposant d'un dispositif de mesure suffisamment subtil pour tirer profit d'une des propriétés des q-bits, qui est précisément de changer d'état lorsqu'on veut le mesurer. « *En dépit de ses propriétés exceptionnelles, notre molécule est clairement poussée dans ses derniers retranchements par l'algorithme de Shor* », reconnaissent les protagonistes. De la même façon, ils admettent que si leur méthode de stockage de l'information quantique dans des noyaux atomiques est en principe extensible à des systèmes comportant de nombreux q-bits, leur expérience ne prouve pas que ce changement d'échelle soit possible.

2° Algorithme de Grover

Plus fascinant encore est le travail effectué par Lov Grover des laboratoires Bell. Celui-ci a développé une série d'instructions pour un ordinateur quantique permettant des recherches très précises et très rapides. Avec un ordinateur classique, si une liste non triée contient 10 000 objets il faudra 5 000 étapes pour repérer l'objet voulu. Avec l'algorithme de recherche de Grover il faut seulement 100 étapes. Comment fait-on pour réaliser un tel miracle ? Au départ il faut préparer un registre quantique dans

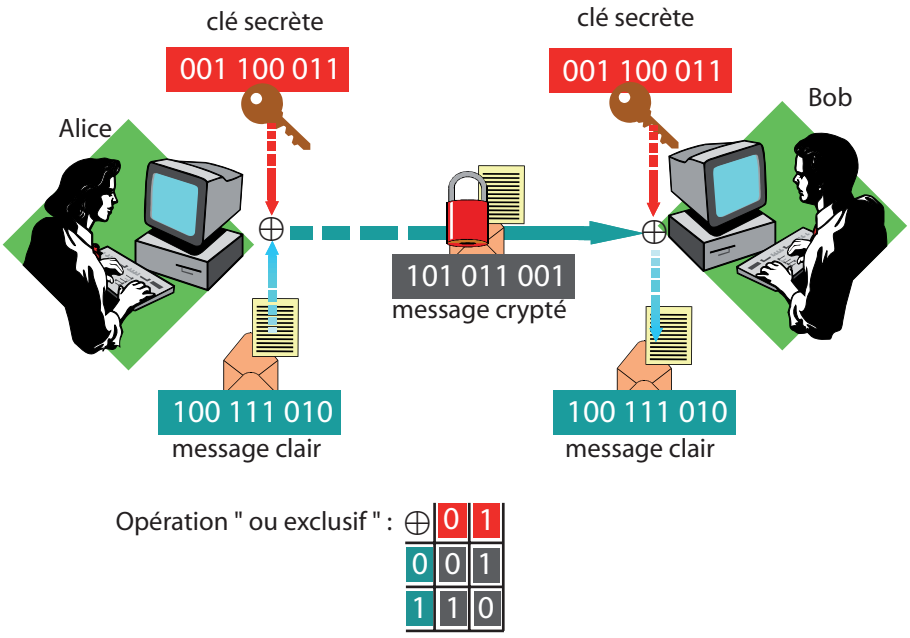
une superposition de tous les états possibles (ou objets) de la liste. On y applique ensuite les instructions quantiques. Cet algorithme peut être décrit en terme d'onde. Rappelons qu'un objet quantique est une particule et une onde. Comme toute onde elle peut interférer avec d'autres ondes. Ces interférences peuvent être constructives (les ondes se renforcent, comme lorsque deux crêtes de vagues se rencontrent) ou destructives. Tout le secret de l'algorithme de Grover se trouve là : les bonnes solutions de la recherche se renforcent et émergent de l'ensemble tandis que les autres s'annulent et sont rejetées.

Le travail de L. Grover peut s'appliquer pour résoudre d'autres problèmes : la factorisation, dont nous avons déjà parlé, l'estimation d'une moyenne dans un large ensemble de nombres ou bien alors la recherche d'un objet dont nous avons une partie de l'information (comme la reconnaissance de signal d'une transmission de données corrompues par un bruit de fond). Dans tous ces cas, l'algorithme de L. Grover est bien plus puissant que n'importe quel algorithme classique. De plus, cet algorithme est assez robuste face au problème de la décohérence.

Pragmatisme quantique

La cryptographie quantique intervient dans le cadre de la cryptographie à clé secrète : elle va permettre à Alice et Bob de convenir d'une clé dont le secret soit garanti. Ils pourront ensuite crypter et décrypter classiquement un message en utilisant cette clé.

Parmi les méthodes de cryptographie à clé secrète, le « one time pad » est le seul qui garantisse une sécurité absolue. Alice et Bob se sont mis d'accord sur une suite aléatoire de 0 et de 1, la clé de cryptage, qui a la même longueur que le message qu'Alice doit transmettre à Bob. Le message crypté envoyé par Alice est le « ou exclusif », bit à bit, du message en clair et de la clé.



Bob reçoit donc une suite aléatoire de 0 et de 1, vide d'information pour quiconque ne possède pas la clé, puis fait un « ou exclusif[259] » de cette suite et de la clé, ce qui reconstitue chez lui le message en clair. Pour éviter les indiscrétions, on ne doit pas utiliser la même clé plus d'une fois et, surtout, la clé doit être secrète. On a donc reporté un problème crucial en amont : Alice et Bob doivent disposer d'un

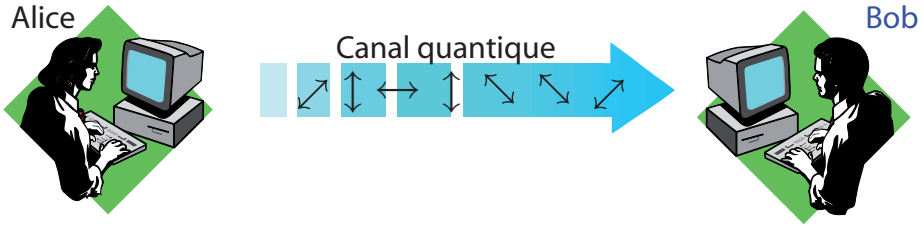
[259] La fonction OU exclusif, souvent appelée XOR (eXclusive OR), est un opérateur logique de l'algèbre de Boole. À deux événements, qui peuvent avoir chacun la valeur VRAI ou FAUX, il associe un résultat qui a lui-même la valeur VRAI ou FAUX.

moyen de communication absolument sûr pour se mettre d'accord sur une clé chaque fois qu'il veulent échanger un message confidentiel.

