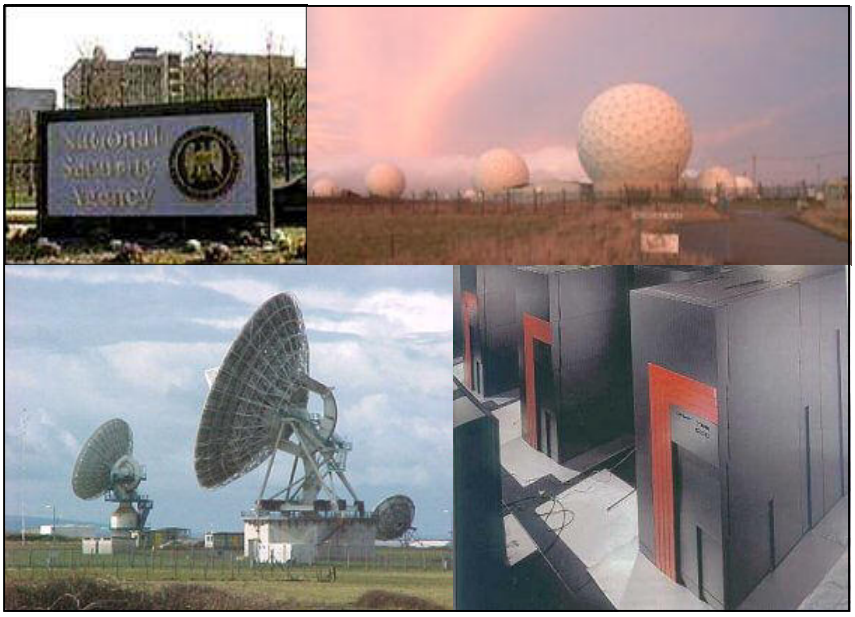
Université de la Méditerranée
Institut Universitaire de Technologie
Département GTR

Projet de communication

Enseignant : René Massi

Echelon



Le pouvoir du secret

Cabos Lilian Dequidt Davy Jacob Fabien

SOMMAIRE

1. La NSA

➢ La 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.
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'accord BRUSA-SIGINT

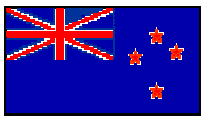
Le printemps 1943 vit la signature de l'accord BRUSA-SIGINT ainsi qu'un échange de personnel. Le contenu de l'accord, qui concerne notamment le partage du travail, est en résumé l'échange de toute information provenant de la découverte, de l'identification et de l'écoute de signaux, ainsi que des algorithmes des codes et clés de cryptage. Les Américains étaient compétents pour le Japon; les Britanniques pour l'Allemagne et l'Italie.
Après la 2nd guerre mondiale, 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 Etats-Unis (CommonWealth).

➢ 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.
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 1947.

➢ 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. A cet accord de base furent bientôt ajoutés les réseaux de trois pays du Commonwealth, le Canada, l'Australie et la Nouvelle Zélande.
Les organisations ainsi rassemblées sont:

	Etats-Unis **La N.S.A** : National Security Agency Employés : entre 38 000 et 40 000 (dont 20 000 au Q.G de la N.S.A) Budget : environ 3,6 milliards de $ par an Nom de code : Oscar	
	Royaume-Uni **Le G.C.H.Q** : Government Communications Headquarters Employés : environ 15 000 Budget : environ 730 millions de $ par an Nom de code : Alpha	
	Canada **Le C.S.E** : Communications Security Establishment Employés : environ 900 Budget : environ 70 millions de $ par an Nom de code : Uniform	
	Australie **Le D.S.D** : Defense Signals Directorate Employés : environ 1000 Budget: Non connu Nom de code : Echo	
	Nouvelle-Zélande **Le G.C.S.B** : Governement Communications Security Bureau Employés : environ 250 Budget : environ 20 millions de $ par an Nom de code : India	

Source 2002

L'accord UKUSA répartit les équipements, les tâches et les résultats entre les gouvernements signataires.
Grâce à la répartition géographique des 5 associés, une surveillance des communications mondiales est possible. Toutes les informations collectées sont gérées par ces 5 agences.

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 d'interception sont gérées officiellement par des militaires, qui assurent au moins pour partie ces interceptions. Ces dispositions garantissent un contrôle militaire strict des installations tout en permettant d'en camoufler les activités.

