Le système d'interception ECHELON est-il devenu un acteur majeur de l'hégémonisme des Etats-Unis ?

Mémoire de géopolitique

du lieutenant colonel EMG Bernard ESCHBACH

14° promotion du collège interarmées de défense

Dans le cadre du séminaire « géopolitique des Etats-Unis »

Directeur de séminaire : Monsieur Nicolas Kessler

Mars 2007

FICHE DOCUMENTAIRE

1. Le système d'interception ECHELON est-il devenu un acteur majeur de l'hégémonisme des Etats-Unis ?
2. 2007_memoire_geop_Le système d'interception ECHELON_ESCHBACH.doc
3. Lieutenant-colonel Bernard ESCHBACH, Armée de Terre, Suisse
4. 12 mars 2007
5. Division C - groupe C4
6. Mémoire de géopolitique dans le cadre du séminaire *"Géopolitique des Etats-Unis"*
7. Découvert dans le courant des années quatre-vingt-dix par le grand public, le système d'interception ECHELON a suscité une large polémique au sein des institutions européennes. Rattaché à la *National Security Agency* (NSA) américaine et continuité d'une alliance datant de la Deuxième Guerre Mondiale entre pays Anglo-Saxons, ce système permet une écoute systématique des communications au niveau planétaire. Fonctionnant à la limite des juridictions nationales et internationales, ECHELON a permis à quelques entreprises américaines de gagner d'importants contrats. Malgré des dérives et des limitations certaines, ce système d'écoute reste un acteur très important dans la chaîne du renseignement américain. Son point fort, outre sa nature globale, reste sa capacité d'adaptation aux nouvelles technologies, notamment aux enjeux liés à la maîtrise de l'Internet.
8. Mots clés : USA - ECHELON – NSA – Hégémonie – Guerre de l'information.

Le système d'interception ECHELON est-il devenu un acteur majeur de l'hégémonisme des Etats-Unis ?

SOMMAIRE

INTRODUCTION

L'information, une matière première stratégique. La notion de "guerre de l'information" n'est pas nouvelle. De tout temps, la recherche du renseignement a été une priorité des décideurs. La source du pouvoir réside dans la connaissance de l'information sous toutes ses formes. Cette notion de maîtrise de l'information est un des éléments constitutifs du concept de puissance. Les états forts ont d'ailleurs toujours beaucoup investi dans leurs services de renseignement, que ce soit dans le domaine militaire ou civil.

La Guerre Froide a permis pendant des années à beaucoup d'agences de renseignement de développer des outils puissants d'écoute et d'interception des télécommunications. Les fonds consacrés étaient immenses dès lors qu'il était question de sécurité nationale ou de défense des intérêts stratégiques. Pour un certain nombre de services de renseignements occidentaux, la chute du mur de Berlin n'impliqua qu'un simple changement dans les cibles à explorer, changement qui le plus souvent ne s'est pas accompagné de diminution des effectifs ou des budgets. Un de ces organismes était la très discrète *National Security Agency* (NSA). Cette dernière continua de croître en termes de budget, de personnel et de capacités de détection et d'acquisition de l'information avec ce que l'on a appelé dans les années quatre-vingt-dix le système ECHELON.

La fin d'un monde bipolaire marqua également l'avènement de la compétition économique comme moteur des sociétés. Les notions d'intelligence économique ou de concurrence oblique sont devenues des thèmes à la mode. Les Etats-Unis ont alors été le premier pays à utiliser de manière coordonnée leurs outils de renseignement au profit d'entreprises civiles, au profit de leur recherche de puissance.

Le système d'interception ECHELON est-il devenu un acteur majeur de l'hégémonisme des Etats-Unis ?

Autrement dit, est-ce que les moyens colossaux mis en œuvre par la NSA pour rechercher et exploiter l'information en général sont rentables ? Est-ce que le méconnu système d'interception ECHELON possède les capacités de renforcer d'une manière significative l'hyperpuissance américaine ?

Afin de répondre à cette problématique, nous allons commencer par faire le point sur la notion d'information en général. Nous continuerons par une présentation du monde du renseignement américain en se focalisant sur la NSA. La présentation du fonctionnement et des capacités du système ECHELON devrait nous permettre de finalement répondre au questionnement posé.

Parler du monde de l'ombre n'est pas chose aisée. C'est d'autant plus difficile lors qu'il s'agit de décrire la NSA et le système ECHELON. Toujours méconnu du grand public, les sources de renseignement sur ces sujets sont très peu nombreuses. C'est sur Internet que l'on trouve le plus d'information. Et là encore, la plupart du temps, seuls existent quelques articles de base et quelques graphiques qui sont repris et déclinés selon les aspirations des internautes. Les sources les plus fiables proviennent d'un rapport sur le système d'interception ECHELON[1] commandité par le Parlement européen. Malheureusement, ce dossier volumineux traite principalement de problématiques juridiques, aspects que nous avons volontairement laissés de côté dans ce mémoire pour en limiter le champ.

La véracité des données présentées dans ce mémoire est donc principalement due à un recoupement des informations et à l'analyse du sérieux des sites traitant du sujet.

PREMIERE PARTIE : L'INFORMATION, UNE MATIERE PREMIERE STRATEGIQUE

1. La notion de puissance en général

Raymond Aron, dans plusieurs de ses ouvrages a donné une définition désormais classique de la puissance : *"Au sens le plus général, la puissance est la capacité de faire, produire ou détruire. J'appelle puissance sur la scène internationale la capacité d'une unité politique d'imposer sa volonté à d'autres unités. En bref, la puissance politique n'est pas un absolu mais une relation humaine"*[2]. Ailleurs il précise que *"en tant que concept politique, la puissance désigne un potentiel, non un acte, on peut définir la puissance comme le potentiel que possède un homme ou un groupe d'établir des rapports conformes à ses désirs avec d'autres hommes ou d'autres groupes"*. A cette définition générale, nous pouvons ajouter un certain nombre d'éléments, de critères constitutifs de la puissance qui vont plus tard nous aider à mettre en lumière la problématique posée :

- **Critères objectifs :** supériorité technologique, contrôle et développement du savoir, capacité normative universelle, capacité de discrimination et destruction sélective.
- **Critères subjectifs :** capacité à reproduire du sens, cohésion de la société, capacité d'ouverture.
- **Buts de toute action :** savoir, sécuriser, interdire, coopérer et développer.

Durant la période précédant la chute du mur de Berlin, nous nous sommes trouvés dans une logique de production de masse. La puissance traditionnelle était mesurée à la grandeur et à l'accumulation des moyens (soldats, canons, têtes nucléaires …) dont un état pouvait disposer, créant une hiérarchie mesurable dans l'ordre des nations.

---

[1] Parlement européen, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques,* PE 305.391, 11 juillet 2001.

[2] ARON Raymond, *Paix et guerre entre les nations*, Calmann-Lévy, Paris, 1984.

Avec la fin de l'Union soviétique et l'avènement de la mondialisation, une nouvelle ère est apparue. La puissance militaire n'est plus qu'un élément subalterne. Sa maîtrise est nécessaire mais elle n'apporte pas les moyens d'une influence réelle sur le monde. Avec le primat de l'économie, la nouvelle puissance se doit également de maîtriser les éléments culturels, l'idéologie, l'information et la communication. Si durant la période précédente, les critères objectifs étaient prédominants (Hard power), après la guerre froide, les critères subjectifs sont devenus primordiaux, c'est-à-dire la capacité à produire du sens, à assurer une cohésion de la société (Soft power).

Aujourd'hui, la notion de puissance serait à rechercher dans la maîtrise de nombreux domaines que l'on pourrait lister de la manière suivante :

- supériorité économique ;
- gestion des crises ;
- maîtrise des flux financiers ;
- maîtrise des communications ;
- maîtrise des messages ;
- adéquation entre les objectifs de société et de politique internationale ;
- production de la norme internationale ;
- maîtrise des combinaisons (interaction de l'ensemble des acteurs et des facteurs).

Un Etat puissant, ce qui nécessite donc volonté – c'est-à-dire souveraineté – se caractérise non seulement par son poids territorial, démographique et économique, mais aussi par les moyens dont il dispose pour s'assurer d'une influence durable dans le concert des nations (en termes économiques, culturels et diplomatiques). Celle-ci suppose une capacité à innover en permanence, à acquérir et conserver des parts de marché (en s'appuyant sur des firmes implantés mondialement et sur des instruments monétaires solides), à diffuser ses propres valeurs, à disposer des moyens financiers et militaires de "peser" dans l'arbitrage des conflits régionaux.

2. L'importance de l'information

Les études sur la guerre de l'information sont déjà lancées depuis longtemps outre-Atlantique. Le nombre de publications lui étant consacrées est déjà considérable. On y parle d'opérations de maîtrise de l'information, d'attaques d'objectifs transmettant des informations. Ce sont essentiellement des stratégiques qui cherchent à définir ce que pourrait être la guerre de l'information.

Les origines de la "guerre de l'information" remontent à la nuit des temps puisque d'Alexandre le Grand à Belissaire et de du Guesclin à Napoléon, tous les chefs de guerre dans un premier temps,

puis tous les dirigeants politiques dans un deuxième temps (surtout lors de la guerre froide), ont tenté d'imposer par tous les moyens leurs visées et leurs desseins à leurs ennemis.

D'un point de vue géopolitique, les nouveaux rapports de forces, qui se dessinent sur l'échiquier mondial de l'après guerre froide, ont fait apparaître de nouvelles techniques de combat. La maîtrise, le contrôle, la diffusion de la connaissance et de l'information ainsi que la protection des capacités de maîtrise, de contrôle et de diffusion de l'information sont ainsi utilisés non plus seulement comme un vecteur de connaissance et d'anticipation, mais comme une arme offensive qui fait de l'information, des systèmes d'information et des capacités informationnelles l'enjeu politico-militaro-économique du XXIe siècle.

La source du pouvoir réside dans la connaissance de l'information sous toutes ses formes, et il sera essentiel de combiner tous les moyens disponibles pour pouvoir l'intercepter et la décoder à chaque instant en vue d'obtenir une longueur d'avance majeure sur les uns et les autres.

3. L'information militaire

La "guerre de l'information" ou GI (en anglais *Infowar* ou *Information Warfare*) regroupe l'ensemble des méthodes et actions visant à infliger un dommage à un rival ou à se garantir une supériorité par l'acquisition d'information (données ou connaissances), par la dégradation des systèmes d'acquisition d'information de l'adversaire ou par des méthodes d'influence et de propagation de messages favorables à ses desseins stratégiques.

Dans le principal document public consacré aux plans prospectifs à 30 ans, le gouvernement américain construit déjà des scénarios possibles d'emploi des armes de maîtrise de l'information. Baptisé Air Force 2025[3], ce document décrit tous les domaines où s'exerce la puissance militaire. Le renforcement de la maîtrise de l'information a été réaffirmée par le Président Bush dans son rapport de stratégie national de sécurité[4] daté de 2002 dans son chapitre sur la sécurité nationale des Etats-Unis : *"Les innovations au sein des forces armées passeront par l'expérimentation de nouvelles tactiques, le renforcement des opérations communes, une meilleure exploitation des services de renseignement et la mise en œuvre des plus récentes avancées de la science et de la technologie. Nous devons transformer le traitement des informations fournies par nos services secrets et l'adapter à la nature nouvelle de la menace. Nos services de renseignements doivent être intégrés à nos systèmes de défense et fonctionner en collaboration avec ceux de nos alliés."*

[3] *Information Operations : Wisdom Warfare For 2025*, A Research Paper Presented to Air Force 2025, April 96.
[4] President BUSH, *The National Security Strategy of the United States of America*, Septembre 2002.

Concrètement et loin des classiques armements offensifs et défensifs, la doctrine de guerre de l'information défini neuf domaines principaux :

- la guerre du commandement et de la conduite des opérations
- la guerre du renseignement
- la guerre électronique
- la guerre informatique par le piratage
- la guerre de l'information économique
- la guerre des cyber-systèmes (intelligence artificielle)
- le blocus de l'information
- la guerre des systèmes d'information et de commandement (SIC)

le tout, formalisé dans un règlement *Information Operations* du quartier général de l'Armée de Terre[5]. Cette nouvelle doctrine est basée sur le concept de *Revolution in Military Affairs* (RMA). Ce concept bien connu, fruit de la révolution de l'information et des évolutions technologiques permet de gérer la chaîne du renseignement, depuis la collecte de l'information jusqu'au guidage des munitions voire la gestion médiatique des conflits. La RMA se présente comme une large réflexion prônant la suprématie de l'information comme préalable à l'emploi des forces.

4. L'information économique

La compétition économique est devenue le terrain d'affrontement principal dans ce qu'il est convenu d'appeler la recherche de puissance. Les spécialistes s'accordent pour reconnaître qu'une nouvelle révolution est en marche, fondée sur l'information et la connaissance. En effet, l'internationalisation des échanges impose aux différents acteurs économiques d'adopter une démarche anticipative (et non plus réactive) face aux changements de leurs environnements. L'efficacité de leur stratégie repose alors sur le déploiement de véritables dispositifs d'intelligence économique qui instituent la gestion stratégique de l'information comme levier majeur au service de la performance économique.