C'est pour convenir d'une clé de « one time pad » que la physique quantique vole au secours d'Alice et Bob. À titre d'exemple, voici le protocole BB84 (Bennett et Brassard, 1984) de distribution de clé quantique. Pour constituer la clé, Alice envoie à Bob une suite aléatoire de 0 et de 1, quatre fois plus longue que la clé dont ils auront besoin. Mais chacun de ces bits est codé par un qubit qui circulera sur la ligne entre Alice et Bob. Imaginons que chaque qubit soit un photon qui peut être polarisé à 0, 45, 90 ou 135 degrés. Quand Alice doit envoyer le bit 0, elle tire à pile ou face et code ce 0 soit par un qubit à 0 degré, soit par un qubit à 45 degrés. Idem pour 1 : soit 90 degrés, soit 135 degrés. Mais Bob ne sait à l'avance ni s'il va recevoir un 0 ou un 1, ni si Alice l'aura codé dans la base standard {0,90} ou dans la base diagonale {45,135}. Il tire donc lui aussi chaque fois à pile ou face pour choisir la base, standard ou diagonale, dans laquelle il mesurera le qubit qu'il reçoit.

> ***One time pad*** ou ***masque jetable***, également appelé chiffre de Vernam est un algorithme de cryptographie inventé par Gilbert Vernam en 1917, ingénieur à l'*American Telephone and Telegraph Company*, chargé de la sécurité des téléscripteurs. Il s'agit en fait d'un chiffre de Vigenère à clé aléatoire aussi longue que le message clair. Bien que simple, ce chiffrement est le seul qui soit théoriquement impossible à casser, même s'il présente d'importantes difficultés de mise en œuvre pratique.
>
> Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :
>
> — La clé doit être une suite de caractères aussi longue que le message à chiffrer.
>
> — Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
>
> — Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de masque jetable).
>
> L'intérêt considérable de cette méthode de chiffrement, c'est que si les trois règles ci-dessus sont respectées strictement, le système offre une sécurité théorique absolue, comme l'a prouvé Claude Shannon en 1949.
>
> L'argument théorique est le suivant, dans son principe : si on ne connaît que le texte chiffré, et que toutes les clés sont équiprobables alors tous les textes clairs sont possibles et avec la même probabilité puisqu'il y a bijection, une fois le chiffré fixé, entre clés et textes clairs. Même une attaque par force brute ne donnera aucune information.
>
> Ce type d'impossibilité, appelé ***sécurité sémantique***, ne repose pas sur la difficulté du calcul, comme c'est le cas avec les autres systèmes de chiffrement en usage. Autrement dit, le système du masque jetable est inconditionnellement sûr.
>
> La seule attaque possible consiste donc à déterminer l'ensemble de la clé.

Pour chaque qubit où ce choix est le même que celui d'Alice, le 0 (le 1) que Bob observe est correct à 100 % : Alice avait bien codé un 0 (un 1). Mais les lois de la mesure quantique n'accordent à Bob qu'une probabilité de 50 % d'observer 0 (ou 1) si Alice avait codé 0 (ou 1) dans une base différente de celle qu'il a choisie. Quand tous les bits de la suite aléatoire codés de cette manière auront été envoyés par Alice, puis reçus et observés par Bob avec 50% de chance de se tromper d'outil d'observation, Alice et Bob se disent (au téléphone, par exemple : un espionnage de cet échange ne présente plus de risque) la suite des bases qu'ils ont utilisées, Alice pour coder, Bob pour observer, sans révéler les bits codés ou observés. La probabilité de coïncidence entre le choix d'Alice et celui de Bob fait qu'ils ne retiennent alors qu'une moitié des bits, approximativement, ceux pour lesquels ils ont fait le même choix de base : cette suite de bits pourrait constituer une clé de cryptage secrète, sauf



envoie	base de codage	polarisation	base de décodage	lit
0	standard	↔	standard	0
0	standard	↔	diagonale	0 ou 1
0	diagonale	⤢	diagonale	0
0	diagonale	⤢	standard	0 ou 1
1	standard	↕	standard	1
1	standard	↕	diagonale	0 ou 1
1	diagonale	⤡	diagonale	1
1	diagonale	⤡	standard	0 ou 1

Les différentes possibilités de codage et décodage des bits codés par des photons polarisés.

si... un observateur indiscret, Eve, intercepte les qubits qui passent sur la ligne, les mesure avec la même

envoie	base de codage	qubit envoyé	base de décodage	lit	qubit renvoyé	base de décodage	lit
			standard	0	↔		0
0	standard	↔		0	⤢	standard	ou 0
			diagonale	ou 1			1
					⤡		ou 0
							1

Supposons qu'Alice envoie un 0 codé dans la base {0,90} et que Bob choisisse la même base pour observer le qubit qu'il reçoit. S'ils ont été espionnés, alors le qubit observé par Bob pourra être différent de celui envoyé par Alice.

ignorance que Bob de la base de codage choisie par Alice, ce qui peut modifier le qubit si elle ne choisit pas la bonne base, puis renvoie ce qubit, éventuellement modifié, à Bob qui croit le recevoir d'Alice. Supposons qu'Alice ait envoyé un 0 codé dans la base {0,90} et qu'Eve utilise cette même base pour espionner à ce moment : elle observera un 0, puis renverra un qubit identique à Bob. Si Bob utilise lui aussi la base {0,90} pour observer ce qubit, Alice et Bob ne détecteront pas que ce bit, qu'ils conserveront, est connu par l'espionne. Mais Eve a 50% de chances de se tromper de base pour espionner, donc de renvoyer à Bob un bit codé dans une base différente de celle choisie par Alice. S'il s'agit d'un bit pour

lequel Alice et Bob ont utilisé la même base, il y alors 50% de chances que Bob observe un 1 (un 0) alors qu'Alice avait codé un 0 (un 1) : si Eve espionne, 25% des bits codés par Alice et observés par Bob dans la même base seront différents.