2. *Le réseau Echelon*

➢ La présentation

L'opération Shamrock commença dés 1945, les 3 plus grandes compagnies de télécommunication américaines : Western Union, RCA et ITT, fournissaient quotidiennement à la NSA des transcriptions de tous les télégrammes entrant et sortant des états-Unis. Un télégramme sur 40 étaient analysé, soit plus de 150 000 messages pas mois. Shamrock dura plus de 30 ans.
L'opération Minaret commença en 1967, la NSA écoutait des pacifistes américains contre la guerre du Vietnam, ainsi que des militants pour l'égalité des droits civiques : Jane Fonda, Martin Luther King, et MalcomX été des cibles de 1er plan. Plus de 6000 étrangers et 1700 organisations ont été espionnés.
Découvertes, ces actions ont choqué le public américain, qui voulait en savoir plus sur l'activité des services secrets.
En 1970 des lois ont-été voté pour mettre fin au programme Shamrock et Minaret mais l'année suivante une nouvelle base d'écoute a été construite au USA et l'espionnage des communications continua, ces écoutes se faisaient directement aux satellites : Echelon venait de naître.

Echelon est un système d'écoute des télécommunications, formé de radars, antennes et ordinateurs qui captent toutes formes de communications (comme les communications téléphoniques, radio, les e-mails, …).

Interceptions

Chaque pays qui collabore avec Echelon définit une liste de mots clés (ou keywords) que les messages ou communications doivent contenir pour être interceptés, ce sont les dictionnaires. Mais il ne suffit pas que le message ou la communication contienne tel ou tel mot clé, il faut qu'il ait un sens, sinon l'ordinateur le refusera immédiatement. Les ordinateurs comprennent le contenu sémantique de l'information.

Traitement

Les messages sont ensuite traités par des super-calculateurs, par exemple des Cray que la NSA utilise. Ces ordinateurs sont capables de casser le cryptage des messages ou des communications. De plus, comme la plupart des produits de sécurité actuels sont américains, ils ne sont pas fiables et contiennent des "BackDoors" qui permettent à la NSA de lire le message sans aucun problème. En effet, une loi aux Etats-Unis interdit l'exportation de produits de sécurité (Cryptage, firewall, stéganographie...). Le seul moyen pour exporter le produit est de la faire vérifier par un organisme de contrôle, qui verra le code source, et autorisera ou non l'exportation. Mais en cherchant plus loin, on peut découvrir que ces organismes dépendent en réalité de la NSA! Elle pose donc une condition pour l'exportation : l'affaiblissement des clés de codage pour pouvoir casser le message plus facilement ou une backdoor. Le créateur du produit n'a pas d'autre choix que d'accepter pour ses intérêts commerciaux. Tous les produits américains sont donc piégés par la NSA (Exemple le plus connu : Windows de Microsoft).

Partage de l'information

Une fois les messages interceptés et triés, c'est la NSA qui décide ce qu'elle partage avec les autres pays membres. Les éléments interceptés sont ensuite transmis à chaque agence par l'intermédiaire d'un système informatique du nom de PLATFORM, centre nerveux qui relie chaque agence UKUSA depuis 1983, basé au QG de la NSA à Fort Meade, (Maryland).

➢ Les Technologies

Sur terre

Les antennes terrestres

Etant donné que les satellites INTELSAT furent les premier 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, mises 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 écouter ces trois satellites.
Au début des années 1970, Yakima fut créée dans le nord-est des Etats-Unis; en 1972/73, Morwenstow fut créée dans le sud de l'Angleterre. Yakima disposait de deux grandes antennes (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 satellites ne permettaient plus de capter le totalité des communications.
Ainsi, à la fin des années 70, Sugar Grove fut construite dans l'Est des Etats-Unis (elle existait déjà pour écouter les communications russes); elle entra en service en 1980. A la même époque, une station fut mise en place à Hong-Kong. Dès lors, dans les années 80, les quatres stations - Yakima, Morwenstow, Sugar Grove et Hong-Kong - permettaient l'écoute globale des communications INTELSAT.