Il existe passablement de définitions de l'intelligence économique. En voici une générée par le Commissariat Général du Plan : "*L'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de délais et de coûts. L'information utile est celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par*

[5] *Information Operations*, FM 100-6, Headquarters, Department of the Army, August 1996.

l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel. Ces actions, au sein de l'entreprise, s'ordonnent autour d'un cycle ininterrompu, générateur d'une vision partagée des objectifs de l'entreprise."[6]

La notion de "concurrence oblique" est aussi parfois utilisée. Il s'agit de l'ensemble des moyens non directement économiques mis en œuvre pour emporter un marché ou pour empêcher un concurrent de l'emporter. Il s'agit aussi bien d'arguments juridiques que de pressions politiques ou de mesures protectionnistes ouvertes ou déguisées et d'espionnage économique.

La pratique de l'intelligence économique peut suivre les aspects méthodologiques suivants :

- La captation et la production du savoir :
  il s'agit de recueillir de l'information par l'intermédiaire de réseaux (formels et informels), en fait, d'accumuler le maximum de renseignements dits stratégiques ou à forte valeur ajoutée.
- La mise en œuvre d'une compétence collective :
  il s'agit de nourrir le flux informationnel de l'entreprise et de s'assurer de sa bonne circulation et de sa bonne utilisation.
- Acquisition d'une méthodologie efficace :
  une fois l'information recueillie, vérifiée et enrichie, il faut l'analyser pour lui donner du sens.
- Action et contre-action :
  l'information doit être utilisée dans des actions concrètes. Elle doit permettre d'agir ou de riposter à des mutations et des crises, ou simplement de réaliser les objectifs de croissance de l'entreprise.

Les entreprises américaines peuvent mobiliser à leur profit d'immenses moyens qui ne tiennent pas seulement à la puissance économique des Etats-Unis mais aussi à une volonté politique forte. La clef de ce système repose dans l'imbrication, encore inimaginable en Europe, entre le public et le privé. Force est de constater que les dépenses militaires et les systèmes de renseignement américains ne servent pas qu'à la défense nationale et à la lutte contre le terrorisme. Un exemple est la création en décembre 2000 par directive présidentielle de l'*Office for the National Counterintelligence Executive* (ONCIX). Cet office a pour mission d'établir un dialogue entre l'administration et le secteur privé pour définir les informations, technologies et industries "critiques" dont la perte pourrait diminuer la puissance des Etats-Unis.

[6] *Intelligence économique et stratégie des entreprises*, La Documentation Française, Paris, 1994.

On notera la volonté timide de la France de combler son retard par la création en 1997, juste à côté de l'Ecole Militaire, de l'Ecole de Guerre Economique (EGE).

5. Conclusion partielle

Quelle que soit la définition adoptée, une des caractéristiques de la puissance réside dans la connaissance de l'information sous toutes ses formes. Aux Etats-Unis, l'accès à l'information a été reconnu comme un besoin interdisciplinaire. Non seulement il existe une volonté d'accéder aux renseignements utiles à tous les secteurs de la nation mais cette recherche trouve également sa place dans un cadre théorique et des processus de collaboration bien défini.

La volonté est présente, les mentalités sont ouvertes, les processus interdépartementaux existent, il faut maintenant se pencher sur les outils concrets d'acquisition et d'exploitation de cette information. C'est ce que nous allons faire dans les parties suivantes en présentant tout d'abord le monde du renseignement américain puis la recherche pratique d'information avec le système ECHELON.

DEUXIEME PARTIE : OUTILS DE GESTION ET D'ACQUISITION DE L'INFORMATION

1. Introduction

Avec 100 000 civils et militaires, un budget annuel de 40 milliards de $, le renseignement américain constitue une entité hors normes au regard des autres nations. Au lendemain du 9/11, la question était sur toutes les lèvres : que faisaient les services de renseignements américains ? Beaucoup se sont demandé pourquoi des attaques si spectaculaires n'avaient pu être prévenues. Les ratés des services de renseignements ont poussé le gouvernement américain à remettre en question leur efficacité et à prôner une nouvelle centralisation de la communauté du renseignement.

Bien que l'idée d'un directeur central des renseignements date du milieu des années 50, une fonction plus ou moins similaire était occupée par le directeur de la CIA. Suite aux investigations menées après le 9/11 par la commission ad hoc[7], cette dernière proposa une mise à jour de la communauté du renseignement ainsi que la création d'un Directeur National du renseignement (DNI). Cette refonte du monde des renseignements a été établie par l'acte sur la réforme du renseignement et la prévention du terrorisme de 2004[8] et concrétisée par la nomination du premier Directeur National du renseignement (annexe A).

---

[7] 9/11 Commission.

[8] *Intelligence Reform and Terrorism Prevention Act of 2004.*

2. Les agences de renseignement gouvernementales

Les descriptions succinctes suivantes doivent permettre d'avoir une idée sur le rôle et l'importance de ces différentes agences (annexe B).

Les principales agences de renseignement :

Office of the Director of National Intelligence (ODNI)

création : *2005* budget : *classifié* personnel : *classifié*

missions : *faire fonction de conseiller principal pour le président des Etats-Unis, le conseil pour la sécurité nationale et le conseil pour la sécurité de la patrie, pour tout ce qui concerne le renseignement en rapport avec la sécurité nationale. Faire fonction de coordinateur de la communauté du renseignement, soit l'ensemble des 16 agences de renseignement du pays. Superviser et diriger le programme national du renseignement.*

Department of Homeland Security (DHS)

création : *2003* budget : *inconnu* personnel : *17 000*

missions : *chargé entre autre du contre-espionnage au sein du territoire américain, il est autorisé par la loi votée lors de sa création à suivre les opérations d'achats par cartes de crédit, les données médicales, les déplacements, les abonnements à des magazines et l'utilisation d'Internet ou des messages électroniques. L'ensemble de ces informations est alors rassemblé au sein d'une base de données centrale recensant des informations sur tous les citoyens américains, gérée dans le cadre d'un programme pour "la maîtrise totale de l'information", concrétisation de la loi dite USA PATRIOT Act.*

Central Intelligence Agency (CIA)

création : *1947* budget : *3 Milliards $* personnel : *17 000*

missions : *la CIA est chargée de fournir et d'analyser des informations sur les gouvernements, les entreprises et les individus de tous les pays du monde pour le compte du gouvernement américain. Elle est également chargée des opérations clandestines (renversement de gouvernement, éliminations, sabotages, etc.) mais celles-ci, bien que souvent citées, ne représentent qu'environ 3 % des dépenses de l'agence.*

Federal Bureau of Investigation (FBI)

création : *1908* budget : *4 Milliards $* personnel : *11 400*

missions : *c'est l'agence de police judiciaire fédérale des Etats-Unis. Elle est officiellement en charge de lutter contre plus de 200 délits fédéraux. C'est l'agence fédérale aux Etats-Unis la plus ancienne et ayant le plus large pouvoir d'enquête.*

National Security Agency (NSA)

création : *1952* budget : *4 Milliards $* personnel : *20 000*

missions : *cette agence est responsable de la collecte et de l'analyse de toutes formes de communications, aussi bien militaires et gouvernementales que commerciales ou même personnelles, par radiodiffusion, par Internet ou par tout autre mode de transmission. L'agence a aussi pour mission d'assurer la sécurité des communications (et donc des ordinateurs) du gouvernement américain.*

Les agences de renseignement du département de la défense :

Defense Intelligence Agency (DIA)

création : *1961* budget : *classifié* personnel : *7 500*

missions : *c'est une des principales sources de renseignements militaires du département américain de la défense. Elle est secondée par les services de renseignements des différentes armées.*

Air Force

Army

Navy

US Marines Corps

National Reconnaissance Office (NRO)

National Geospatial-Intelligence Agency (NGA)

Les agences de renseignement des autres départements :

Drug Enforcement Agency (DEA)

Coast Guard Investigative Service (CGIS)

Bureau of Intelligence and Research

Energy Intelligence

Tresory Intelligence

3. La National Security Agency (NSA)

L'Agence de Sécurité National est devenue célèbre pour le grand public durant les années 90. Elle apparaît dans un certain nombre de films[9] en remplacement de la CIA devenue trop connue pour attirer le public. La NSA a reçu un grand nombre de surnoms, en particulier dus à sa très grande

[9] *Ennemi d'Etat*, 1998 et *Code Mercury*, 1998.

discrétion et à ses caractéristiques, par exemple, *SIGINT City, Crypto City, The Puzzle Palace, No Such Agency, Never Say Anything.*

Plus sérieusement, la NSA est l'acteur incontournable de tout renseignement d'origine électromagnétique (SIGINT). La notion de *Signal Intelligence* est définie comme la branche du travail de renseignement couvrant ce qui relève tant de la *Communication Intelligence* (COMINT) et de l'*Electronic Intelligence* (ELINT) que de la *Telemetry Intelligence* (TELINT). Dans un monde où l'information est essentiellement véhiculée par des moyens de ce genre, on comprend aisément la place prépondérante donnée à la NSA dans l'ensemble des agences de renseignement.

3.1. Historique

La NSA est l'héritière des divers services américains d'écoute électronique et de décryptage ayant existé jusqu'à la fin de la Seconde Guerre mondiale. La NSA est le successeur de la *Armed Forces Security Agency* (AFSA). Elle voit le jour le 4 novembre 1952 grâce à une directive du président Harry TRUMAN (annexe C). Contrairement à la CIA, la NSA est restée très discrète et son existence ne fut reconnue qu'en 1957. Les missions initiales de la NSA se basent sur une directive[10] datant de 1947 et ont été complétées par des directives du département de la défense (DoD) datant de 1971 et de 1991. Le concept général de la NSA peut être résumé de la manière suivante :

- la NSA est un service distinct au sein du ministère de la défense, qui est placé sous la direction du ministère de la défense;
- la NSA assure, d'une part la mission SIGINT des Etats-Unis et met, d'autre part, à la disposition de tous les ministères et services des systèmes de communications sûrs (COMPUSEC);
- la surveillance électronique sert à rassembler des communications extérieures à l'intention des militaires et responsables politiques;
- la NSA ne peut transmettre des informations qu'à des destinataires autorisé par le gouvernement; elle ne peut en transmettre directement aux entreprises américaines.

3.2. Organisation et moyens

La NSA est rattachée organiquement au département de la défense comme une des 17 agences de défense (annexe D). Son siège principal se trouve à Ft Meade à environ 16 kilomètres au nord-est de Washington, DC, sur une base militaire entièrement dédiée à la NSA aux accès dédiés et extrêmement protégés.

Aujourd'hui, la NSA emploie quelque 20 000 employés au siège de Ft Meade et se trouve être le plus grand employeur de mathématiciens au monde.

[10] *National Security Council Intelligence Directive No. 6.*

Son budget annuel reste difficile à évaluer. L'estimation la plus courante donne un montant de 4 Milliards de $. Il est à noter que ce budget stagne pour la première fois et que la NSA semble connaître quelques problèmes de trésorerie qui pourrait freiner son développement.
La NSA gère également un parc de 31 supercalculateurs ainsi que 52 systèmes informatiques reliés entre eux provoquant même une pénurie d'alimentation électrique.

3.3. Domaines d'activité

Les activités principales de la NSA couvrent les domaines suivants :

- sécurité informatique;
- cryptographie;
- analyse des langues étrangères;
- mise au point de supercalculateurs;
- et surtout, elle assure la collection, l'exploitation, le stockage et la distribution des écoutes issues de l'exploration électronique. Une anecdote veut qu'en douze heures, la NSA aspire et traite une somme d'information équivalente à la bibliothèque du Congrès américain.

3.4. Principaux partenaires

le National Reconnaissance Office (NRO)

Le NRO est responsable de l'image et du visible. Ce service, créé en 1960 et officiellement reconnu en 1992, est chargé de la mise au point et de la gestion des satellites de surveillance.
Il emploie près de 3 000 personnes et son budget est classifié.
Il est responsable de la mise en service de stations partout dans le monde qui collectent et distribuent des renseignements provenant des satellites de reconnaissance.

La Defense Intelligence Agency (DIA)

La DIA est un organe de renseignement exclusivement militaire. Créé en 1961, il est le principal outil de création et de gestion du renseignement militaire.
Il emploie environ 8 000 personnes à travers le monde et son budget est également classifié.

Il faut ajouter à cette liste d'autres services comme le *Secret Service*, notamment chargé de la protection de la Maison-Blanche, de celle du Président et des personnalités politiques importantes ainsi que des ambassades américaines à l'étranger.

La NSA effectue également des audits pour des entreprises privées. L'exemple le plus marquant est le test de sécurité effectué par les spécialistes de la NSA sur les différents systèmes d'exploitation de Microsoft, y compris le dernier né VISTA.