C'est pourquoi Alice et Bob se téléphonent une deuxième fois, choisissent au hasard une moitié des bits retenus à l'issue de leur premier échange, et sacrifient ces bits, car maintenant ils les comparent et Eve peut écouter : s'il n'y a pas de différence, ils savent avec quasi certitude que leur clé n'a pas été espionnée (si m bits sont comparés, la probabilité qu'ils soient tous identiques malgré un espionnage est de (3/4)m, soit 3.10-13 pour m=100). Ils doivent évidemment tenir compte d'une ligne normalement bruitée, mais tant que le taux de différences est inférieur au taux normal d'erreurs, ils peuvent considérer que les bits restants (1/4 de la suite initiale) constituent une clé secrète, sinon ils rejettent le tout et recommencent.

Il existe d'autres protocoles que BB84 pour la distribution de clé quantique. Tous exploitent le fait que la mesure quantique perturbe l'état du qubit mesuré pour, in fine, détecter la présence d'un observateur indiscret. Ceci est impossible avec des bits classiques. On peut d'ailleurs noter que « cryptographie quantique » est un abus de langage, car rien n'est crypté, il s'agit de transmission sûre de l'information grâce aux propriétés de la matière à l'échelle quantique. Plusieurs expérimentations du protocole BB84 ont été faites, avec des transmissions sur plusieurs dizaines de kilomètres, soit par fibre optique, soit dans l'air. Un objectif majeur concerne les communications sûres entre le sol et des satellites. Quelques sociétés industrielles sont déjà sur les rangs et commencent à mettre des produits sur le marché, comme ID Quantique à Genève ou MagiQ Technologies à New York et Boston.

Applications pratiques

Une équipe de chercheurs du Groupe de physique appliquée de l'Université de Genève a monté une petite entreprise destinée à commercialiser des appareils de cryptographie quantique. Cette technique assure aux transferts de données sensibles une sécurité absolue, contrairement à ce qui existe actuellement sur le marché. Une banque genevoise, soucieuse comme toutes ses consœurs de la confidentialité de ses transactions, a accepté de jouer le rôle de client test pour éprouver la fiabilité du dispositif.

Dans le laboratoire de Nicolas Gisin, professeur au sein du Groupe de physique appliquée de l'Université de Genève, Alice et Bob existent bel et bien, mais ils ne sont pas de chair et d'os. Ce sont deux boîtes remplies d'électronique et d'optique qui communiquent entre elles par une fibre optique.

Ce qu'elles se disent, personne, et surtout pas Eve, ne peut le savoir. Si l'espionne tentait d'intercepter ne serait-ce qu'une parcelle d'information, elle perturberait la communication, alertant immédiatement Alice ou Bob. Il faut dire que les vecteurs de l'information sont des photons très particuliers — on les dit « corrélés » — et qu'ils obéissent aux lois de la physique quantique[260].

[260] La cryptographie quantique a été inspirée par une propriété singulière des photons, les particules élémentaires de la lumière. Il s'agit du phénomène de corrélation entre deux photons. Il arrive que des atomes, en réarrangeant leur nuage électronique, émettent simultanément deux de ces grains de lumière dans des directions opposées. Il se trouve que les deux membres de ce couple de photons sont dans des états identiques à tout point de vue. Ils possèdent la même longueur d'onde, la même phase et la même polarisation. Mieux encore : alors même qu'ils s'éloignent l'un de l'autre, les deux photons continuent à garder entre eux un certain « contact ». Le monde quantique a, par ailleurs, cette particularité que le scientifique n'a aucun moyen de savoir quels sont les paramètres du photon avant de le « mesurer ». Mais s'il le fait, il détruit le grain de lumière qui est absorbé et annihilé par son détecteur. Tant qu'ils sont libres, les deux photons décrits ci-dessus se trouvent donc, pour l'observateur extérieur, dans un état totalement indéterminé. Plus exactement, selon la formulation de la théorie quantique, ils sont dans tous les états quantiques possibles à la fois. Ce n'est qu'au moment de la mesure que les paramètres de la particule sont figés, c'est-à-dire que le photon acquiert une polarisation et une phase précises et uniques. Dans le cas de deux photons corrélés, dès que la mesure est réalisée sur le premier, le second adopte instantanément le même état avant même d'être détecté à son tour. C'est un peu comme si l'information passait d'un photon à l'autre à une vitesse infinie. Les physiciens ont vite compris l'avantage que l'on pouvait tirer de cette corrélation. De tels photons peuvent être injectés dans une fibre optique, l'un allant vers Alice et l'autre vers Bob. Lorsque Alice mesure un paramètre (la phase ou la polarisation) de la particule, cette valeur est immédiatement adoptée par celle qui se dirige vers Bob. À chaque paire de photons est attribué un « 0 » ou un « 1 » suivant le

Avec trois collègues de son équipe, Grégoire Ribordy, Hugo Zbinden et Olivier Guinnard, Nicolas Gisin a fondé en automne dernier une petite entreprise, *id Quantique*, dans l'intention de commercialiser les appareils qu'ils ont développés pour les besoins de leurs recherches. Leur idée semble plaire puisque *id Quantique* fait partie des quelques entreprises triées sur le volet qui ont représenté la Suisse à Cebit. Cette gigantesque foire d'électronique s'est tenue à Hanovre du 13 au 20 mars 2002.

La cryptographie quantique emprunte les airs

Source : NOUVELOBS.COM, 12.03.2007

Deux télescopes des îles Canaries ont échangé une information hautement sécurisée sous forme de photons, battant le record de transmission sans fil d'une clef de codage indispensable à la cryptographie quantique. L'équipe d'Anton Zeilinger, de l'Université de Vienne, a utilisé un laser pour envoyer des photons codés depuis un télescope de la Palma vers un autre situé à Tenerife, à 144 kilomètres de distance, rapporte la revue *Nature*.