Satellites en orbite au-dessus de l'océan Indien

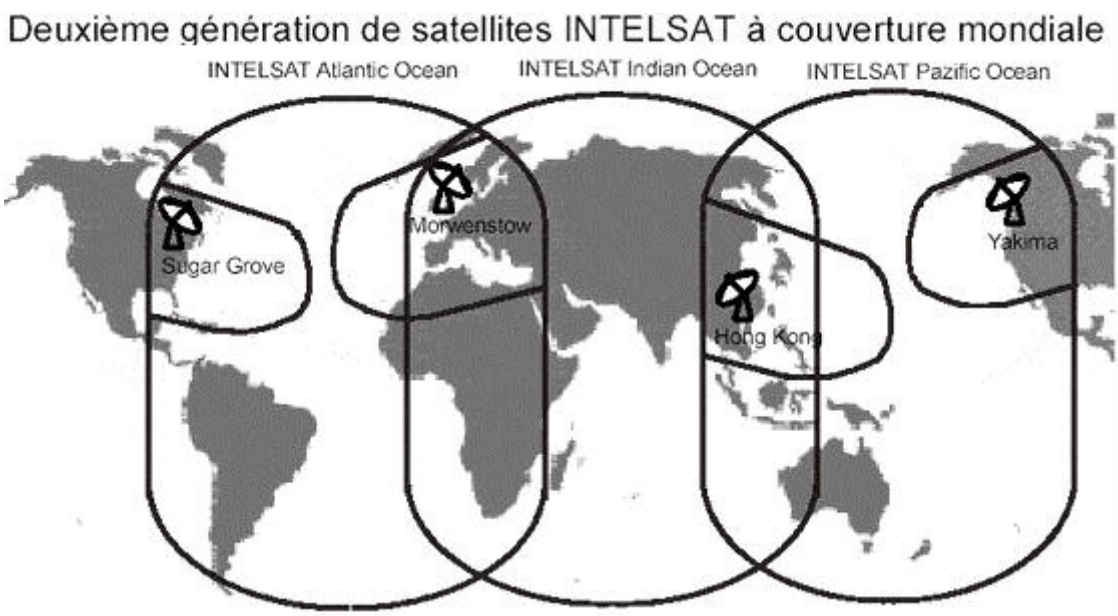
Satellites ciblés	Stations d'interceptions
INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E)	Geraldton, Australie Pine Gap, Australie
EXPRESS 6A (80°E)	Morwenstow, Royaume-Uni
INMARSAT zone indienne	Menwith Hill, Royaume-Uni Geraldton, Australie
INTELSAT APR1 (83°), APR-2 (110.5°)	Pine Gap, Australie Misawa, Japon

Satellites en orbite au dessus du Pacifique

Satellites ciblés	Stations d'interceptions
	Waihopai, Nouvelle Zelande
INTELSAT 802 (174°), 702 (176°), 701 (180°)	Geraldton, Australie
GORIZONT 41(130°E), 42 (142°E), LM 1 (75°E)	Pine Gap, Australie
INMARSAT zone pacifique	Misawa, Japon Yakima, Etats-Unis: uniquement Intelsat et Inmarsat

Satellites en orbite au dessus de l'Atlantique

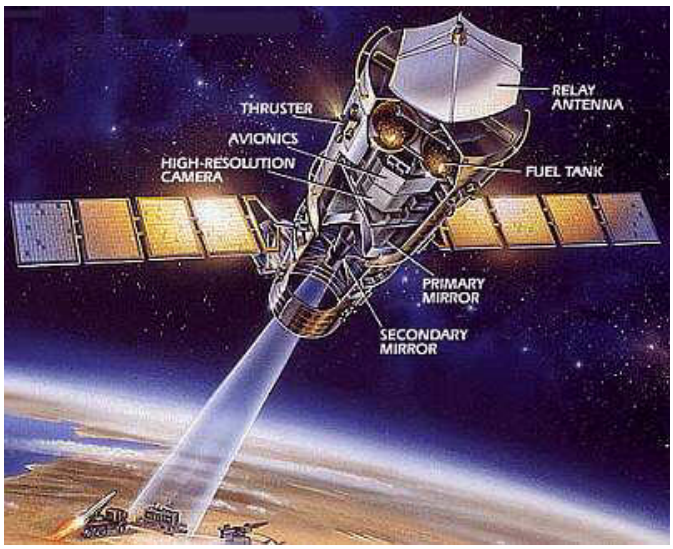
Satellites ciblés	Stations d'interceptions
INTELSAT 805 (304,5°), 706 (307°), 709 (310°)	Sugar Gove, Etats-Unis
601 (325,5°), 801 (328°), 511 (330,5°), 605 (332,5°)	Buckley Field, Etats-unis
303 (335,5°), 705 (342°)	Sabana Seca, Puerto Rico
EXPRESS 2 (14°W), 3A (11°W)	Morwenstow, Royaume-Uni
INMARSAT zone atlanrique	Menwith Hill, Royaume-Uni
INTELSTAT 707 (359°)	Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni



Dans l'espace

Les satellites espions KeyHole (KH) :