3. Conclusion partielle

Un problème caractéristique et limitatif de l'ensemble des services de renseignements de tous les pays reste le cloisonnement. Le monde du renseignement américain en est vraisemblablement l'exemple le plus frappant. La commission 9/11 l'a bien montré, les différentes agences fonctionnaient selon l'esprit de la guerre froide, chacune dans son domaine, sans échange performant d'information entre les spécialistes, malgré le réseau interne *Intelink*. Le fait d'instituer un coordinateur central n'a pas permis de faire sauter toutes les barrières, notamment techniques. Comme le montre un bon article d'un journaliste du New York Times[11], les solutions pourraient venir du monde civil. *Galileo Awards*, une compétition interne visant à trouver des solutions à ces problèmes de partage de l'information et de compétence, a mis en avant deux pistes de solutions bien connues : l'encyclopédie Wikipedia et les blogs. *Intelwiki* doit permettre à chaque membre de la communauté du renseignement d'ouvrir, de compléter ou de corriger un sujet selon ses connaissances sans passer par une voie hiérarchique très contraignante, le tout dans des délais très courts. D'une manière semblable, les blogs permettent de collecter rapidement sur un sujet un nombre important d'avis, de commentaires ou de liens. Les problèmes sont donc reconnus, les solutions innovantes existent, seuls quelques anciens responsables au sein des agences, produits de la guerre froide, limitent encore l'adaptation du monde du renseignement aux réalités actuelles

Outre le nombre d'agences, c'est le caractère global qui fait la particularité du système de renseignement américain. La mondialisation des conflits, du commerce, des relations politiques nécessitent également une mondialisation des sources de renseignements. Alors que tous les pays disposent d'un service de renseignement extérieur, seuls les Etats-Unis arrivent à couvrir l'ensemble de la planète.

En ce qui concerne la NSA, la nomination comme directeur de la DNI du vice-amiral Mc Connell, ancien directeur de la NSA montre l'importance de cette agence généraliste dans le monde du renseignement américain. En effet, si la plupart des agences de renseignement sont spécialisées dans un domaine (militaire, intérieur, extérieur, espace, etc.), la NSA couvre un large spectre et devrait permettre de s'adapter rapidement aux nouvelles technologies, surtout à Internet.

Après avoir vu les organismes chargés de l'exploitation de l'information, il nous reste à découvrir le principal système d'acquisition de l'information brute, le système appelé communément ECHELON.

[11] THOMPSON Clive, *Open-Source Spying*,, New York Times, 3 décembre 2006.

TROISIEME PARTIE : LE SYSTEME D'INTERCEPTION ECHELON

1. Introduction

Mis à part les professionnels du renseignement, le nom ECHELON commence à être connu par une partie du grand public. Ces connaissances restent malgré tout lacunaires et largement suscitées par des fictions à succès ou quelques reportages télévisuels.

Il nous faut ici définir l'histoire, la nature et les capacités de ce système d'interception, remarquer ce qui fait son particularisme et apprécier son importance dans l'affirmation de la puissance de l'Etat américain.

2. Le système d'interception ECHELON

2.1. Mise au jour du système ECHELON

"They've got it taped". C'est le 12 août 1988 qu'un journaliste anglais, Ducan Campbell rédige le véritable premier article[12] sur ECHELON. Il y décrit les grandes lignes du projet P415 et cite notamment le témoignage d'une ancienne employée de Lookheed, Margaret Newsham. En 1996, un nouveau zélandais, Nicky Hager décrivait dans un livre[13] les détails le fonctionnement du système. Jusqu'à la publication du livre d'Hager, seuls les spécialistes du renseignement connaissaient l'existence du système Echelon. Les citoyens européens et leurs représentants à Bruxelles ignoraient tout des activités réelles de la NSA. Personne n'osait croire que les Etats-Unis utilisaient leurs satellites espions et leurs dispositifs d'écoute pour épier les pays alliés.

Après sa parution, le livre de Nicky Hager déclenchait un tollé au Parlement européen. Sur l'initiative d'un député britannique, le Parlement publie tout d'abord le rapport *Evaluation des techniques de contrôle politique* en septembre 98 puis la commission des Libertés Publiques et des Affaires Intérieures demande à la STOA (Scientific and Technological Option Assessment) d'établir une étude à ce sujet. C'est finalement après avoir constitué une commission temporaire sur le système d'interception ECHELON que le Parlement européen publie un volumineux *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (Système d'interception ECHELON)*[14].

2.2. Signaux électromagnétiques

---

[12] *Somebody is listnening*, News Statesman, 12 août 1988.
[13] HAGER Nicky, *Secret Power*, Craig Potton Publishing, 1996.
[14] op. cit. p. 2.

Avant de présenter plus en détail ce système d'interception ECHELON, il convient de préciser et d'expliciter quelques termes techniques afin de faciliter la compréhension du sujet.

SIGINT : on entend par *Signal Intelligence* l'interception et l'exploitation des signaux électromagnétiques, quelle qu'en soit la nature. Ce terme englobe toutes les formes d'interception de tous les signaux électromagnétiques.

COMINT : On entend par *Communication Intelligence* l'acquisition de renseignements par l'interception et l'exploitation des signaux électromagnétiques pouvant être traduits en langage humain. Les exemples les plus courants sont le morse, les ondes radio et les communications téléphoniques en général. Ce genre d'interception permet de reconstituer les messages émis.

ELINT : On entend par *Electronic Intelligence* l'acquisition de renseignements par l'interception et l'exploitation des radiations électromagnétiques émises par des appareils durant leur fonctionnement. Typiquement les radiations émises par des radars, mais aussi par des radios ou des véhicules. Ce genre d'interception permet de localiser l'emplacement des appareils et des troupes qui les desservent.

IMINT : On entend par *Imagery Intelligence* l'acquisition de renseignements par la prise et l'exploitation d'image. Ces images peuvent être produites par des caméras standard, des caméras thermiques ou autres systèmes radars d'imagerie.

Le renseignement basé sur l'interception de sources électromagnétiques est pratiqué par l'ensemble des nations quelque peu développées. C'est une activité très large qui peut fournir des renseignements sur les activités militaires, diplomatiques, économiques ou scientifiques. Globalement, environ 15 – 20 milliards € sont dépensés annuellement dans ce domaine. La majeure partie de ces fonds sont investis par les membres de l'UKUSA.

2.3. Historique et partenaires

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). 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, d'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. 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.

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 Etats-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. 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: 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 (annexe E).

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 Etats-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'oeuvre 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 Etats-Unis, par exemple, c'est le *Naval Security Group* (NAVSECGRU) ou l'*Air Intelligence Agency* (AIA) ou encore le *United States Army Intelligence and Security Command* (INSCOM) qui assure avec la NSA le fonctionnement des stations. Dans les stations britanniques, il s'agit de la *Royal Air Force* (RAF) 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 ECHELON 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 aussi du fait du rôle de la NSA qui centralise l'ensemble des données collectées et les redistribue, donc les filtre.

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 Etats-Unis des relations "moins inégales" qu'avec les autres membres du pacte.

2.4. Cycle du renseignement

ECHELON est un instrument de collecte d'information. Son activité s'inscrit dans un cycle dont il constitue une étape. Ce cycle du renseignement (Annexe F) est le même pour la plus grande partie des pays utilisant un tel système, il comprend une phase de planification des besoins, une phase de collection des informations, une phase d'exploitation des données recueillies puis une phase de diffusion des produits sous forme de rapports. Il est à noter qu'une station d'écoute comme celle de Menwith Hill en Grande-Bretagne est composée de 3 bureaux principaux : opération et planification, collection de l'information, exploitation et production.

Phase de planification et conduite :

Il s'agit tout d'abord de déterminer les besoins des clients. Dans le cas de l'UKUSA, ces clients sont les gouvernements (via leurs services de renseignement) membre de l'alliance, pour les Etats-Unis, les principaux départements comme la défense, les affaires étrangères, la sécurité, le commerce ou l'intérieur. Ces besoins sont ensuite transformés en missions concrètes, priorisées et transmises au bon endroit pour exécution.

Phase de collecte de l'information :

Il s'agit ici vraisemblablement de la phase actuellement la plus délicate du cycle de renseignement. En effet, le flux d'information électronique généré aujourd'hui dans monde est énorme. Sauf si le besoin peut être très clairement déterminé (source, moyen de transport de l'information, destinataire, nature de l'information), il s'agit de collecter le maximum d'information brut provenant de tous les médias existants, de faire un premier tri et de stocker ces informations. Cela nécessite des moyens technologiques gigantesques, travaillant en temps réels et interconnectés. La plupart de temps, ces tâches sont entièrement automatisées

et ne nécessitent pas d'intervention humaine. Certaines stations d'écoute du système ECHELON fonctionnent sans aucun personnel.

Phase d'exploitation de l'information :
Il s'agit dans tout d'abord de convertir l'information brute sélectionnée en un produit propre à l'analyse. C'est durant cette première phase que les besoins en outils de sélection (mots-clés, contexte, provenance), de décryptage ou de traduction sont fondamentaux. L'information est alors classifiée en fonction de sa nature et de sa provenance.
L'étape suivante consiste à transformer l'information brute en renseignement proprement dit. C'est ce travail qui va déterminer la qualité d'un renseignement.

Phase de diffusion du renseignement :
Il s'agit finalement de diffuser sous forme de rapport les renseignements aux demandeurs. Ces rapports ne peuvent aller qu'à des organes gouvernementaux dûment accrédités. Au sein de l'alliance UKUSA, seuls les Etats-Unis ont accès à l'ensemble des données, les autres pays pouvant émettre des besoins en renseignements. En ce qui concerne les renseignements d'ordre économique, ces derniers doivent transiter par une institution gouvernementale avant d'être communiqués à une entreprise. Cela ne pose pas de problèmes aux Etats-Unis. Dès 1993, un *Office of Executive Support* a été créé pour résoudre ce genre de situation. C'est d'ailleurs la même année que le président Clinton officialisé le support en renseignement aux organisations commerciales en créant le *National Economic Council*, institution similaire à la NSA.

2.5. Installations et moyens du système

Afin de procéder à la collecte des informations brutes, ce système global doit posséder un certain nombre d'installation d'écoute ou de perception, principalement des antennes et des satellites couvrant l'ensemble du spectre des communications électromagnétiques mondiales. Afin d'effectuer un premier tri, des ordinateurs puissants doivent se situer à l'emplacement des stations d'écoute.

Antennes

La récolte systématique de communications transitant par satellite commença pour la NSA en 1971. Deux stations terrestres furent construites dans ce but : la 1ère à Morenstow, Cornwal en Grande-Bretagne avec 2 paraboles de 30 m 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 2ème station fut construite à Yakima, près de Washington, pour intercepter les communications transitant par le satellite Intelsat de l'océan Pacifique. La

situation resta telle quelle jusqu'à la fin des années 70. C'est alors qu'un 3ème site toujours aux Etats-unis fut installé à Sugar Grove, en West Virginia. La responsabilité du site fut confiée à *l'US Naval Security Group*. Par la suite, le réseau d'écoute ECHELON se développa de pair avec le besoin croissant en télécommunications entre 1985 et 1995. Des stations furent implantées au Canada, en Australie ainsi qu'en nouvelle Zélande. Bien entendu, celles qui existaient déjà furent agrandies et modernisées (annexe G).

Il existe sur la surface du globe une multitude d'antennes diverses, comment reconnaît-on une station d'interception ?

Critères 1 : accès de l'installation

Les installations de la poste, de la radiotélévision ou des instituts de recherche disposant de grandes antennes sont accessibles aux visiteurs, les stations d'interception ne le sont pas. La plupart du temps, elles sont gérées officiellement par des militaires qui assurent également une partie au moins de l'interception.

Critères 2 : types d'antennes

Dans les installations de critère 1, il existe différents types d'antennes, pouvant se distinguer en fonction de leur structure caractéristique. Leur forme donne des indications quant au but poursuivi par l'installation d'interception. Ainsi, des rangées d'antennes verticales formant un cercle de grand diamètre sont utilisées pour déterminer l'orientation des signaux hertziens. Des antennes directionnelles, comparables à des antennes de télévision classiques gigantesques, servent pour intercepter des signaux hertziens non dirigés. Pour la réception des signaux satellitaires, on utilise en revanche exclusivement des antennes paraboliques. Lorsque ces antennes sont à découvert, il est possible de calculer le satellite dont les émissions sont interceptées. Souvent cependant, des radômes masquent l'orientation de l'antenne (annexe H).

Critère 3 :·dimensions de l'antenne

Dans une installation conforme au critère 1, les antennes de réception des satellites peuvent êtres utilisés dans les buts suivants :

- réception des satellites de communication militaires;
- réception des satellites-espions IMINT;
- réception des satellites SIGINT;
- réception servant à l'interception des satellites de communications civils.

Il n'est pas possible de déduire la mission que remplissent les antennes à partir de leur aspect extérieur. Toutefois, leur diamètre fournit certaines indications à cet égard. Pour l'interception des communications civiles, des antennes de 15 à 20 m de diamètre sont nécessaires. Pour les communications militaires, la réception des signaux SIGINT et IMINT, des antennes de dimension beaucoup plus réduite suffisent. Ainsi, si une station d'écoute dispose d'antennes

d'un diamètre d'environ 20 m, il est certain que l'interception des communications civiles y est pratiquée.