Là où la cryptographie « classique » utilise de complexes algorithmes pour protéger un réseau, la cryptographie quantique a recours aux photons pour transporter la précieuse clef qui permet d'accéder aux informations codées. En effet, si quelqu'un essaie d'intercepter l'information, la polarisation du photon est modifiée et l'émetteur comme le récepteur savent que leur échange a été piraté. Le système est encore plus efficace si les photons sont envoyés un par un plutôt que par paquets.

Ces photons peuvent voyager par fibre optique, mais à partir de 100 km le signal se dégrade. Pour qu'une armée — par exemple — puisse utiliser un réseau crypté à la mode quantique, la clef doit pouvoir voyager sur de longues distances par les airs.

L'équipe d'Anton Zeilinger a annoncé[261] avoir réussi à transmettre la fameuse clef photon par photon sur une distance de 144 km. Pour cela Zeilinger et ses collègues ont eu recours à la téléportation quantique qui permet, à partir de paires de particules intriquées, de faire voyager une information sans support physique. Les chercheurs ont donc créé des paires de photons ayant la même polarisation pour transmettre la clef. Le débit est de 178 photons (ou unités d'information) par seconde, très loin des vitesses de connexions des réseaux internet. Cependant, l'objectif n'est pas de transmettre une grande une quantité d'informations, mais d'avoir le maximum de sécurité.

Les réseaux quantiques

Test d'un réseau informatique à cryptographie quantique réussi

Source : bulletins-electroniques, 3/05/2007

Une équipe de scientifiques chinois, dirigée par le professeur GUO Guangcan du « laboratoire national clé » en information quantique de l'Université de Science et Technologie de Chine (USTC) à Pékin, a annoncé le 2 avril 2007 le succès du test d'un réseau informatique à communications sécurisées par cryptographie quantique, réalisé en mars 2007.

L'expérience a consisté à transmettre des données, notamment pour application multimédia, sécurisées par encryptage quantique (tentative de mise en œuvre des prédicats de la mécanique quantique afin d'assurer la confidentialité, l'intégrité et la non-interception de transmissions de données) entre 4 utilisateurs du réseau commercial du groupe China Telecom. Les « routeurs quantiques » développés ont

résultat de la mesure et en respectant un protocole décidé à l'avance. Si Eve, la jalouse, tente d'intercepter cette information, elle ne peut faire autrement que de détruire le photon et donc de révéler sa présence.

[261] Congrès de la Société américaine de physique (PAS), 5-9 mars 2007, Denver, USA.

permis des transmissions entre un ordinateur et, soit un autre parmi trois, soit les trois autres en même temps, avec des distances de 32 à 42,6 km entre deux ordinateurs.

Cette équipe avait déjà réalisé en 2004 une expérience point à point sur une distance de 124 km entre Pékin et Tianjin par fibre optique, le record mondial étant actuellement de 148,7 km.

D'après Pr. Guo, l'information quantique ne peut pas être copiée et toute interception est facilement détectable, ce qui donne à la cryptographie quantique un gros avantage par rapport à la cryptographie « traditionnelle » qui peut être décodée, en particulier concernant l'application à de futurs ordinateurs quantiques.

D'après les scientifiques, il s'agirait du premier réseau de ce type capable d'effectuer des communications simultanées, ce qui constitue un pas important vers l'utilisation pratique de la cryptographie quantique en particulier pour Internet.

Record de distance pour le transfert quantique

Source : futura-sciences.com le 13/06/2007

Une équipe de physiciens travaillant à l'observatoire de Roque de los Muchachos, sur l'île de La Palma, a réussi à transmettre une clé quantique de cryptographie en utilisant l'effet EPR sur une distance de 144 km. Cette technique pourrait ouvrir la voie à un réseau mondial de communications quantiques. La téléportation d'états quantiques par ce moyen est aussi envisageable.

De telles expériences de transfert quantique de codes avaient déjà eu lieu par le passé, mais jusqu'ici, n'avaient jamais dépassé de grandes distances et le record pour la téléportation d'états quantiques est quant à lui de treize kilomètres. En décuplant potentiellement cette valeur, c'est une amélioration sensible qui vient d'être réalisée, et celle-ci laisse entrevoir d'autres progrès futurs, qui pourraient déboucher sur une application pratique du procédé.

Le principe repose sur l'intrication quantique (*quantum entanglement*) de deux particules, comme des photons, avec pour conséquence que toute modification apportée à l'une d'elles se répercute instantanément sur la seconde, et cela quelle que soit la distance qui les sépare. Dans la pratique, une des deux particules ainsi créées est conservée sur place, et la seconde transmise par voie optique vers un récepteur.

Dans l'expérience qui vient d'être réalisée, des paires de photons polarisés et intriqués ont été produites à l'observatoire Roque de los Muchachos. Pour chaque paire, un des photons était mesuré sur place alors que son jumeau était transmis à 144 km de là vers la station terrestre optique de Teneriffe de l'ESA, utilisée comme récepteur. Une suite aléatoire de nombres définissant une clé pour la cryptographie était alors générée et transmise de façon totalement sûre.

Robert Ursin, de l'université de Vienne, déclare que cette expérience démontre la possibilité de transmettre certaines informations sensibles par satellite par ce procédé, notamment des codes de sécurité. Et il ne dissimule pas son rêve de pouvoir expérimenter prochainement dans l'espace, à des distances autrement importantes. La confirmation des corrélations quantiques EPR sur de telles distances ouvre la voie à la possibilité de téléporter des qubits d'information en utilisant non plus deux, mais trois particules.

Cependant, l'intrication quantique n'est actuellement contrôlable que pour les formes les plus simples de la matière, et la téléportation porte uniquement sur de l'information. Les scientifiques croient qu'une approche fondamentalement nouvelle sera nécessaire si on veut un jour l'utiliser pour déplacer des personnes ou même des objets inanimés. On ne peut donc pas encore imaginer réaliser un système de téléportation tel que celui de Star Trek, ce que confirme Robert Ursin : « Il s'agissait d'une simple étude de faisabilité financée par l'Agence Spatiale Européenne. En principe, de telles expériences peuvent être utilisées pour déplacer de l'information par téléportation entre deux endroits distants, mais notre système n'est pas capable de transporter de la matière », ajoute-t-il. « Nous pensons que voyager par ce moyen serait une très bonne idée de science-fiction, mais j'ai peur que téléporter des personnes ne soit

pas possible avec la technologie actuelle. Mais il ne serait pas exclu d'organiser l'information pour transmettre des données complexes par ce moyen », assure-t-il.