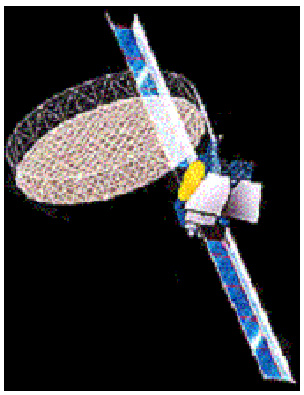
La technologie utilisée dans les satellites de reconnaissance militaire représente un des secrets les mieux gardés au monde. En 1959, les Américains lancent le premier modèle : KH-1 Corona, lancé en 16 exemplaires (dont 7 échecs). Ces satellites utilisaient des cartouches de film récupérables qui revenaient sur Terre à bord d'une capsule munie d'un bouclier. Aujourd'hui, cette technologie est abandonnée et a été remplacée par la transmission numérique des images au sol, parfois même en temps réel. La durée de vie de ces satellites atteint ainsi, ou même dépasse, les trois années sur orbite.
Le premier KH-11, nom de code Kennan, a été lancé le 19 décembre 1976 par une Titan 3B. Il possède une résolution de 15 centimètres. Ce satellite avait une masse de 11,6 tonnes pour une longueur totale de 13,48 m et 4,3 m de diamètre. Il était alimenté par deux panneaux solaires fournissant 5 kW d'électricité. Mais surtout, son objectif était formé d'un miroir de 2,3 m de diamètre lui assurant une définition exceptionnelle.
Le dernier KH-11 a été placé sur orbite en 1988. Deux ans plus tard, l'armée américaine lançait la série des KH-12 (nom de code Crystal). Il avait les mêmes caractéristiques que le KH-11, mais était beaucoup plus lourd : près de 20 tonnes. L'augmentation de poids est due à un système de capteurs plus perfectionnés et capables de travailler jusque dans le proche infrarouge, ainsi qu'à l'embarquement d'une quantité supérieure de carburant pour permettre davantage de possibilités de manœuvres et une durée de vie plus longue.
Puis en 1995, une nouvelle version du KH-12 "Improved Crystal", est lancée. Cette fois-ci, son poids est de 27 tonnes, et il a une résolution au sol inférieure à 10 centimètres, de nuit comme de jour, même avec une couche nuageuse. Avec le KH-12 Improved Crystal, on peut presque identifier un visage.



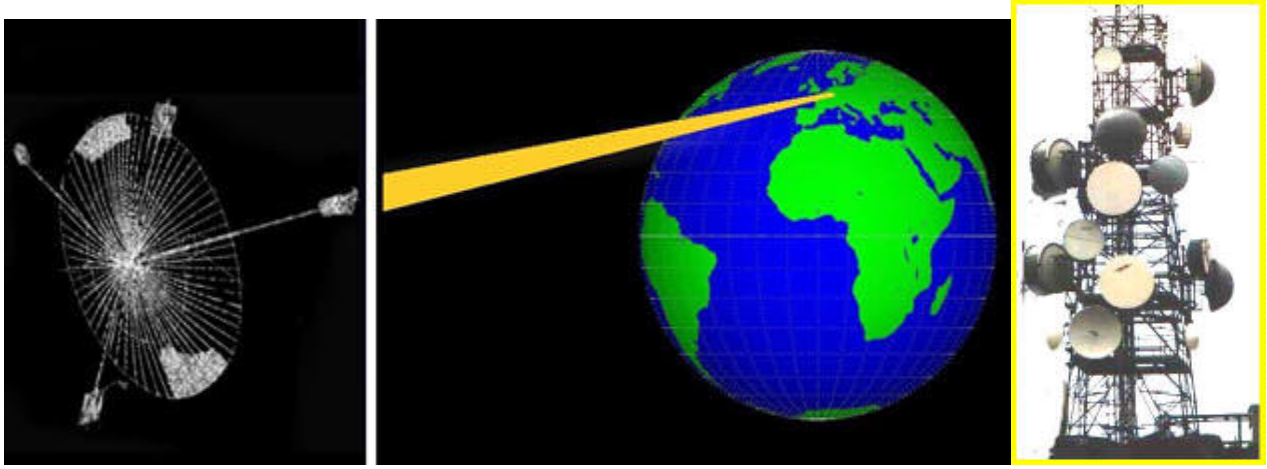
Satellites espions KH-11
AFB en Californie, depuis une Titan 4

Lancement d'un KH-11 à Vandenberg

Les satellites espions de télécommunications :



La NSA possède plusieurs satellites qui servent à espionner les communications. Ces satellites ont pour nom de code Magnum, Mentor, Orion, Trumpet, Mercury, Advanced Vortex.
Les télécommunications par voie de micro-ondes qui transportent nos communications interurbaines se propagent en lignes droites, de tours relais en tours relais distantes de 30 à 50 km. A la fin des années 60, les américains se sont rendus compte que l'énergie dépassait les tours relais et se perdait dans l'espace. En plaçant un satellite d'écoute au bon endroit dans l'espace, on pouvait intercepter toutes les communications. Vu le succès de ces interceptions, les américains développèrent de nouveaux satellites capables de cibler sur demande nos téléphones, données informatiques…
Ces satellites de 100 mètres de diamètre coûtent 1 milliard de dollars par exemplaire. L'Amérique est le seul pays à posséder de tels satellites, et même ses partenaires n'y ont que partiellement accès.