Aujourd'hui, il est estimé, que le réseau ECHELON utilise 120 antennes, pays du pacte UKUSA compris, à des fins d'écoutes et de renseignements. Si l'on essaye de répartir les antennes en catégories (sachant que plusieurs antennes peuvent être installées par station d'écoute):
40 sont pointées vers des satellites commerciaux.
30 sont destinées à diriger les satellites d'écoutes (type Mercury, Keyhole...).
50 sont pointées vers l'ex URSS, mais depuis, un certain nombre ont dû être réorientée vers d'autres objectifs tels que les satellites commerciaux.

Satellites

Des satellites peuvent également êtres utilisés pour acquérir des sources électromagnétiques. Laissons de côté les satellites d'imagerie de type Keyhole, leurs données n'étant pas directement traitées dans le cadre du système ECHELON si ce n'est pour transmission de donnée.
Les satellites de type Mercury sont eux utilisés pour l'écoute des communications. Ils sont placés juste à côté d'un satellite relayant des communications transcontinentales de type INTELSAT, Par la taille de leurs paraboles (de 80 à 100 m), les signaux initialement reçus par le satellite civil le seront également par celui militaire. Ce dernier retransmettra à la station d'écoute concernée par la région afin d'analyser les données. Les derniers satellites de ce genre (Trumpet) coûterait la bagatelle d'un milliard $ (annexe I).
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 de relais terrestre (en revanche INTELSAT utilise le principe des relais terrestre).

Ordinateurs

Comme nous l'avons vu, la NSA dispose d'un parc de supercalculateur impressionnant. On dit que l'agence est le plus grand consommateur de matériel informatique au monde. Elle travaille par ailleurs en étroite collaboration avec quelques grands fabricants américains tels que Motorola, Intel, IBM et le fabricant de superordinateur CRAY/SGI. Ces superordinateurs

sont capables de traiter 1,3 trillion d'opérations à la seconde[15]. Cela pose d'ailleurs un problème assez délicat à Ft Meade : la consommation en électricité[16] est gigantesque et l'approvisionnement ne devrait plus suffire dans les prochaines 2 années sans que ce problème n'ai été reconnu.

Autre dispositif capital : les capacités de stockage sont elles aussi démesurées. Une tour permet de gérer 6 000 cassettes de stockage de donnée avec une capacité de 50 gigabytes chacune. Cela donne 300 terabytes ou l'équivalent de 3 000 fois le tour de la terre avec des feuilles A4.

Afin de relier toutes les stations d'ECHELON entre elles, une sorte d'Internet très protégé a été mise en place. Ce réseau PLATFORM (aussi appelé INTERLINK) relie également les clients potentiels du système.

2.6. Capacités d'interception du système

Lorsque deux personnes se trouvant à une certaine distance l'une de l'autre souhaitent communiquer entre elles, elles ont besoin d'un support de communication qui peut être :

- l'air (le son)
- la lumière (morse, fibre optique)
- l'électricité (télégraphe, téléphone)
- une onde électromagnétique (radio sous toutes ses formes)

Si la NSA, supporté par ECHELON veut effectuer un *Monitoring* de la planète, voyons quelles sont ses capacités à écouter nos conversations.

Communications via satellite

Si un satellite est utilisé comme relais pour les conversations (INTELSAT), il va recevoir les ondes et les retransmettre sur une partie de la surface de la terre. En pointant une antenne parabolique dans la direction du satellite, il est possible de capter l'ensemble des communications (annexe J). Les différentes zones attribuées aux membres de l'UKUSA permettent une couverture pratiquement complète de la terre (annexe E).

Communications via relais terrestres

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 rendu 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 (annexe J). Vu le succès de ces

[15] 1,3 teraflops.
[16] Baltimoresun, édition du 26 janvier 2007.

interceptions, les Américains développèrent de nouveaux satellites capables de cibler sur demande nos téléphones, données informatiques, pagers.

Communications par câble

Le câble sert à acheminer toutes sortes de communications (voix, téléfax, courrier électronique, données). Les communications tributaires du câble ne peuvent être interceptées que dans le cas où un accès au câble est possible (annexe K). C'est là que les certains accords passés avec les principales compagnies de télécommunication deviennent nécessaires.

En ce qui concerne les câbles sous-marins, y compris les câbles en fibre optique, une solution consiste à attendre qu'ils sortent de la mer et d'appliquer le principe précédent. L'autre solution, plus coûteuse mais plus discrète consiste à pirater les amplificateurs de signal nécessaires à transporter l'information sur de longues distances. Cela peut être réalisé par des sous-marins ou alors en branchant un câble parallèle depuis un de ces amplificateurs.

Internet

C'est le nouveau défi de ce XXIe siècle pour la NSA. En simplifiant, il existe plusieurs solutions et pistes pour asseoir son emprise sur Internet. La plus facile consiste, comme pour les liaisons câblées, à se brancher sur les différents *Router* qui servent de carrefours à l'ensemble du trafic mondial (annexe L). Le leader dans ce domaine étant la firme CISCO, partenaire privilégié de la NSA, cela ne devrait pas trop poser de problèmes. La deuxième solution, qui commence à être mieux connue par le grand public (principe des spams) met en œuvre des programmes *renifleurs* qui sont chargés d'explorer la toile à la recherche d'information correspondant aux besoins, l'objectif avoué étant d'aller tous les recoins d'Internet en moins d'une demi-heure (annexe M pour plus de détails).

Les dictionnaires

Avec la masse de données circulant quotidiennement dans le monde, il s'agit naturellement de pouvoir exploiter ces informations. Les ordinateurs chargés d'effectuer ces tâches ont été appelés *Dictionnaires*. Ces ordinateurs contiennent les listes de cibles et d'informations liées aux objectifs, ce qui permet de sélectionner automatiquement les messages dignes d'intérêt.

Des ordinateurs *Dictionnaires* 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.

Les ordinateurs assignés à ces tâches obéissent à plusieurs milliers d'exigences différentes qu'on appelle *Nombres* (codes à quatre chiffres).

Le triage et la sélection effectués par ces ordinateurs peuvent êtres comparés à l'usage des moteurs de recherche, qui sélectionnent les pages Web par mots ou expressions clés, et établissent des liens. La fonction d'expédition des *Dictionnaires* peut être comparée au courrier électronique. Quand cela sera 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, téléfax et e-mail) 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 *Dictionnaires* 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 Etats-Unis et leurs alliés. Une fois les nouveaux mots insérés dans le système, quelques minutes suffisent pour que les *Dictionnaires* fassent apparaître les messages qui les contiennent.

2.7. Les affaires connues d'espionnage

Le monde du renseignement est domaine fermé. Les exemples que l'on peut trouver sur les activités du système d'interception ECHELON ont rarement été confirmés par les acteurs eux-mêmes. Il existe une multitude de petits exemples de l'influence du système sur la prise de décision en général. Les faits suivants sont les plus marquants et ceux que l'on retrouve le plus souvent.

Espionnage contre des personnes

1945-1973 Opération SHAMROCK

A partir de 1945, la NSA a obtenu systématiquement des bureaux des principales entreprises américaines de télégraphie (RCA Global, ITT World Communications, Western Union) l'accès aux messages câblés. C'est le début de l'opération SHAMROCK qui dura près de 30 ans. De 1966 à 1973, la circulation totale de télégrammes aux Etats-Unis était d'environ 72 millions de messages par an. Selon la commission *Church* du Sénat américain, les analystes de la NSA en sélectionnaient environ 1,8 million, soit un sur quarante, pour les exploiter avec l'aide des autres agences américaines.

1967-1975 Opération MINARET

A partir de 1967, l'opération MINARET débute. Les pacifistes (contre la guerre du Viêt-nam), les militants pour l'égalité des droits civiques (Martin Luther King, Malcolm X, Jane Fonda…) sont mis systématiquement sur écoute. Pour légitimer leurs actions, les différentes agences américaines ont volontairement porté des accusations à leur encontre. Ainsi 450 américains et 3 000 étrangers étaient considérés comme des trafiquants de drogue internationaux, 1 000 Américains et 1 700 étrangers étaient classés comme agitateurs publics ou terroristes, 30 organisations américaines et 700 étrangers étaient désignés comme extrémistes.

Le 8 août 1975, le lieutenant-général Lew Allen directeur de la NSA, reconnaît devant la commission Pike de la chambre des Représentants que : *"La NSA intercepte systématiquement les communications internationales, les appels téléphoniques comme les messages câblés"*. Il reconnaissait également que des messages adressés à des citoyens américains ou émanant d'eux ont été interceptés dans le processus destiné à rassembler des renseignements concernant l'étranger, ce qui est contraire à la constitution américaine.

En août 1977, Abdeen M. Jabara, avocat de Detroit, intenta un procès au FBI. Il devint le premier et le seul Américain à provoquer la révélation de l'étendue de la surveillance exercée sur lui par la NSA. Entre 1967 et 1973, la NSA avait procuré au FBI le contenu de six appels téléphoniques et télégrammes passés à l'étranger par cet homme. Celui-ci appris également que la NSA avait transmis des renseignements le concernant à treize agences fédérales américaines et à trois gouvernements étrangers. Il obtint temporairement qu'il soit interdit à la NSA d'écouter ses communications, et la destruction du matériel et des dossiers le concernant. Quelques années plus tard le dossier fut classé sans suite.

Espionnage économique

1994 Airbus-McDonnell Douglas

Dans le cadre d'un contrat d'achat d'avions de 6 milliards de $ entre Airbus et la compagnie aérienne d'Arabie Saoudite, la NSA a intercepté les téléfax 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 mise au jour une manoeuvre de corruption d'Airbus (pots-de-vin à des membres de la commission chargés 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 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 pénétrations du marché américain sont à jamais anéanties. Le préjudice s'élève à plusieurs millions de DM.

1994 Thomson CSF-Raython

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 de $.

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 auprès de Brasilia pour retourner la situation.

1994 Accord général sur les tarifs douaniers et le commerce (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.

1992-1998 General Motors

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).

Espionnage diplomatique

1975 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 la 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.

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.

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'Etat commanditaire, la Libye, a été immédiatement identifié par les Etats-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 Koweit

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'Etat ne réussira probablement pas.

2.8. Limitations techniques du système

Avec ces formidables moyens techniques, humains et financiers, les services de renseignements américains ne peuvent pourtant pas tout voir et tout intercepter. La surabondance de l'information collectée empêche un tri sans failles. Les informations d'importance capitale manquées par la gigantesque machinerie sont nombreuses, à un point

tel que les hommes du renseignement US leur ont donné une appellation spécifique : *Intelligence failures.*

Capacité de traitement de l'information

La NSA capterait un million de conversations satellites par demi-heure. Sur ce million de communications, 6 500 seraient retenues par sondage, 1 000 correspondraient aux critères prédéfinis, 10 seraient choisies par les analystes, un seul rapport étant produit sur cette base. La proportion est ici de 1 sur 1 million, soit 0,0001 pour cent[17].

L'aspect humain est aussi limitatif. A Ft Meade, les interprétateurs de photographies satellitaires sont complètement débordés. Bien que superpuissants, les ordinateurs de la NSA sont incapables de rivaliser avec l'homme et son intuition. Et les moyens humains de production du renseignement sont totalement saturés. Pour résumer la situation, les employés de la NSA cherchent chaque jour des aiguilles dans des meules de foin. A n'en pas douter, cela doit être éprouvant psychologiquement.

Capacité de traduction de l'information

La traduction automatique et fiable de l'information est un rêve poursuivi par les agences de renseignement depuis longtemps. La problématique est multiple. Il s'agit tout d'abord de traduire dans des centaines de langues et dialectes si nécessaire les dictionnaires de mots-clé. Les messages doivent ensuite êtres numérisés. Ici interviennent les problèmes de reconnaissance de caractère ou de reconnaissance vocale. A ce moment, des programmes de traduction peuvent intervenir. Ces derniers doivent cependant également posséder des dictionnaires techniques propres à la catégorie d'information à traduire (scientifique, économique, religieuse, culturelle, historique, etc).

Pour le moment, dans le domaine de la traduction, les programmes automatisés ne peuvent pas encore remplacer d'une manière fiable la traduction humaine.

Capacité de décryptage de l'information

Il existe actuellement des développements technologiques qui rendent les écoutes électroniques de plus en plus difficiles. La NSA est à ce titre très alarmée par le développement de programmes de cryptage efficaces qui permettent de coder les communications électroniques. Les algorithmes puissants disponibles sur le marché public sont devenus pour certains quasiment impénétrables, mais ils créent en tout cas de tels délais et un tel surcoût pour l'exploitation des écoutes qu'ils rendent toute interception inefficace. La NSA conserve une quantité énorme de messages non décryptés, dans l'attente d'avoir plus

[17] *Système d'interception des communications par satellite de Département fédéral de la défense, de la protection de la population et des sports (projet "ONYX"),* Rapport de la Délégation des Commissions de gestion des Chambres fédérales du 10 novembre 2003, p.1396.

tard connaissance d'une clé, ou de disposer du temps pour casser le code. Quand cela se produira, ces documents auront perdu leurs valeurs dans notre société mondialisée ou le maître mot est la vitesse.