La cryptographie quantique sécurise les votes (en Suisse)

Source : atelier.fr le 12/10/2007

La Suisse utilisera la cryptographie quantique pour ses prochaines élections nationales. Le système se focalisera sur la sécurisation du transfert des votes au centre de dépouillement.

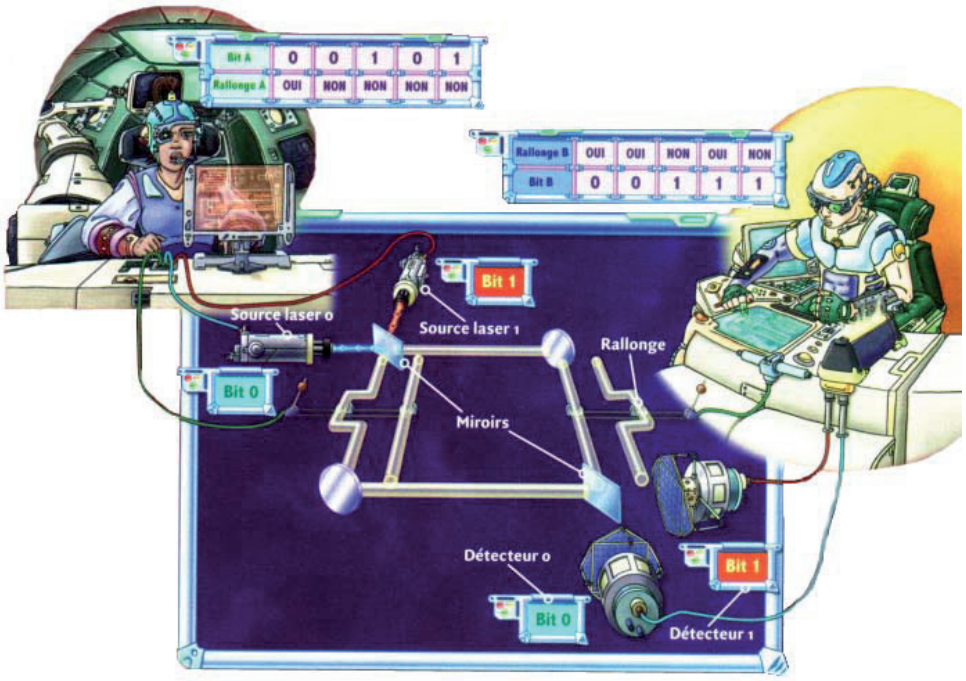
La sécurité des votes électroniques est peut-être une question de cryptographie quantique. Sous la complexité du terme se cache un codage inviolable de données développé par l'université de Genève. Il vise à sécuriser le réseau qui relie l'espace de dépouillement des votes au centre de données gouvernemental où les résultats sont enregistrés. Industrialisé par la spin-off de l'université *id Quantique*, il sera déployé pour la première fois lors des élections nationales du 21 octobre. Ce, en partenariat avec le Centre des technologies de l'information de Genève.

Éradiquer les risques d'altération

Le dispositif, sur lequel les chercheurs travaillent depuis une dizaine d'années, utilise un système de cryptage quantique à 1GHz et une ligne en fibre optique pour transmettre les données. Il ne vise pas à protéger des attaques externes, mais « à vérifier que les données n'ont pas subi d'altération lors de leur transit entre la saisie et le stockage », souligne Robert Hensler, chancelier du comté. Les informations sont inscrites, via un procédé quantique, sur des photons qui explosent lors de toute tentative d'intrusion lors du transfert.

Vers un réseau national de communication quantique

Cette initiative, qui inaugurera l'utilisation de la cryptographie quantique dans les systèmes de vote, devrait n'être qu'un prélude avant la création d'un réseau pilote de communication quantique genevois. Celui-ci, baptisé *SwissQuantum*, devrait ressembler à l'ancêtre d'Internet apparu aux États-Unis dans les années 70. Pour y parvenir, les scientifiques souhaitent maintenant mettre au point une plate-forme de test et de validation des technologies quantiques dans le but de rendre les réseaux de communication toujours plus sûrs. Un idéal qui devrait rencontrer l'aval de nombreux secteurs professionnels comme ceux de la banque, de l'assurance et du hi-tech, pour qui la confidentialité des données est primordiale.



Le nouveau visage d'Alice et Bob

Conclusion

Le dernier cri, improprement nommé ***Cryptographie quantique***, n'est en fait qu'un moyen de s'assurer d'une part de l'authenticité, mais surtout de l'***intégrité*** des communications. Reste que la sécurité réelle des communications repose sur une chaîne de précautions et des protocoles qui doivent être suivis à la lettre.

C'est pourquoi nous traiterons, dans le tome II de la question de la sécurité informatique en général et sur le réseau Internet en particulier puisqu'à l'heure actuelle c'est par lui que passe la majorité des communications, sous la forme de e-mails, mais aussi de transfert de fichiers (P2P)[262], ou de téléphonie (VoIP)[263] .

C'est également dans ce deuxième tome que nous aborderons la question des législations en vigueur de par le monde concernant en particulier le détournement ou la capture de la correspondance privée, sous quelque forme que ce soit.

[262] Le terme pair-à-pair est la traduction de l'anglais Peer-to-Peer, laquelle est souvent abrégée P2P. On trouve parfois la traduction « poste-à-poste » ou par « égal-à-égal ». Il ne doit pas être confondu avec la notion de liaison point à point, désignée en anglais par l'expression Point-to-Point ou avec le protocole point à point, ou PPP. Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, de partager simplement des informations — des fichiers le plus souvent, mais également des flux multimédia continus (streaming), le calcul réparti, la téléphonie (comme Skype), etc. sur Internet.