Satellites en orbite géostationnaire, comme Vortex, qui interceptent les télécommunications micro-ondes (IC-2000, Duncan Campbell)

Sous l'eau

Opération Ivy Bells - Années 1970 à 1981, dans la Mer d'Okhotsk

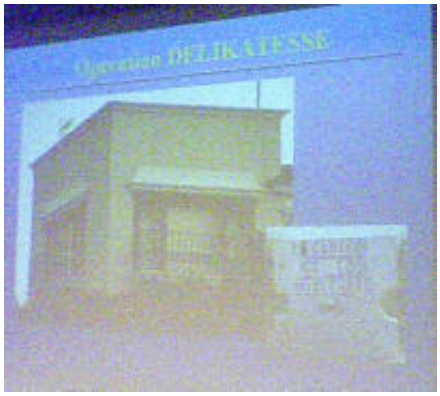
Le gouvernement américain a appris l'existence d'un câble sous-marin connectant les bases navales soviétiques principales à Vladivostok et Petropavlovsk. Une des premières missions fut réalisée en 1971 par l'USS Halibut (SSN-587). Elle consistait à installer un manchon autour du câble. Cette bretelle (développée par la NSA) pouvait intercepter toutes les communications transitant par le câble en captant les émissions électromagnétiques sans avoir à ouvrir celui-ci, ce qui aurait put être détecté. Au cas où les Russes auraient voulu exécuter une opération de maintenance, le manchon se serait détaché et serait tombé au fond de la mer. Toutes les 6 à 8 semaines, un sous-marin venait chercher les enregistrements et remettait en place une nouvelle bande. Les Russes étaient sûrs de leurs moyens de communication et les conversations n'étaient pas protégées. Mais en 1981, un bateau de sauvetage russe récupère le dispositif d'espionnage. Après des investigations, la NSA découvre un traître : Robert Pelton a vendu aux Russes en 1980 des informations confidentielles sur cette opération pour 35 000 $. Le manchon récupéré par les Russes en 1981 est désormais exposé dans le musée du KGB (l'ancien quartier général de KGB) à Moscou.

Un nouvel enjeu : l'interception des fibres optiques

La fibre optique, nouveau moyen de communication, pose de sérieux problèmes à la NSA. Le premier, c'est l'interception; en effet, une fibre optique n'émet pas de radiations électromagnétiques, les manchons ne peuvent donc pas servir. Le seul point faible de cette technologie, c'est la perte de signal. Sur de grandes distances, le signal lumineux faiblit et doit être amplifié à nouveau. Il passe par ce qu'on appelle un répéteur, qui transforme le signal optique en signal électrique, amplifie et retransforme à nouveau ce signal en signal optique. Il y a des répéteurs tous les 100 ou 150 km environ. C'est donc sur ces boîtiers que peut se fixer la NSA pour espionner. Le deuxième problème qui se pose, c'est le traitement des données de ces fibres optiques, qui ont une capacité gigantesque et largement supérieure aux autres moyens de communication. La NSA a donc énormément de mal à traiter l'information de ces fibres, perdue dans la masse de données. La fibre optique est le nouveau challenge de la NSA.

Opération Delikatesse

Opération Delikatesse consiste à effectuer des interceptions en posant des dispositifs sur les câbles sous-marins qui passent sous la mer en Méditerranée, voire sur les câble transatlantiques. Cela n'est possible à l'heure actuelle qu'au niveau des répéteurs.



Cette maison ressemble peut être à une magnifique villa de bord de plage, sauf que c'est aussi là qu'on retrouve une partie des moyens techniques nécessaires à l'interception des câbles sous-marins. On ne peut se brancher sur un câble fibre optique sans déclencher une alarme chez l'opérateur ou sans sa complicité. On peut donc aussi faire de l'interception sur les derniers points de raccordement terrestres avant qu'ils ne partent à l'eau, ou encore sur les points de destination.
On peut aussi intercepter les micro-ondes des faisceaux hertziens, voire satellites, qui sont en amont ou aval de ces station de distribution pour les câbles sous-marins en fibre optique.

Les ambassades : lieux d'écoutes

D'autres lieux d'interception : les ambassades. L'exemple le plus flagrant est bien évidemment celui des Etats-Unis. Le matériel arrive dans l'ambassade par valise diplomatique, il peut se composer d'une petite antenne et d'un enregistreur que l'on installe dans un placard mais il peut aussi prendre tout un étage.
Par exemple, a Paris, le dernier étage de l'ambassade américaine n'a pas de fenêtres et il y a sur le toit une sorte de structure en verre abritant un mini dôme. Selon Mike Frost un ancien agent du CSE Canadien, ceci est sûrement une antenne d'écoute, elle permettrait d'écouter le parlement qui est la cible n°1, mais aussi le bureau du 1er ministre, les autres ambassades étrangères ainsi que toutes les cibles potentiels dans la zone.
Aucun moyen d'empêcher cela car l'ambassade est protégée par l'immunité diplomatique. Mais les Etats-Unis ne sont pas les seuls à avoir eu cette idée. La Russie par exemple utilise aussi ce moyen (l'ambassade de Russie à Buenos Aires a un système d'écoute très développé). La France utilise aussi cette méthode.