2.9. Dérives

Le droit au respect de la vie privée s'inscrit dans les droits de la personnalité. Un article de la Convention Européenne des Droits de l'Homme[18] (CEDH) garantit le respect de ces droits : "Toute personne a droit au respect de sa vie privée et familiale de son domicile et de sa correspondance". Cette convention s'inscrit dans un ensemble d'actes juridiques internationaux et nationaux reconnaissant ce principe protecteur.

Les conventions concernant les droits de l'homme permettent une protection efficace contre les interceptions illégales de communication. Cette protection est moins évidente contre les interceptions légales et surtout si elles sont étrangères, c'est-à-dire que l'interceptant est un pays autre que celui de l'émettant. C'est la base même du principe de fonctionnement de l'alliance UKUSA où chaque pays espionne pour le compte de l'autre.

2.10. Développement possible

La NSA avec le système ECHELON devra faire face dans le futur à de nouveaux défis. D'un côté, la prolifération de nouveaux systèmes va limiter la collecte d'information. D'un autre côté, les budgets alloués aux services de renseignement n'arrive plus à suivre la demande.

Une des options principales est de limiter les investissements dans les écoutes COMINT et de se focaliser sur Internet, notamment en multipliant les efforts pour accéder directement aux données de nos ordinateurs.

Comme la guerre menée contre les systèmes de cryptage (programmes libres d'accès) semble perdue, l'intention est de s'approprier l'information sur les disques durs, avant qu'elle ne soit cryptée et envoyée. Cela va nécessiter une collaboration accrue avec les producteurs de système d'exploitation ainsi que la main mise sur le fonctionnement des réseaux en général.

Le ciblage, donc la détermination des objectifs à atteindre devra également gagner en priorité. A partir du moment où les sources possibles de renseignement sont identifiées, la collecte d'information devient beaucoup plus simple. Cela nécessite une plus grande collaboration

[18] Article 8, paragraphe 1.

interdépartementale, c'est peut-être pour cela que le directeur actuel du service de renseignement national américain est un ancien directeur de la NSA.

3. Conclusion partielle

L'alliance UKUSA et plus généralement les possibilités d'interception du système ECHELON permettent maintenant depuis une cinquantaine d'année la récolte d'information à un niveau planétaire. Une organisation de cette ampleur avec son expérience est unique.

Il est évident que le système peine à s'adapter au flux toujours plus important d'information circulant dans le monde. Les pistes envisagées pour résoudre ce problème semble cependant aller dans la bonne direction. La maîtrise d'Internet, le contournement des solutions de cryptage, un meilleur ciblage en amont des sources doivent permettre à la NSA de s'adapter à cette nouvelle situation. La restructuration déjà initiée des activités d'interception d'ECHELON porte à croire que les résultats devraient rapidement se faire sentir.

4. Les autres systèmes des autres pays

Il est communément admis qu'une cinquantaine de pays dans le monde disposent de leur propre système d'écoute. Même hors de l'alliance UKUSA, les échanges de données sont monnaies courantes au sein des services de renseignement. Depuis 1993, sans aucune communication au Parlement européen, les responsables de la lutte contre la criminalité de la majeure partie des pays européens et de l'alliance UKUSA se rencontrent discrètement sous les auspices de l'organisation ILETS (Interception Law Enforcement Telecomunication Seminar). Ce sont les membres d'ILETS qui ont rédigé les premières listes de modifications à apporter aux systèmes de communication afin de faciliter les interceptions. Listes qui serviront à la création des textes discutés par les Instances européennes.

Voyons brièvement quels sont les principaux systèmes d'écoute hors alliance UKUSA :

4.1. La France — FRENCHECHELON

Système d'écoute géré par la DGSE (direction générale de la sécurité extérieure).

Stations d'écoute au sol et satellite HELIOS.

4.2. La Suisse — ONYX

Système d'écoute géré par la SRM (service de renseignement militaire).

Stations d'écoute au sol.

4.3. La Belgique — NiceTrack

Système d'écoute géré par la CTIF (système central d'interception technique).

Surveillance d'Internet.

4.4. Les Pays-Bas DUTCHECHELON
Système d'écoute géré par la MIVD (Defense Intelligence and Security Service)
Stations d'écoute au sol.

4.5. La Russie SORM-2
Système d'écoute géré par différents organismes de sécurité.
Stations d'écoute au sol et surveillance d'Internet.

CONCLUSION

Le système d'interception ECHELON est-il devenu un acteur majeur de l'hégémonisme des Etats-Unis ?

La puissance désigne le potentiel d'un groupe d'établir des rapports conformes à ses désirs. La couverture mondiale du système d'interception ECHELON permet aux membres de l'alliance UKUSA d'intervenir partout sur la planète. Quel que soit le domaine d'activité ou l'emplacement géographique, il existe une possibilité pour le gouvernement américain de s'immiscer dans vos affaires et d'en tirer profit.

La puissance est à rechercher dans la maîtrise de nombreux domaines. Le système d'interception ECHELON ne se limite pas à la recherche d'information militaire. Il s'intègre dans des processus interdépartementaux de recherche et d'exploitation de l'information. Il a les capacités de participer à la supériorité économique du pays, à la gestion des crises, à la maîtrise des flux financiers ainsi qu'à la maîtrise des communications et des messages.

La puissance d'un état se caractérise par les moyens dont il dispose pour s'assurer d'une influence durable dans le concert des nations. L'expérience accumulée dans les écoutes depuis un demi-siècle ainsi que la constance d'investissements importants consentis dans ce domaine permettent aux Etats-Unis d'avoir une avance inégalable dans l'interception et l'exploitation de l'information au niveau planétaire.

La source du pouvoir réside dans la connaissance de l'information sous toutes ses formes. La NSA met les moyens pour s'adapter rapidement aux nouvelles technologies. Les écueils dus à l'apparition de la fibre optique ainsi qu'à la démocratisation des méthodes de cryptage sont en passe d'êtres surmontés. L'enjeu majeur que constitue la maîtrise de l'Internet a été rapidement reconnu. Les efforts investis pour contrôler la toile portent déjà leurs fruits.

La compétition économique est devenue le terrain d'affrontement principal dans ce qu'il est convenu d'appeler la recherche de puissance. L'intégration du système d'interception ECHELON dans des

processus d'appui à la suprématie économique de Etats-Unis ne doit plus à démontrée. Le système peut participer d'une manière déterminante à la captation d'information et à la production de renseignements enrichissant le flux informationnel des entreprises à caractère stratégique.

Les moyens colossaux mis en œuvre par la NSA pour rechercher et exploiter l'information en général sont rentables ?

Il est toujours très difficile chiffrer concrètement un rendement lorsque l'on parle de puissance à long terme. Le monde du renseignement américain coûte très cher. Une possibilité pour en apprécier la rentabilité serait de mettre en relation les 40 milliards de $ de budget annuel des agences américaines avec les chiffres du commerce mondial actuel. La valeur des exportations mondiales de marchandises[19] a passé en 2005 la barre des 10 000 milliards de $. Les exportations de services commerciaux ont atteint cette même année les 2 400 milliards de $.

Le ratio entre ces deux données ne doit pas laisser planer d'incertitude. Le commerce mondial représente des sommes colossales. Il ne fait aucun doute que le monde du renseignement américain joue un rôle dans ce domaine et que les investissements consentis sont d'une manière ou d'une autre rentabilisés.

Pour conclure, il faut bien noter que tous les pays industrialisés se sont dotés de systèmes d'écoute semblable au système d'interception ECHELON. La différence majeure réside dans les investissements, la nature globale et l'intégration du système dans des processus interdépartementaux concrets d'exploitation de l'information. Malgré des limites évidentes mais en comparaison avec les possibilités des autres nations, le système ECHELON représente acteur considérable de la puissance américaine.

[19] OMC, *Commerce mondial 2005, perspectives pour 2006*, communiqué de presse du 11 avril 2006.

BIBLIOGRAPHIE

PARUTIONS OFFICIELLES

- Parlement européen, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques,* PE 305.391, 11 juillet 2001.
- Parlement européen, *Development of surveillance technology and risk of abus of economic information,* Document de travail pour le Panel STOA, Luxembourg, octobre 1999.
- *Communications Intelligence Activities,* Memorandum for The Secretary of State, The Secretary of Defense, Oct 24, 1952.
- BEST Richard A. Jr., *The National Security Agency : Issues for Congress*, January 16, 2001.
- Parlement européen, *Une évaluation des techniques de contrôle politique, Résumé analytique élaboré pour servir de document de base pour la séance de session du mois de septembre 1998.*
- *Information Operations : Wisdom Warfare For 2025,* A Research Paper Presented to Air Force 2025, April 96.
- *The National Counterintelligence Strategy of the United States,* Office of the National Counterintelligence Executive, March 2005.
- Parlement suisse, *Système d'interception des communications par satellite de Département fédéral de la défense, de la protection de la population et des sports (projet "ONYX"),* Rapport de la Délégation des Commissions de gestion des Chambres fédérales du 10 novembre 2003.

OUVRAGES ET ETUDES

- HAGER Nicky, *Secret Power,* Craig Potto Publishing, 1996.
- DOREL Gérard, Atlas de l'empire américain, Editions Autrement, 2006.

ARTICLES

- GORMAN Siobhan, *NSA electricity crisis gets Senate scrunity,* Baltimore Sun, January 26, 2007.
- LEPREVOST Franck et WARUSFEL Bertrand, *Echelon : origines et perspectives d'un débat transnational.*
- CAMPBELL Duncan, *Somebody's listening*, New Statesman, August 12, 1988.
- LAMBERTY Denis, *Faut-il avoir peur d'Echelon ?,* La tribune no 35, CID.
- CISSE Amadou, *Peut-on parler d'une faillite du renseignement américain avec les événements du 11 septembre 2001 ?,* Ecole des Hautes Etudes Internationales, 3ème Cycle – 2003-2004.
- Commissariat Général du Plan, *Intelligence économique et stratégie des entreprises*.
- ESCHBACH Bernard, *Die Sicherheitspolitischen Herausforderungen der Postmoderne (Globalisierung, Entstaatlichung und Neue Kriege),* ZAL-IIa, 2006.
- MANACH Jean-Marc, Echelon/Frenchelon : mythes et réalités, Conférence à l'IEO de Rennes, avril 2005.
- BELL Aaron, Machine Translation : not now, but someday, June 03, 2004.
- HERBERT Jean-Paul, *L'évolution des relations stratégiques transatlantiques vers une nouvelle course aux armements,* EHESS.

SITES INTERNET OFFICIELS

- **http://www.nsa.gov**
  Site de la National Security Agency.
- **http://www.nro.gov**
  Site du National Reconnaissance Office.
- **http://www.fas.org/spp/military/docops/usaf/2025/index.html**
  Etude de l'US Air Force visant à examiner les concepts, capacités et technologies possibles afin d'acquérir la dominance de l'information.

- **http://dni.gov/index.htm**
  Homepage de l'office du directeur national des renseignements.
- **http://www.armees.com**
  Etats-Unis : Nomination approuvées par des commissions du Sénat.
- **http://www.archives.gov**
  Archives nationales américaines.
- **http://www.fas.org**
  Federation of American Scientists.
- **http://www.usinfo.state.gov**
  Information : Les Etats-Unis sont à la pointe du progrès.
- **http://www.ege.fr**
  Ecole de Guerre Economique.

SOURCES OUVERTES

- **http://fr.wikipedia.org**
  Encyclopédie libre version française.
- **http://en.wikipedia.org**
  Encyclopédie libre version anglaise.
- **http://www.infoguerre.com**
  Un débat stratégique doit définir la finalité d'Echelon.
  Mutation du renseignement dans les affrontements économiques.
  Les origines de la guerre de l'information.
  Les principes de la guerre de l'information.
  Périls et potentialités de la guerre de l'information.
  Les applications économiques de la guerre de l'information.
  La domination par l'information.
  Focus sur le NCIX : le contre-espionnage économique.
  Echelon : l'inquiétude européenne rebondit au Japon.
  Le concept de puissance et l'intelligence économique.
- **http://meridien.canalblog.com**
  Casus Belli.
- **http://www.stratisc.org**
  Institut de stratégie comparée.
- **http://www.ifri.org**
  Institut français des relations internationales.
- **http://www.futura-sciences.com**
  Du satellite espion à Echelon.
- **http://www.confidentiel.net**
  La National Security Agency.
  La NSA espionne le monde.
- **http://www.cryptome.org**
  Echelon's Architect.
  Interview : Echelon was my baby.
- **http://www.techno.science.net**
  Echelon.
- **http://www.strategique.free.fr**
  Entreprises : la guerre de l'information.
- **http://www.clifti.org**
  Echelon et Frenchelon, France-USA : mêmes méthodes.
  ENFOPOL et ILETS, ou comment les USA persuadent les européens de nous espionner.
- **http://www.astrosurf.com**
  Du satellite espion à Echelon.