[263] La voix sur réseau IP, parfois appelée téléphonie IP ou téléphonie sur Internet, et souvent abrégée en « VoIP » (abrégé de l'anglais Voice over IP), est une technique qui permet de communiquer par voix à distance via le réseau Internet, ou tout autre réseau acceptant le protocole TCP/IP.

Table des matières

COMMUNIQUER : UNE NÉCESSITÉ VITALE POUR L'HOMME **1**

Préface 3

Communiquer à distance ***5***

La voix 5
L'appareil vocal et son fonctionnement 5
Les sifflements 7
Les sifflets 8
Les trompes et les conques 10
Un autre usage des conques : 11
Les tambours 12
Les messages tambourinés 12
Le tam-tam 13
Les cloches 14
Les xylophones 15
Systèmes de communication sonore originaux 16
Messagerie unilatérale et bilatérale 16
Les relais de transmission 16
Structure des messages 17
Confidentialité 17
Et la tonalité ? 17
Impossibilités techniques 17
Conclusion 17
Les messages visuels 18
Quelques faits historiques 18
Les signaux de fumée. 19
Les phares et les sémaphores 19

LE TÉLÉGRAPHE **21**

Le télégraphe 23
Les techniques du télégraphe Chappe 26
Le code ou vocabulaire 27
D'autres télégraphes optiques. 33
L'électricité dans les transmissions. 39
Le télégraphe Morse 41
Le télégraphe électrique dans les autres pays 45
Autres appareils de transmission électrique de textes et d'images originaux. 48
Les ancêtres du Fax. 48
Les applications du télégraphe électrique. 58
Autres péripéties et faits divers des débuts du télégraphe électrique 58
Autres exemples historiques : 58
Après l'avènement du télégraphe électrique : 58
Le câble sous-marin 63
Le câble transatlantique 64

LE TÉLÉPHONE, PETITE HISTOIRE ET TECHNIQUE **69**

Le téléphone. 71
Établissement et conception des premiers réseaux téléphoniques. 76
La vie des centraux téléphoniques 76
Réseau public à batterie centrale 78
Des chiffres et des lettres 79

Le réseau téléphonique commuté (RTC) ... 80
Schéma de principe simplifié du RTC ... 81
La boucle locale. ... 82
La partie « Branchement » ... 82
La partie « Distribution » ... 83
La partie « Transport » ... 83
La structure en anneau ... 83
Phases d'établissement d'une communication. ... 83
Liaison entre le téléphone et le central téléphonique ... 83
Décrochage du combiné ... 84
Numérotation décimale ... 85
Numérotation par fréquences vocales ou DTMF (dual tone multi frequency) ... 86
Activation de la sonnerie ... 86
Transmission de la voix ... 87
Numéris, le réseau numérique à intégration de service (RNIS) de France Télécom. ... 87
Le réseau Transpac ... 88
Le réseau à large bande ATM ... 89

LA T.S.F. 91

Le Radiophone. (par le comte Th. Du Moncel.) ... 93
Émission radio à ondes courtes. ... 100
La radio d'aujourd'hui. ... 101
La révolution numérique ... 103
Rappel historique ... 103
Autres modes de communication utilisant l'infrastructure du réseau téléphonique ... 105
La télécopie ... 105
Le vidéotex ... 105
La télématique vocale ... 106
La téléaction ... 106
Échanges électroniques de documents. Courrier électronique ... 106
Informatique et télécommunications ... 108
Micro-ordinateurs et communication ... 108

L'histoire du téléphone portable ... 111

La création du téléphone « mobile » ... 111
Le téléphone de voiture en France. ... 111
Le Radiocom 2000 ... 112
Le réseau NMT-F ... 112
De l'analogique au numérique : le GSM. ... 113
Une tentative avortée : le Bi Bop ... 113
Le GSM : un développement continu ... 113
Architecture réseau et protocole ... 113
Amélioration : le damier hexagonal ... 115
Évolutions futures ... 117

Les satellites de télécommunication ... 119

Fonctionnement général ... 119
Avantages d'un satellite par rapport aux communications terrestres. ... 119
Les différents types de satellites de télécommunication ... 119
Affaiblissement possible du signal ... 120
Deux ressources fondamentales ... 120
Modulation du signal ... 120
Types de couvertures d'un satellite géostationnaire ... 120
Services commerciaux ... 120
Services internationaux ... 121

Intelsat 121
Inmarsat 121
Les services régionaux 121
En Europe : 121
Arabsat : 122
Palapa : 122

INTERNET **123**

...Et l'Homme créa l'Internet 125

Memex : 125
Le protocole de communication 134
TCP/IP est un protocole, c'est-à-dire des règles de communication. 137
Petite histoire de Linux 146
1991 : naissance du noyau Linux 147
Pourquoi un nom de domaine ? 149
Naissance d'un produit culte 150
La « gouvernance » 151
Les deux faces de la liberté. 152
Réflexions en marge de l'histoire d'Internet par Josette Lanteigne 153
L'information est un principe organisateur 154
La technique est globalisante 155
Internet a-t-il un futur ? 156

ÉCOUTES TÉLÉPHONIQUES ET CAPTURE DES TÉLÉCOMMUNICATIONS **159**

Introduction à l'espionnage économique : 161

Danger de la sous-traitance 162

Préambule 165

Le maillon faible 165

Télégraphe et secret 166

Les problèmes du télégraphe optique de Chappe 166
Le télégraphe électrique 166

Le téléphone 167

Piratage physique des installations téléphoniques : 167

Les guerres et les écoutes téléphoniques 167
L'histoire de la Source K. *(Extrait de « Résistance PTT »)* *167*
L'écoute en temps réel d'une ligne par un micro sucre : 174
Raccordement sur une ligne analogique : 175
Un fait historique d'écoute microphonique 175
Liaisons numériques et analogiques : 186
L'affaire du Canard Enchaîné 186
Liaison numérique / numérique : 187
Écoutes téléphoniques sauvages par les fonctions soft 188
Écoute par la fonction de décroché automatique : 188
Écoute téléphonique par la fonction conférence : 188
Écoute par la fonction double appel : 189
Écoute par fonction priorité d'appels vers l'extérieur : 189