3. Les actions d'Echelon

1972 : Watergate

Un trop grand pouvoir est synonyme de dérapage.

Elu président des États-Unis en 1968 et nouveau candidat pour le parti républicain en 1972, Richard Nixon fait procéder à des écoutes téléphoniques illégales au siège du parti démocrate durant la campagne électorale.
Tout commence par l'arrestation dans la nuit du 17 juin 1972 de cinq cambrioleurs qui ont pénétré dans l'immeuble du Watergate à Washington où se trouve le quartier général du parti démocrate et c'est alors que commence une chasse à l'homme dans laquelle la grande presse nationale tient le rôle du chasseur et le président celui du gibier. Les policiers découvrent que les cambrioleurs ont des liens avec le comité pour la réélection du président Nixon.
Deux reporters du Washington Post Carl Bernstein et Bob Woodward ne se contentent pas de l'enquête officielle. Les enquêtes de ce journal conduisirent à l'inculpation du président Nixon et révélèrent un plan d'action gouvernemental consistant en un espionnage systématique de l'opposition politique. Le scandale qui en résulta contraignit ce dernier à démissionner en 1974.

La politique américaine

En théorie, les Etats-Unis devaient cibler, grâce au réseau échelon, ses ennemis, mais en pratique pas du tout. Ils ciblent leurs alliés et leurs partenaires commerciaux.
Dans les années 90, une fois le bloc communiste dissout, les services secrets américains, n'ayant plus d'ennemie à écouter, se demande à quoi ils pourraient servir.
Sous l'impulsion du président des Etats-Unis de l'époque Bill Clinton, une nouvelle fonction leurs est assignés. Ils se sont intéressé à des sociétés comme Airbus, et à ses marchés potentiels, ses clients, ses prix de vente, sa gamme de produits etc.
Ses informations sont ensuite envoyés à leurs concurrents américains, afin qu'ils puissent modifier leurs offres en fonction de ces informations.
Cette nouvelle politique économique a permis au Etats-Unis de remporter près de 70 marché de grande importance, faisant gagner plusieurs milliards de dollars aux entreprises américaines leurs permettant de créer des dizaines de milliers d'emplois.

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 ont été collectées sont transmises à Boeing et Mc Donell-Douglas. Ce dernier a obtenu le marché.

1994-96 : Enercon

L'ingénieur A. Wobben, de la société Enercon, 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 $.

1994 : Projet Sivam

James Woolsey, un ancien directeur de la NSA, indique que si les américains ont recours à ses pratiques c'est parce que les européens usent de pots de vin pour conquérir des marchés dans le tiers monde.

Une affaire illustre particulièrement bien l'hypocrisie de la version américaine, en 1994, le Brésil lance un appel d'offre internationale autour du projet SIVAM.
L'objectif est d'assurer la couverture radar de l'Amazonie, un marché stratégique de 1.4 milliard de dollars.
Raytheon l'américain fait concurrence à Thomson CSF le français.
Thomson pense remporter le marché mais quelques jours avant que l'affaire ne soit concluse, un scandale éclate dans les journaux américains : grâce à la NSA, des tentatives de corruptions de hauts fonctionnaires brésiliens par le groupe français auraient été déjoués.
Raytheon remporte finalement le marché. Le réseau échelon aurait permis d'écouter ses conversations.
Mais quelques mois plus tard la presse brésilienne publie des articles qui démontrent que Raytheon la compagnie américaine à corrompue elle aussi des fonctionnaires brésiliens.

Autre écoutes …

D'après Fred Stock, ancien agent canadien lui aussi, lors d'un interview, déclare que des agences comme la croix rouge, Greenpeace, ou Amnistie international étaient sur écoute.
La princesse Diana lors de sa lutte contre les mines anti-personnelle a été ciblée, même la reine d'Angleterre ou le Pape.
Où allaient-ils? Qui voyaient-t-ils? Qui leurs rendaient visite? Ils en savaient beaucoup sur la vie de ses gens là.

4. L'opposition à Echelon

Le Jam Echelon Day

Le principal objectif du Global Jam Echelon Day ('Journée de brouillage d'Echelon', exécutée en 1999 et le 21 octobre 2001) est d'attirer l'attention du public sur l'existence d'Echelon et d'appeler à un contrôle accru des agences gouvernementales qui en ont la charge. L'échec de la surveillance électronique généralisée à prévenir les récents attentats (11 sept 2001) ne fait qu'inciter à dénoncer le gaspillage d'un tel espionnage généralisé des télécommunications.