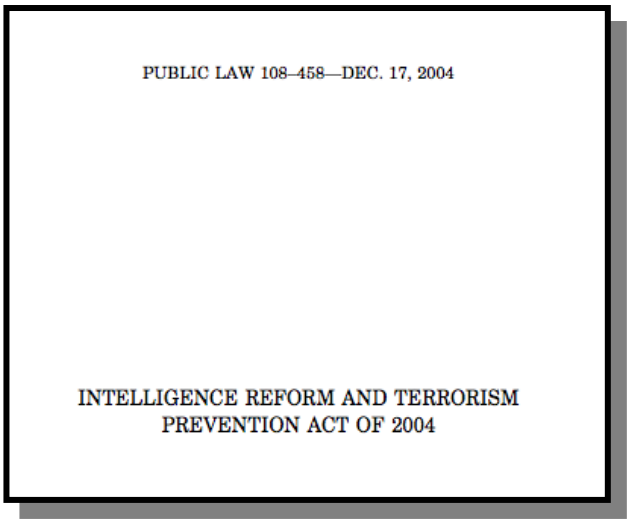
- **http://www.cyber-rights.org**
  Interception Capabilities 2000
- **http://www.silicon.fr**
  USA : Echelon espiionne ses propres citoyens.
- **http://www.reseau.echelon.free.fr**
  Microsoft et la N.S.A.
  Informations sur le réseau Echelon.
- **http://www.perso.orange.fr/nakite**
  La National Security Agency.
- **http://www.echelononline.free.fr**
  Connaître le réseau Echelon.
- **http://www.automatesintelligents.com**
  Body of secrets.
- **http://www.jpney.com**
  Visite exclusive à la NSA : au cœur des écoutes américaines.

GLOSSAIRE

AFSA	Armed Forces Security Agency
AIA	Air Intelligence Agency
CEDH	Convention Européenne des Droits de l'Homme
CGIS	Coast Guard Investigative Service
CIA	Central Intelligence Agency
COMINT	Communication Intelligence
COMPUSEC	Computer Security
CSE	Communication Security Establishment (Ca)
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DSD	Defense Signal Directorate (Aus)
DUTCHECHELON	Système d'écoute des Pays-Bas
ECHELON	Nom communément donné au système d'interception global de l'UKUSA
EGE	Ecole de Guerre Economique
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FRENCHECHELON	Système d'écoute de la France
GCHQ	Government Communication Headquarter (GB)
GCSB	Government Communications Security Bureau (NZ)
GI	Guerre de l'information
HUMINT	Human Intelligence
IAO	Information Awareness Office
ILETS	Interception Law Enforcement Telecomunication Seminar
IMINT	Imagery Intelligence
INSCOM	United States Army Intelligence and Security Command
INTELINK	Intranet entre les agences de sécurité gouvernementales
INTELSAT	Satellites de communication civil couvrants l'ensemble de la planète
INTERLINK	Intranet des agences de renseignement américaines
NAVSECGRU	Naval Security Group
NGA	National Geospatial-Intelligence Agency
Nice Track	Système de surveillance de la Belgique
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ONCIX	Office of the National Counterintelligence Executive
ONYX	Système d'écoute de la Suisse
PLATFORM	Intranet des agences de renseignement américaines
RAF	Royal Air Force
RMA	Revolution in Military Affairs
SIGINT	Signal Intelligence
SORM-2	Système d'écoute de la Russie
STOA	Scientific and Technological Option Assessment
TELINT	Telemetry Intelligence
TIA	Total Information Awareness
UKUSA	Alliance SIGINT entre les USA, Grande-Bretagne, Canada, Australie et Nouvelle-Zélande

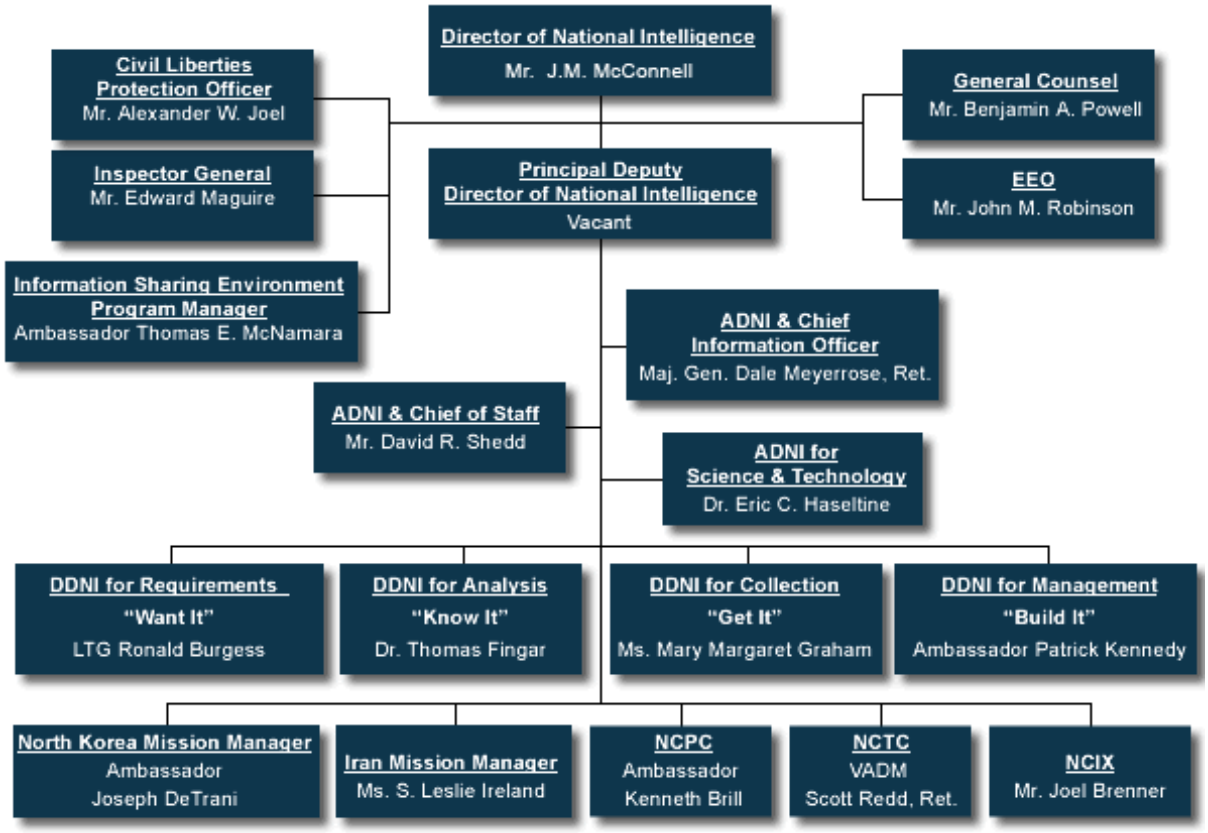
ANNEXES

ANNEXE A : CONSEQUENCES DU RAPPORT DE LA COMMISSION 9/11


PUBLIC LAW 108–458—DEC. 17, 2004

INTELLIGENCE REFORM AND TERRORISM
PREVENTION ACT OF 2004

Acte d'institution de la communauté du renseignement



Organigramme du bureau du Directeur

ANNEXE B : AGENCES DE RENSEIGNEMENT GOUVERNEMENTALES

	Agences	Création	Personnel	Budget
1	Office of the Director of National Intelligence	2004	100’000	40 Mia $
2	Air Force Intelligence			
3	Army Intelligence			
4	Central Intelligence Agency	1947	17’000	3 Mia $
5	Coast Guard Intelligence			
6	Defense Intelligence Agency	1961	7’500	classifié
7	Department of Energy			
8	Department of Homeland Security	2003	17’000	inconnu
9	Department of State	1946	300	inconnu
10	Department of Treasury			
11	Federal Bureau of Investigation	1908	11’400	4 Mia $
12	Marine Corps Intelligence			
13	National Geospatial-Intelligence Agency			
14	National Reconnaissance Office	1960	3’000	classifié
15	National Security Agency	1952	20’000	4 Mia $
16	Navy Intelligence			

ANNEXE C : DIRECTIVE DU PRESIDENT TRUMAN INSTITUANT LA NSA

A 20907 9/4/54/080 COPY

Oct 24 1952

MEMORANDUM FOR: The Secretary of State
The Secretary of Defense

SUBJECT: Communications Intelligence Activities.

The communications intelligence (COMINT) activities of the United States are a national responsibility. They must be so organized and managed as to exploit to the maximum the available resources in all participating departments and agencies and to satisfy the legitimate intelligence requirements of all such departments and agencies.

I therefore designate the Secretaries of State and Defense as a Special Committee of the National Security Council for COMINT, which Committee shall, with the assistance of the Director of Central Intelligence, establish policies governing COMINT activities, and keep me advised of such policies through the Executive Secretary of the National Security Council.

I further designate the Department of Defense as executive agent of the Government, for the production of COMINT information.

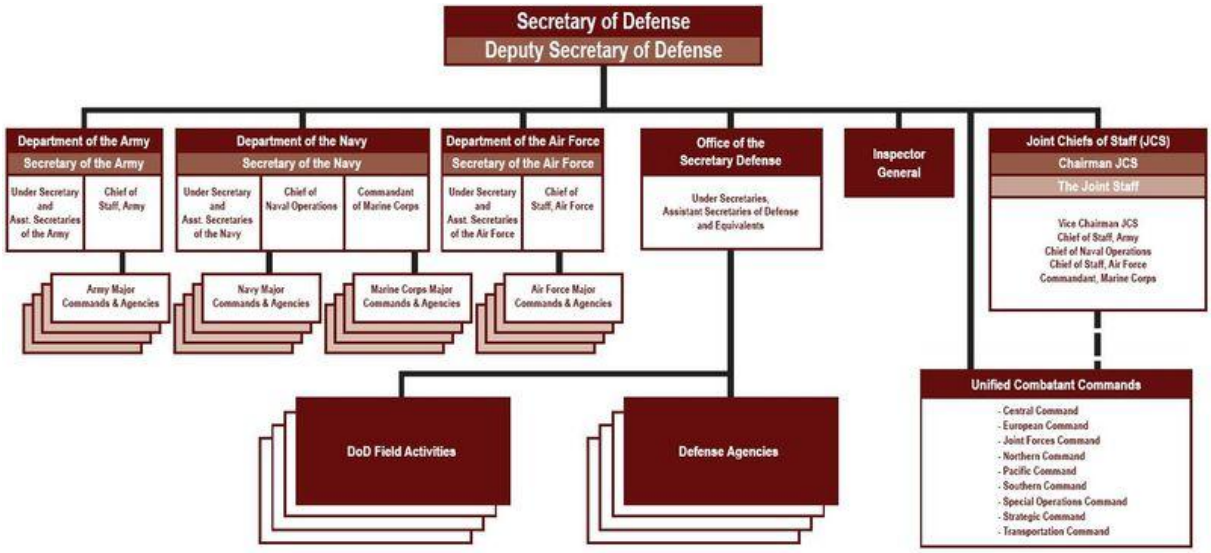
I direct this Special Committee to prepare and issue directives which shall include the provisions set forth below and such other provisions as the Special Committee may determine to be necessary.

1. A directive to the United States Communications Intelligence Board (USCIB). This directive will replace the National Security Council Intelligence Directive No. 9, and shall prescribe USCIB's new composition, responsibilities and procedures in the COMINT fields. This directive shall include the following provisions:

a. USCIB shall be reconstituted as a body acting for and under the Special Committee, and shall operate in accordance with the provisions of the new directive. Only those departments or agencies represented in USCIB are authorized to engage in COMINT activities

COPY NUMBER ___ OF ___ COPIES
PAGE 1 OF 8 PAGES

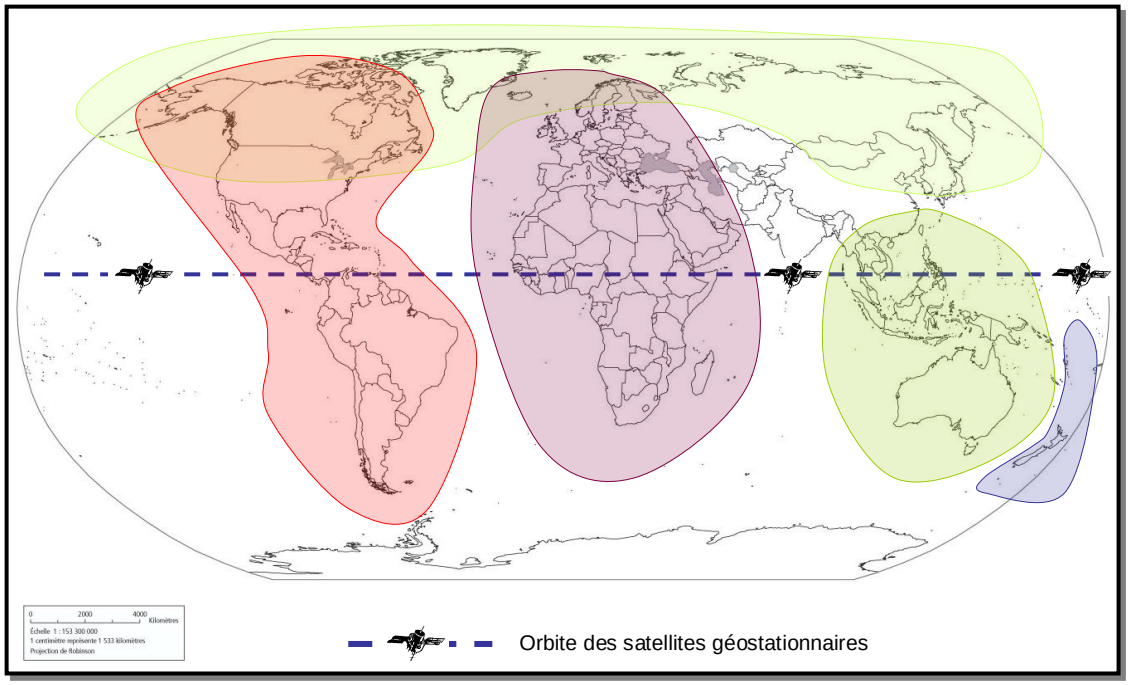
ANNEXE D : DEPARTEMENT DE LA DEFENSE ET NSA