Affaires contemporaines d'écoutes téléphoniques 190

Un roman-feuilleton policier à l'américaine 190
Affaire des écoutes de l'Élysée 195
Le procès des écoutes de l'Élysée sous Mitterrand débute le lundi 15 novembre 2004 195
Le Monde (15 novembre 2004) « grandes oreilles de l'Élysée » 196
Tf1 (17 novembre 2004) « Les petites oreilles » de l'Élysée à la barre 197
Le Parisien, jeudi 18 novembre 2004, « Dès le départ, il y a eu des dérapages » 197
Le Parisien, jeudi 25 novembre : Le commandant Beau tient sa revanche 198
Le Parisien, lundi 29 novembre 2004, Écoutes : Quilès n'a rien vu, rien entendu 199
Liberation, mercredi 01 décembre 2004, Écoutes : au service secret de sa majesté Mitterrand 200
Libération, vendredi 03 décembre 2004, Écoutes de l'Élysée : Joxe charge Mitterrand et pleure 202
Libération, 23 février 2005 Le procès des écoutes de l'Élysée, Les oreilles de Mitterrand ne rougissent pas 203
Libération, Novembre 2005 Le procès des écoutes de l'Élysée 204
Libération, jeudi 10 novembre 2005, Écoutes téléphoniques : les leçons d'un procès 205
Le jugement 205
Djokhar Doudaev tombe dans le piège 207

Quelques affaires de plus... 208

Cambriolage à France Télécom: 208
Des opérateurs non contrôlés : 208
Le CNCIS épingle les officines et opérateurs : 209
Les « grandes oreilles » de la France 210
Les moyens d'enregistrement téléphoniques : 210
Système d'interception ou d'écoute électronique téléphonique automatique : 211
Nouveau service France Telecom : l'espionnage gratuit ! 212
Le Busch à oreilles.. 213

Les portables aussi... 214

Les radiotéléphones : 214
1-Micro espion GSM (Fiche du revendeur) 214

Autres systèmes en vente libre 215

Diagramme d'un réseau simple de GSM 218
Comment opérer un système d'interception passif : 218
Fonctionnement : 218
Composition du système : 219
Fonctions du système : 219
Les écoutes officielles : 219

Conclusion : 220

À L'ÉCOUTE DES ONDES 221

Les moyens hertziens et la perte de confidentialité des communications : 223

Les ondes, le moyen le moins sûr de communiquer. 223
La tragique affaire Szek 223
La Radio et la Résistance 224
Le 31 mai 1942 à 2 heures du matin... 225
Piratage et écoute d'une base TSF : 232
Transmissions informatiques radio sans fil : 233
Les faisceaux hertziens : 234
Transmissions informatiques infrarouges (IR) : 234

Les gadgets d'espionnage électronique : 235

Les microémetteurs : 235

Les caméras CCD : ... 235
Des moyens variés : ... 236
Systèmes informatisés d'interception radio : ... 237
Les moyens d'enregistrement radio : ... 237

Espionnage de tous les systèmes sans fil ... ***238***

Une mise en garde est aussi a effectuer sur tous les équipements sans fil : ... 238

« ECHELON »LE RÉSEAU MONDIAL QUI VOUS ÉCOUTE **241**

La chronologie du Réseau ... ***243***

Glossaire ... ***259***

Historique de la National Security Agency. ... ***265***

Introduction ... 265
1 — Qui sont la NSA et le NRO ? ... 265
Le pacte UKUSA ... 265
Le budget de la NSA ... 265
2 — Le NRO (National Reconnaissance Office). ... 266
Historique et présentation ... 266
Budget et fonctionnement. ... 266

Principe général de fonctionnement du réseau ECHELON ... ***267***

Les antennes d'interception dans le monde ... 267
Méthode d'interception ... 268
Exemples d'écoutes commerciales ... 269
Moyens matériels et humains ... 269
Antennes, satellites, ordinateurs et réseaux ... 269
Les antennes ... 269
Les satellites ... 270
Ordinateurs et réseaux ... 271
Les différents types d'écoutes ... 272
Satellites ... 272
Câbles sous-marins ... 273
Internet ... 273
Radio (Micro-ondes, HF, etc.) ... 275
Le personnel humain ... 276
Conclusion ... 276
Perspectives ... 277

Le pacte UKUSA ... ***278***

Les affaires ... ***283***

Les technologies : ... ***287***

Les Dictionnaires ... 287
Les antennes ... 287

Alliés ... ***295***

L'Allemagne ... 295
L'Australie ... 297
Le Canada ... 299
Le Danemark ... 301

Le Royaume-Uni ... 302
Chypre ... 306
L'ancienne station de Hong-Kong ... 307
Le Japon ... 307
La Nouvelle-Zélande ... 310
La Suisse ... 313
Taiwan ... 316

Sources ... 317

La place de la NSA en Europe ... 332
Les révélations du Néo-Zélandais Nicky Hager ... 335
À l'écoute des communications radiotélégraphiques ... 337
Un acte constitutif resté secret jusqu'à aujourd'hui ... 340
Quelqu'un écoute ! ... 356
Synthèse des apports de Nicky Hager ... 358
Vers un projet européen ... 362
Pretty Good Privacy ... 363

Une évaluation des techniques de contrôle politique ... 371

Microsoft et la NSA complices ? ... 387

LES MOYENS DE GARDER LE SECRET DES TÉLÉCOMMUNICATIONS 393

Préface ... 395

ÉCRITURE ET CODES 399

L'aventure des écritures ... 401

Chronologie sommaire ... 401

Généalogie du signe et mémoire du graphe ... 403

L'écriture et les écritures secrètes ... 405

L'écriture cunéiforme ... 405
Premières tentatives de traduction ... 405
Connaissance moderne de l'écriture cunéiforme ... 407
Les hiéroglyphes ... 408
L'écriture pictographique hittite ... 408
Les écritures crétoises ... 409
Les proto-alphabets cananéens ... 409
Les idéogrammes chinois ... 409
L'écriture hiéroglyphique des Mayas ... 410
Le plus vieux document chiffré ... 411
Les écritures codées ... 412
Le chiffre des Templiers ... 412
Cryptogramme du Forban. ... 412
Le manuscrit de Voynich ... 413
Autres écritures secrètes ou indéchiffrables, langues inconnues ... 415
Codex Seraphismus ... 415
Codex Rohonczi ... 415
Écriture de Timothy C. Ely ... 416
Le disque de Phaïtos ... 417