L'idée du Jam Echelon Day est de submerger Echelon d'emails truffés des mot-clefs auxquels il est censé réagir, afin de saturer les super-ordinateurs, comme des vulgaires PC sous Windows. Voyez les sites du JED (Bug Brother et cipherwar) ainsi que le générateur de mots-clés de Bug-Brother.

Au-delà de cet évènement, plus symbolique qu'efficace (on peut en effet penser que les algorithmes d'Echelon sont suffisamment élaborés pour reconnaître et ignorer le spam), le groupe des Hacktivistes cherche à informer et à faire réagir face à la menace que constitue le big brother américain.

Un virus anti-Echelon

Le virus echelon.vbs qui circule sur internet fonctionne sur le même principe. Ce "ver" se propage dans les boites à emails à la façon du célèbre "ILOVEYOU", sans toutefois provoquer de dégât dans votre PC. Les mots-clés cachés qu'il contient sont sensés attirer les "spiders" de la NSA. Une sorte de Jam Echelon Day permanent et automatisé.

Super mamies

Les super mamies sont des femmes qui luttent contre échelon à la base de Menwith Hill. Pendant des années elles ont récupéré des documents en fouillant dans les poubelles de la base, elles ont pu ainsi avoir le nom de plus de 250 systèmes et le nom d'autres bases d'échelon. Elles ont pu aussi pénétrer plusieurs fois dans la base, sans grands résultats. Dans l'ensemble leurs actions sont plutôt symboliques et n'ont pas gêné le fonctionnement de la base.

Congrès européen

En juillet 2000 le congrès nomme une commission pour enquêter sur échelon, cette commission n'a aucun pouvoir, ce qui limite son efficacité. En mai 2001, il était prévu qu'elle rencontre le directeur de la NSA et de la CIA, plus une visite de l'advocacy center ; tous ces rendez-vous sont annulés au dernier moment.
Voici un extrait du rapport du Parlement Européen:
"L'existence d'un système d'écoute des communications fonctionnant, avec la participation des États-Unis, des Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande dans le cadre de l'accord UKUSA, ne fait plus de doute. Il est vraisemblable, eu égard aux indices disponibles, qu'il est dénommé ECHELON (... et) qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires. L'analyse a montré que la puissance de ce système ne peut être aussi grande, tant s'en faut, que ce que certains médias supposent. (...) La France serait en mesure, du moins en ce qui concerne les conditions géographiques - elle est en effet le seul État membre de l'UE à posséder des territoires outre mer - de mettre sur pied à elle seule un système d'écoute mondial. Il ressort de certains indices que la Russie pourrait également exploiter un tel système. (...) Les entreprises doivent protéger tout leur environnement de travail c'est-à-dire aussi les moyens de communication servant à transmettre des informations sensibles. Les particuliers doivent eux aussi être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe."

5. Le réseau français : Frenchelon

Les satellites de la France (Essaim)

Le Ministère de la Défense se dote de satellites espions capables d'intercepter les communications téléphoniques, fax, e-mails... pour écouter le monde entier.
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 de la NSA (Echelon), en a eu également connaissance.
"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 un système d'écoute électronique spatial que seuls les Etats-Unis et la Russie possèdent aujourd'hui. Essaim - c'est son nom - surveillera à son tour l'activité radio et radar de la planète à partir d'une orbite située à 680 kilomètres d'altitude.
Ce système, constitué par une escadrille de quatre microsatellites (120 kilos), sera capable d'écouter et surveiller une zone de 200 à 2500 kilomètres de part et d'autre de la trace de sa trajectoire au sol. C'est donc des bandes de terrain allant jusqu'à 5000 kilomètres de large qu'Essaim placera sous écoute de ses antennes. Compte tenu que les quatre satellites graviteront sur des orbites perpendiculaires au sens de rotation de la Terre, celle-ci sera sous surveillance intégrale. Pas en permanence, puisqu'un même point ne sera écouté que dix minutes toutes les quatre-vingt-treize minutes.
Le système sera commandé à partir d'une station de contrôle du Cnes, installée à Toulouse, qui asssurera les opérations de télécommande et de télémesure des satellites en orbite.
Quant à la propagation des missions et au traitement des signaux, recueillis à partir de l'espace, ils reviendront à une autre station, installée au Celar (Centre d'Electronique et de l'Armement) de Bruz, près de Rennes.

Base de Domme, Sarlat (Dordogne)

C'est l'un des plus grands centres d'écoute du monde. Dans cette base secrète protégée par des miradors, des chiens policiers et des barbelés électrifiés, treize immenses antennes paraboliques espionnent, jour et nuit, toutes les communications internationales qui transitent par les satellites visés.