Organigramme du département de la défense, la NSA se trouve parmi les 17 *Defense Agencies*

Siège de la NSA, Ft Meade, Maryland

ANNEXE E : PARTICIPANTS A L'ALLIANCE UKUSA ET ZONES DE COUVERTURE



Pays du pacte UKUSA

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
http://www.nsa.gov

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
http://www.gchq.gov.uk/

Canada
Le C.S.E : Communications Security Establishment

Employés : environ 900
Budget : environ 70 millions de $ par an
Nom de code : Uniform
http://www.cse-cst.gc.ca/

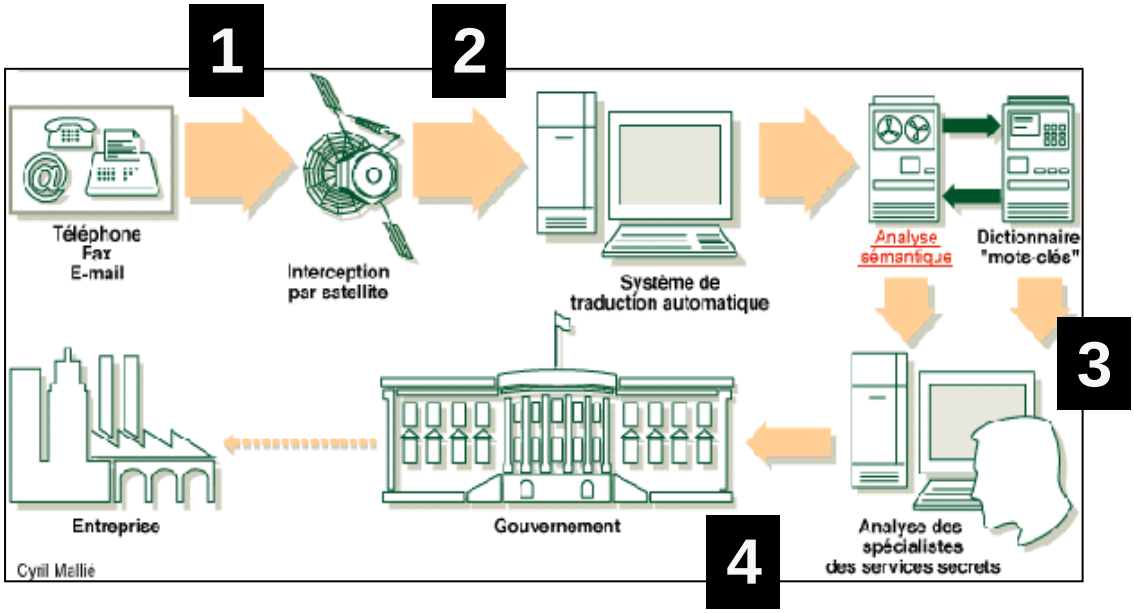
Australie
Le D.S.D : Defense Signals Directorate

Employés : environ 1000
Budget: Non connu
Nom de code : Echo
http://www.dsd.gov.au/dsd/

Nouvelle-Zélande
Le G.C.S.B : Governement Communications Security Bureau

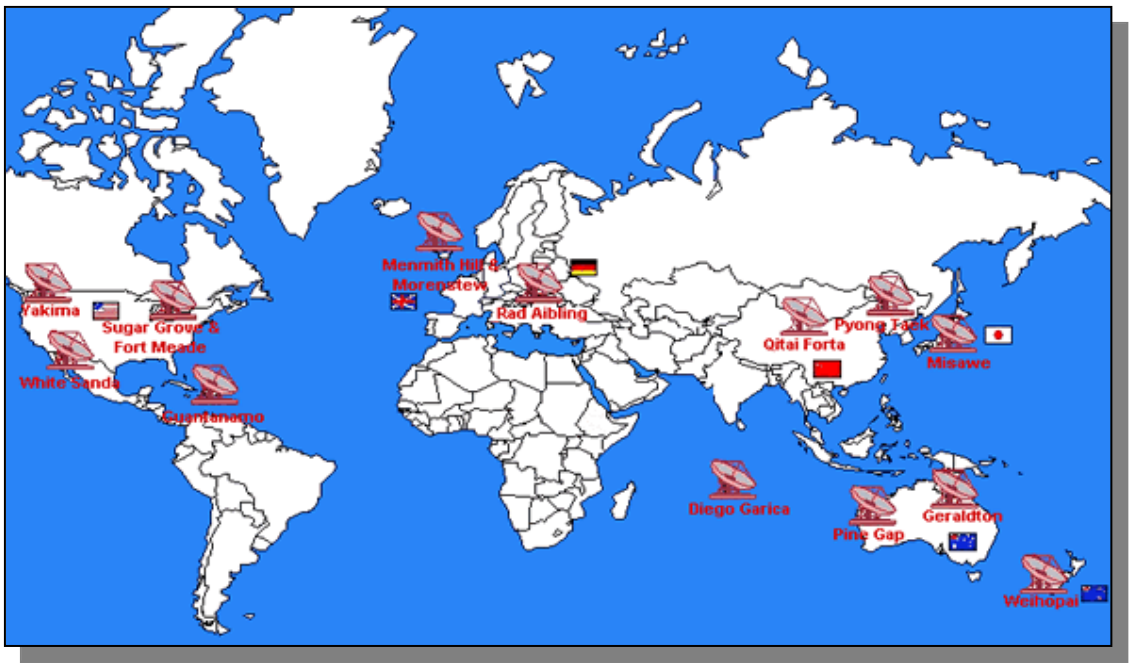
Enployés : environ 250
Budget : environ 20 millions de $ par an
Nom de code : India
http://www.gcsb.govt.nz/

ANNEXE F : LE CYCLE DU RENSEIGNEMENT



1. Phase de planification et conduite
2. Phase de collecte de l'information
3. Phase d'exploitation de l'information
4. Phase de diffusion du renseignement

ANNEXE G : LES PRINCIPALES STATIONS D'ECOUTE DU RESEAU ECHELON



Stations principales		Pays	Cibles	Couverture	Fonction
Yakima	6	Etats-Unis	INTELSAT	Pacifique	COMINT
Sugar Grove	10	Etats-Unis	INTELSAT	Atlantique, N-S Amérique	COMINT
Fort Meade		Etats-Unis			Exploitation de données
Morwenstow	21	Royaume-Uni	INTELSAT	Europe	COMINT
Menwith Hill	30	Royaume-Uni			COMINT + Réception
Geraldton	4	Australie	INTELSAT	Pacifique	COMINT
Waihopai	2	Nouvelle Zélande		Pacifique	COMINT
White Sands		Etats-Unis			IMINT
Guantanamo		Cuba			COMINT
Bad Aibling	14	Allemagne			SIGINT
Qitai Korta		Chine			COMINT
Pyong Teak		Corée du Sud			COMINT
Misawa	1	Japon			COMINT + Crypto
Pine Gap	18	Australie			SIGINT + IMINT
Diego Garcia		Océan indien		Océan indien	COMINT
Sabana Seca	5	Puerto Rico			Exploitation de données

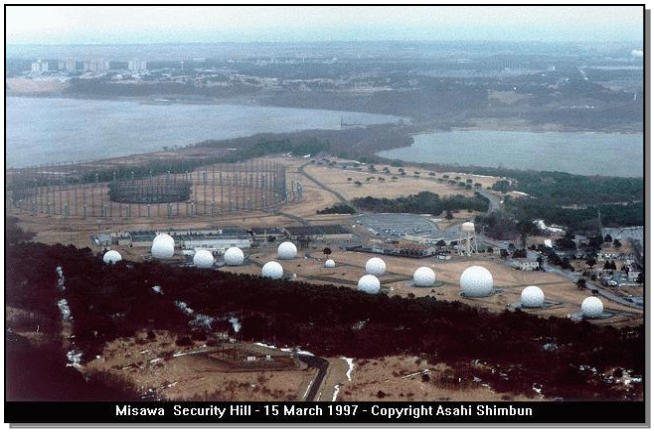
ANNEXE H : LES DIFFERENTS TYPES D'ANTENNES

Radôme - Menwenth Hil (Royaume Uni)

Antenne parabolique - Sugar Grove (Etats-Unis)

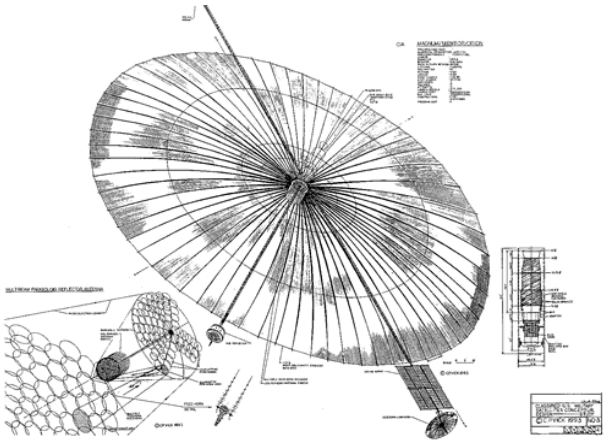
Orientation des signaux hertziens

Ecoute de signaux hertziens

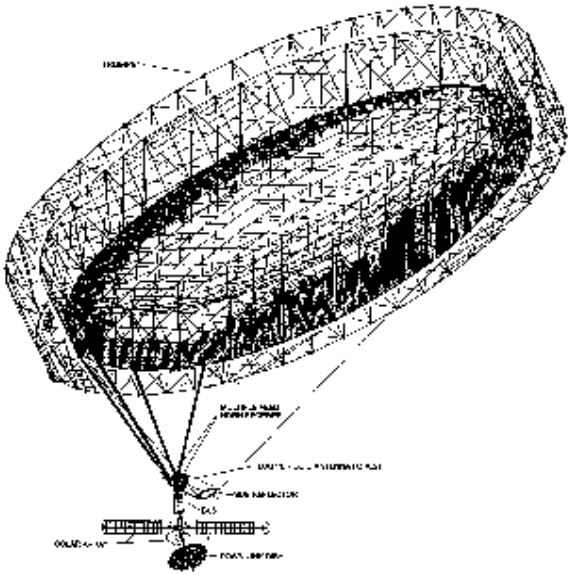


Site de Misawa (Japon)