L'ART DU MESSAGE SECRET 419

La Stéganographie **421**

La Stéganographie : un texte peut en cacher un autre... 423

Un procédé de stéganographie de texte moderne : les pages HTML. 429

Un texte dans une image 431

Le marquage des images 433
Images matricielles (ou images bitmap) 434
Images 2D + t (vidéo), images 3D, images multi-résolution 434
Images stéréoscopiques 435
Images vectorielles 435
Définition et résolution 435
Représentation des couleurs 435
Images 24 bits (ou « *couleurs vraies* ») 436
Images à palettes, images en 256 couleurs (8 bits) 436
Images en teintes (ou niveaux) de gris 437
Images avec gestion de la translucidité 437
Structuration, utilisation de métadonnées 437
Formats d'images 438
Tableau comparatif 438
Formats propriétaires 438
Image numérique et droits d'auteur, une application de la Stéganographie 439
Protection par signature visible 439
Protection par signature cryptée 439
Attaques sur les marquages 440
Commençons par le premier type d'attaques 440
Technique de Watermarking tenant compte de la corrélation HVS-Canaux RGB 442
Marquage sur les bits de poids faibles 443
Signature par modulation d'amplitude sur les images couleur 445
Watermarking par DCT à taille de blocs variable 445
Un regard sur la seconde génération de watermarking 446
Watermarking par modification géométrique 447
Une image dans une image ? 448
Que fait StegaIn ? 449
Les masques 450
Extension de la théorie 450
Utilisation de StegaIn et StegaOut 452
Application 452

La cryptographie **455**

Les grandes dates de l'histoire de la cryptographie 456

La cryptographie, ou l'art du code secret 461

Méthodes par substitution 462
Le chiffre de César 462
Le chiffre de Wolseley 462
Le carré de Polybe 463
Le chiffre bifide de Delastelle 464
Faiblesse du procédé par substitution 465
Le chiffre polyalphabétique 466
La loi de Kerkchoffs 475
Vers la mécanisation et l'automation du cryptage 476
La machine de Hebern 477
Typex 479

SIGABA 480
La machine de Lorentz 481

ENIGMA **483**

Le concept de guerre de mouvement 488
L'intérêt d'Enigma 488
Les différentes machines 489
Procédure de cryptage et d'émission d'un message 490
Principe et fonctionnement de la machine Enigma 492
Schéma électrique de la machine et composants 493
Le réflecteur 496
Casser le chiffre d'Enigma : un exploit 496
La clef 496
Nombre de réglages possibles pour l'orientation des rotors et de leurs bagues 497
Nombre de réglages possibles au niveau de l'ordre des rotors 497
Nombre de réglages possibles au niveau du tableau de fiches 497
Nombre de clefs différentes possibles 498
Comparatif de différentes machines Enigma 498

À l'attaque d'Enigma ***501***

Contexte historique des années 20. 501
Le long travail du Bureau du Chiffre 507
Le décryptement de l'Enigma navale 517
La bataille d'Angleterre 519
L'Afrique du Nord 519
Les armes de la terreur : V1 et V2 519
Opération Overlord : le débarquement en Normandie 520

AUTRES MACHINES MÉCANIQUES, ÉLECTROMÉCANIQUES ET ÉLECTRONIQUES À CRYPTER LES TEXTES **523**

Autres machines à crypter ***525***

CRYPTER LA VOIX **533**

Green Hornet, ou le frelon vert 535
SIGSALY 536
Le PCM 538
Les clés de SIGSALY 539
Les autres matériels de codage de la voix 540
La technologie « Flyball » 541
STU-III 542
STANAG 4591 543
Communications radio cryptées 545
BID/150 545
Fascinator 546

CRYPTAGE ET NOUVELLES TECHNOLOGIES **549**

Introduction 551

Les aventures d'Alice et Bob ***553***

Utilisateurs légitimes : 553
Adversaires : 553
Tierces parties : 553
Preuve à divulgation nulle de connaissance : 554

Fonctions recherchées dans la cryptographie numérique : 554
Les deux types de chiffrement possibles : symétrique et asymétrique 554

Les principaux outils de chiffrement symétrique 555

Kerberos 555
DES 557
Les attaques sur DES 558
AES 560
Histoire 560
Fonctionnement 560

Le cryptage asymétrique, invention de la clé publique 561

RSA 562
Le protocole de cryptographie RSA : 562
Exemple : 564
Points forts et faiblesses : 565
Petits commentaires au sujet de RSA 566
Les certificats numériques 567
Signature et authentification 568
PGP 568
Les protocoles 568
Les attaques révélées sur les divers protocoles 569
Cryptanalyse moderne 570
Attaques sur les systèmes asymétriques 574

La cryptographie quantique 575

La cryptographie quantique, une idée lumineuse 577
La physique quantique 577
La mécanique quantique 579
L'information quantique 579
Étrangeté quantique 580
Conséquence : copie interdite 581
Opérations quantiques 582
Circuits quantiques 584
Enchevêtrement, Intrication quantique 585
Téléportation quantique 586
Ordinateurs classiques et ordinateurs quantiques 589
Ordinateur quantique : rêves ou réalité 591
Quelques modèles avancés 591
Applications 592
Pragmatisme quantique 593
Applications pratiques 596
La cryptographie quantique emprunte les airs 597
Les réseaux quantiques 597
Test d'un réseau informatique à cryptographie quantique réussi 597
Record de distance pour le transfert quantique 598
La cryptographie quantique sécurise les votes (en Suisse) 599

Conclusion 600