Cette base ce situe dans le Périgord, sur le plateau de Domme, à côté de l'aéroport de Sarlat. Le lieu est officiellement (et pudiquement) appelé " centre radioélectrique ". Là, le service français d'espionnage, la DGSE, surveille quotidiennement des centaines de milliers - des millions ? - de discussions téléphoniques, d'e-mails, de fichiers ou de fax. C'est le site principal des " grandes oreilles " de la République.
Ce n'est pas le seul. A l'instar des Etats-Unis et des pays anglo-saxons liés à eux, la France a, ces dix dernières années, mis en place un réseau mondial d'interception. " Le Nouvel Observateur " peut confirmer l'existence - et publier les photos - de trois autres bases d'écoutes " satellitaires " de la DGSE. L'une - dont le nom de code est " Frégate " - est cachée dans la forêt guyanaise, au coeur du centre saptial de Kourou. L'autre, terminée en 1998, est accrochée au flanc du cratère Dziani Dzaha, sur l'île française de Mayotte, dans l'océan Indien. Toutes les deux sont gérées en commun avec le BND (Bundesnachichtendienst), le service secret allemand. Le troisième centre est dans la banlieue ouest de Paris, sur le plateau d'Orgeval, aux Alluets-le-Roi. Au total, une trentaine d'antennes " couvrent " la quasi-totalité du globe, à l'exception du Nord sibérien et d'une partie du Pacifique.
Il y aura bientôt d'autres stations. Elargir son réseau d'écoute " satellitaire " est " une priorité " de la DGSE, comme l'écrit le rapporteur du budget 2001 de la défense, Jean-Michel Boucheron. A cette fin, le service secret français dispose chaque année de moyens financiers accrus. Une nouvelle station est en

construction sur le plateau d'Albion, là où étaient stockés les missiles nucléaires avant le démantèlement des silos ; une cinquième est en projet sur la base aéronavale de Tontouta, en Nouvelle-Calédonie.
Aujourd'hui, sur trois continents, les " grandes oreilles " de la République disposent donc d'une trentaine d'antennes. Mobiles, celles-ci peuvent changer d'orientation plusieurs fois par jour, selon les heures ou les objectifs du service. Tous les pays sont exposés, même les alliés. Les membres de l'Union européenne aussi ? " Bien sûr, dit ce responsable. Grâce aux satellites, on peut espionner tout le monde de chez soi. Pas de coups tordus, pas de risque d'incidents diplomatiques. C'est pour cela qu'on a tant investi... "

6. L'importance de Echelon dans le futur

Au cours de cet année (2004), la marine américaine remettra à la mer le sous-marin USS Jimmy Carter, et, ce sous-marin surpuissant dont la seule remise en état coûtera 400 millions de dollars espionnera pour la NSA les câbles sous-marin du 21éme siècle.
Ce réseau d'espionnage constitue un atout majeur pour la puissance diplomatique, militaire et économique des 5 partenaires.
L'écoute des télécommunications ne connaîtra aucune limite tant qu'elle constituera une source d'information de renseignement et enfin de compte, de pouvoir.
L'intérêt pour les Etats-Unis n'est pas forcement d'écouter la terre entière, mais c'est de créer des liens de dépendance avec certain pays. C'est aussi les encourager à ne jamais développer leur propre système autonome donc à faire en sorte que pour obtenir leurs informations ils soient toujours dépendant des USA.
Aujourd'hui une puissance qui ne maîtrise pas sa propre chaîne d'information est une puissance aveugle.
Le fait de dire que, je vous livre l'information, c'est créer un lien de dépendance qui est terrible.
Car après avec ce système, dans 90% des cas de ce que va vous demander le pays qui vous accueil, vous pouvez leur donner la véritable information mais dans les 10 % restant qui vont vraiment être très important pour vous, vous allez pouvoir les manipuler.
La guerre de l'information a commencé, la domination informationnel du globe se révèle être la nouvelle arme fournissant la toute puissance.
Les USA grâce à leur couverture informationnel global fournirait aux autres nations des comptes rendus régulier concernant notamment leur sécurité.
Ces derniers seraient alors davantage incités à travailler avec les Etats-Unis.
De même que la supériorité nucléaire été la clef du leadership lors de la guerre froide, la puissance de l'informationnelle sera la clef du pouvoir dans les guerres du futur.

L'injustice qui pèse sur ses agences c'est que l'on ne connaît que leurs échecs et jamais leurs succès, qui pour pouvoir se reproduire doivent le plus souvent restés secret.

Sources

Le système Echelon : documentaire audio-visuel, sur France 2 de David Korn-Brzoza