ANNEXE I : LES SATELLITES D'ECOUTE

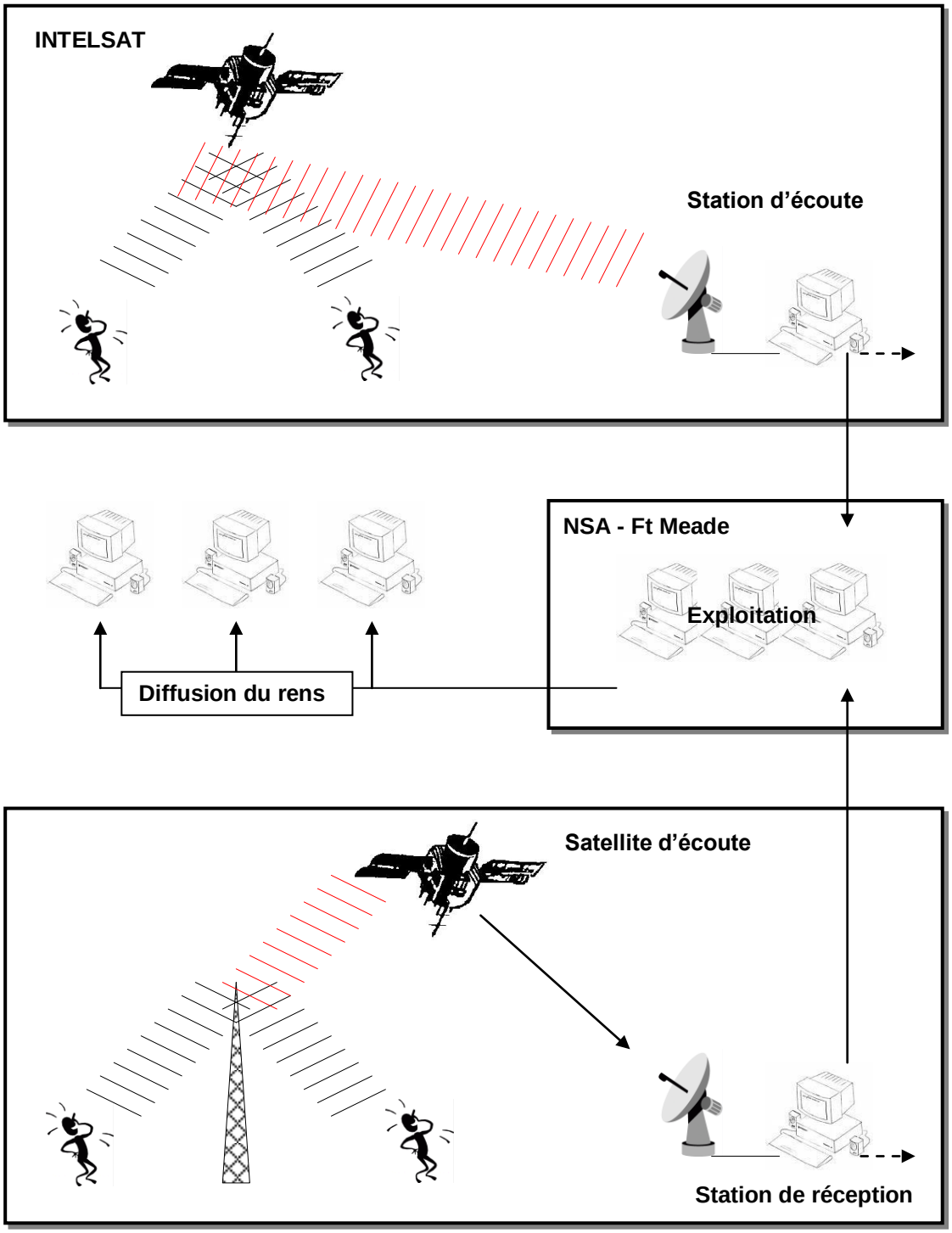


Satellite d'écoute de type MERCURY

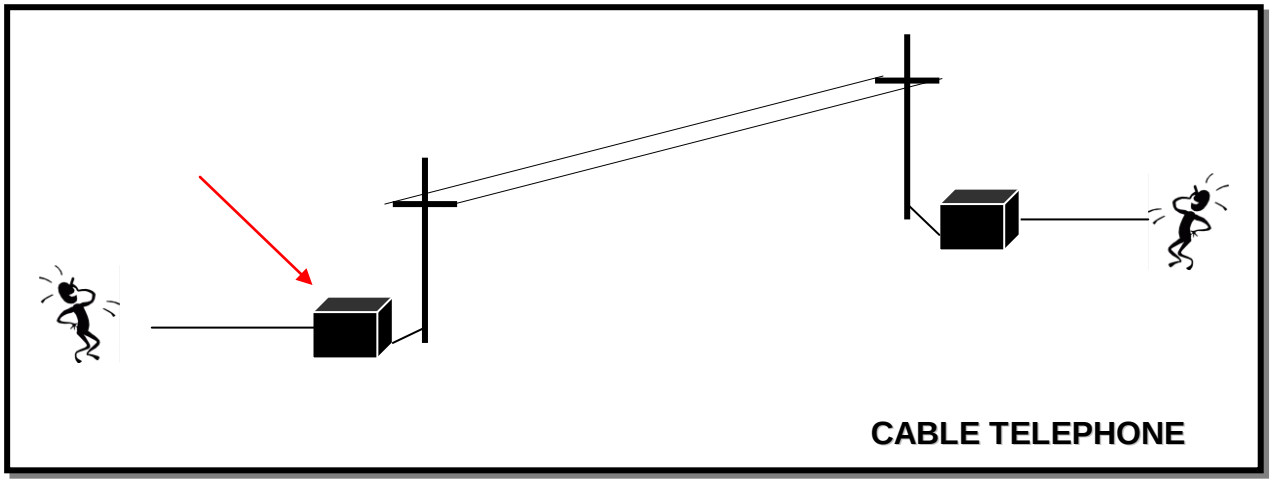


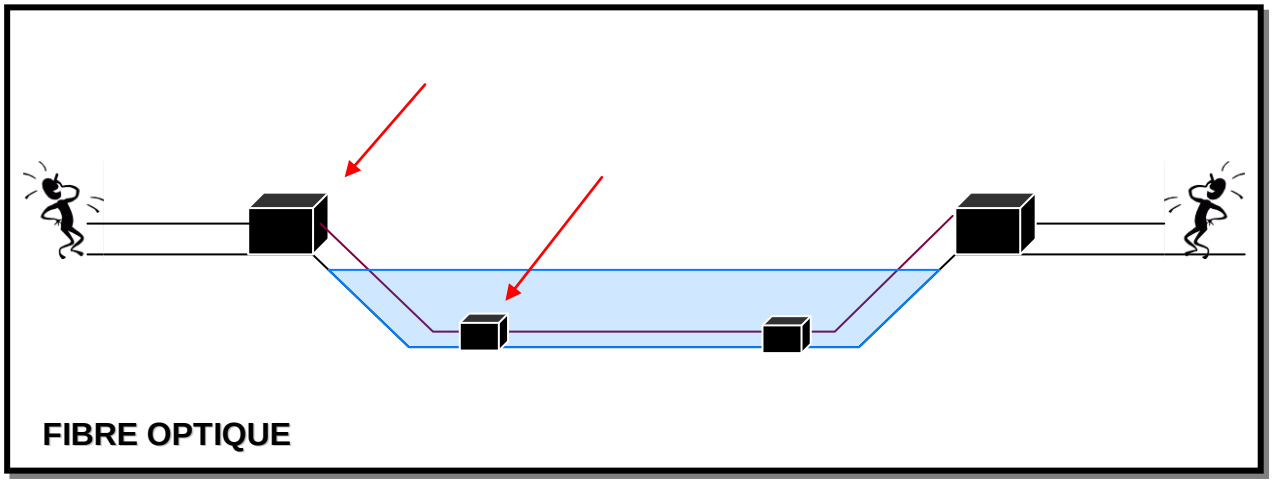
Satellite d'écfoute de type TRUMPET

ANNEXE J : LE FONCTIONNEMENT DES TRANSMISSIONS PAR ONDES



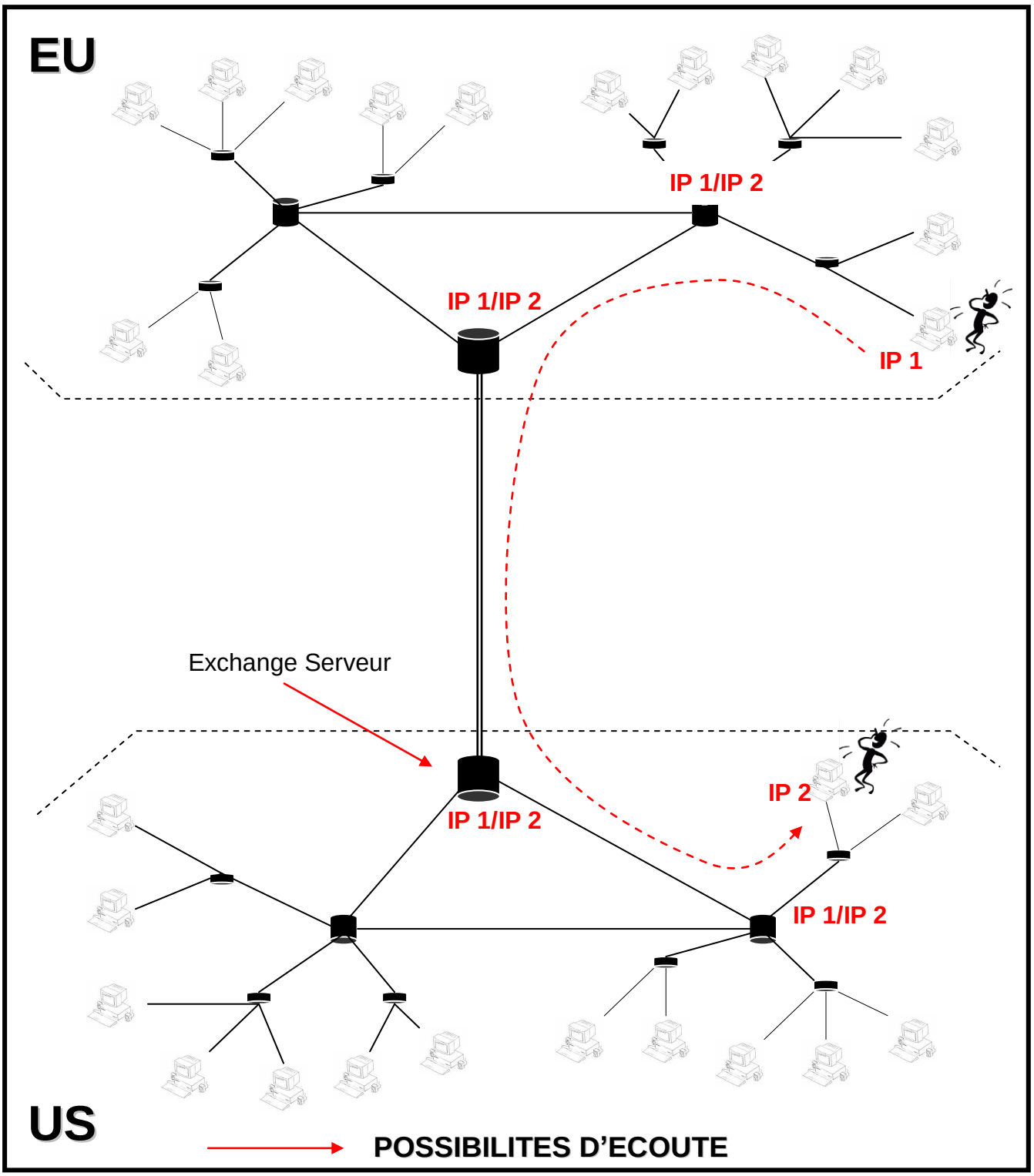
ANNEXE K : LE FONCTIONNEMENT DES TRANSMISSIONS PAR CABLE





POSSIBILITES D'ECOUTE

ANNEXE L : LE FONCTIONNEMENT DES TRANSMISSIONS PAR INTERNET



ANNEXE M : LES POSSIBILLITES D'ECOUTE D'INTERNET

Internet

On peut penser que c'est là le bas blesse pour la NSA. Internet étant un réseau mondial constitué de milliers de serveurs où des quantités de données gigantesques y circulent chaque jour (des milliers de Go ?).

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".

Deuxième point, Internet est originaire des Etats-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 Etats Unis, ainsi que la majorité des ressources qui vont avec (Routeurs, serveurs, backbones...) En clair cela signifie qu'aujourd'hui les ressources physiques se trouvant majoritairement aux USA, de nombreuses connections provenant de l'étranger passeront là bas.

Les messages transitent sur le Web sous forme de "packets" appelé 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 unique pour chaque serveur connecté sur le Web, il devient facile de réaliser un tri selon l'origine, la destination. Ce processus s'effectue bien entendu, en permanence par les routeurs, et les échangeurs afin d'acheminer correctement les messages, mais il facilite aussi 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 Etats Unis sont calmes quand ceux de l'Europe atteignent des pointes d'activité dû 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 US, ce qui rend l'écoute des mails d'autant plus accessible par la NSA.

Des sites où sont hébergés les news group tel que Usenet produisent environ 15 Go de données par jour. Ces données sont accessibles à n'importe qui souhaite les consulter. Elle permet donc à la NSA de 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 donnée de 1 Tera Octet comprenant 90 jours de messages usernet.

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 tel que Altavista, Hotbot. pour ne nommer que les plus connus, 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 jya.com (www.jya.com/crypto.htm) propose de nombreuses informations touchant à la crypto ou les 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.

Il est admis que le trafic Internet au niveau international contenant des informations pouvant intéresser les agences d'écoutes (emails, transfert de fichiers, réseaux privé virtuel), ne représente que quelques pourcents de la majorité du trafic sur les points d'échanges US. Selon un ancien employé de la NSA, cette dernière avait depuis 1995, installé des logiciels de type sniffers (renifleur) pour analyser le trafic sur les 9 échangeurs US (Internet Exchange Point - IXP). 2 de ces points, FIX east, Fix West appartiennent au gouvernement US. Ils sont implantés très proche des autres échangeurs appartenant à des sociétés commerciales : MAE East & MAE West (MCI Worldcom). Les 3 autres sites sont des échangeurs initialement développés par la National Science Foundation pour fournir au Web américain le backbone d'origine du Web (Le backbone représentant en quelque sorte la colonne vertébrale du Web, par où transitent de très nombreuses connexions).

Tableau des échangeurs américains surveillés par la NSA :

Nom de l'échangeur

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

(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 logiciels permettant de capturer des informations intéressantes sur le net. 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.

Source : La National Security Agency
http://perso.orange.fr/nakite/article/nsa/nsa.html

Table des matières