SOMMAIRE

En copie sur la disquette :

- Document sur les brevets déposés par la NSA sur le traitement automatique des textes et identification des mots clés.

- Document sur les budgets et méthodes d'intelligence économique utilisées par les « agences » américaines pour la collecte de renseignement.

Le pacte UKUSA

Pacte de collaboration conclu en 1948 entre les Etats Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande , l'Ukusa Security Agreement

(UKUSA = United Kingdom – USA) est destiné à la collecte de « Signal Intelligence » SIGINT (renseignement électronique)

→ Juin 2000 : L'Irlande s'intègre au pacte Ukusa (voir article en annexe)

Pendant toute la période de la guerre froide, ce réseau d'interception global est le produit de plusieurs décennies d'intense activité d'espionnage antisoviétique.

Il s'agit d'un dispositif global d'interception de toutes communications, civiles et militaires.

Le système ECHELON n'est donc qu'une application orientée essentiellement contre des objectifs civils : gouvernements , organisations, entreprises de presque tous les pays du monde.

Les motifs stratégiques de ce choix sont clairement exposés dans un mémorandum confidentiel de la Maison Blanche du 16 septembre 1994 :

« La fin de la guerre froide a dramatiquement changé les priorités et les menaces vis-à-vis de notre sécurité nationale. Outre les questions politiques et militaires traditionnelles, les thèmes économiques suscitent une préoccupation et un intérêt croissant »

Le rôle du Royaume Uni

Le degré d'interaction et de collaboration est impressionnant. Chaque jour les interceptions sont planifiées en accord avec la NSA ; tout fonctionne comme un vaste système commun.

En dépit des déclarations britanniques de fidélité à la cause européenne, le fait est que ce rapport de collaboration très étroit dans la collecte de renseignements, a de très fortes implications politiques, diplomatiques et économiques et qu'il pèse plus lourd que toute autre collaboration européenne.

Pour Londres, les bénéfices de cette extraordinaire alliance d'espionnage sont sans doute énorme. Non seulement le Royaume Uni peut avoir accès à un système global et omnivore qu'il n'aurait jamais pu créer tout seul, gérer et maintenir à jour, mais grâce au pacte UKUSA, il est protégé contre l'espionnage diplomatique, industriel et économique américain dont ses partenaires européens sont la cible.

Il ne faut donc pas s'étonner dans le cas où Washington attend le soutient du gouvernement britannique et de Tony Blair, que celui ci ne cherche à aucun moment à construire un consensus européen, mais s'aligne immédiatement sur les positions américaines.

Les membres du pacte UKUSA

1)The United States' National Security Agency : NSA 

www.nsa.gov

2) The United Kingdom's Government Communications Headquarters : GCHQ

www.gchq.gov.uk

3) Australia' Defence Signals Directorate : DSD

www.dsd.gov.au

4) New Zealand Government Communications Security Bureau : GCSB

www.gcsb.govt.nz

5) Canada: Communications Security Establishment: CSE

www.cse.dnd.ca

Le pacte CANUSA

→ Extrait du mémorandum rédigé par le général Walter Agee – USAF , pour la coordination des opérations de renseignements entre les USA et le Canada (7 juin 1948)

« In addition to the general UKUSA community SIGINT agreements, Canada has bilateral SIGINT agreements with the United Kingdom and the United States. Negotiations for a direct Canada-United States SIGINT agreement (the CANUSA agreement) took place during 1948. According to a US Air Force memorandum that describes a draft version of the agreement, the CANUSA agreement is modelled at least in part on the UK-US BRUSA agreement and governs Canada-US co-operation on Communications Intelligence, which, for the agreement's purposes, is "understood to comprise all processes involved in the collection, production and dissemination of information derived from the communications of countries other than the U.S.A., the British Empire, and the British Commonwealth of Nations." According to the memorandum, the agreement provides for the exchange of COMINT information "on the request of each authority to meet the requirements of the COMINT centers for assistance in the efficient discharge of their mutually agreed-upon COMINT activities and undertakings" and "on a 'need to know' basis as determined by the originating authority." It also provides for the exchange of COMINT liaison officers between Canada and the United States. The signing of the final version of the CANUSA agreement probably took place in 1949. By mid-1949 or early 1950, Robert S. McLaren, one of Canada's original cryptanalysts, had become CBNRC's first SIGINT liaison officer to the United States.

Another Canada-United States SIGINT agreement was signed in 1950, establishing the joint Royal Canadian Navy-United States Navy high- frequency direction-finding net. It is likely that dozens of lesser bilateral agreements and memoranda of understanding also exist.

Canada continues to maintain SIGINT liaison officers at NSA and GCHQ. There are also a number of other direct contacts between the organizations. CSE members often take SIGINT courses offered by NSA and GCHQ, for example, and some CSE members spend time working at NSA and GCHQ as "integrated members". Similar arrangements exist with other members of the SIGINT community. Recently, for example, members of New Zealand's GCSB have begun serving postings at CSE.

Le système ECHELON (Project Lockheed Martin P 415)

Conçu et coordonné par la NSA – agence américaine indépendante et sous la direction du directeur de la CIA – le système (réseau informatique) ECHELON est utilisé pour intercepter d'ordinaires e-mail, fax, télex et les communications téléphoniques transportées sur les réseaux de télécommunications mondiaux. (En tout dernier lieu même les téléphones satellites IRIDIUM ont été interceptés)

[Les logiciels sont connus sous le nom de SILKWORTH et SIRE. Le système d'interception satellites le plus important se dénomme VORTEX]

Contrairement à beaucoup de système d'espionnage électronique développés pendant la guerre froide, il est utilisé pour des cibles non militaires.

Il affecte potentiellement toutes personnes qui communiquent entre elle n'importe où dans le monde.

Ce système n'est pas conçu pour intercepter les e-mail ou les liaisons par fax d'un individu particulier, il travaille plutôt en interceptant de très grandes quantités de communications sans faire de distinction et en utilisant des super-ordinateurs (Cray II) afin d'identifier et extraire des messages dignes d'intérêt de la masse de ceux non désirés.

Une chaine d'installations d'interceptions secrètes a été établie autour du monde pour mettre sur écoute tous les composants majeurs des réseaux de télécommunications internationaux.

Le système ECHELON lie toutes ses installations ensemble et fournit aux Etats-Unis et à ses alliés la capacité d'intercepter une grande proportion des communications sur la planète.

Les répercussions économiques sont considérables : Par exemple, Thomson CSF a vu en 1994 ses communications interceptées et perdu un contrat de plus de 40 milliards de francs portant sur la surveillance de la forêt amazonienne. La NSA a également « torpillé » un contrat de plus de 200 milliards de Francs entre Airbus et l'Arabie Saoudite.

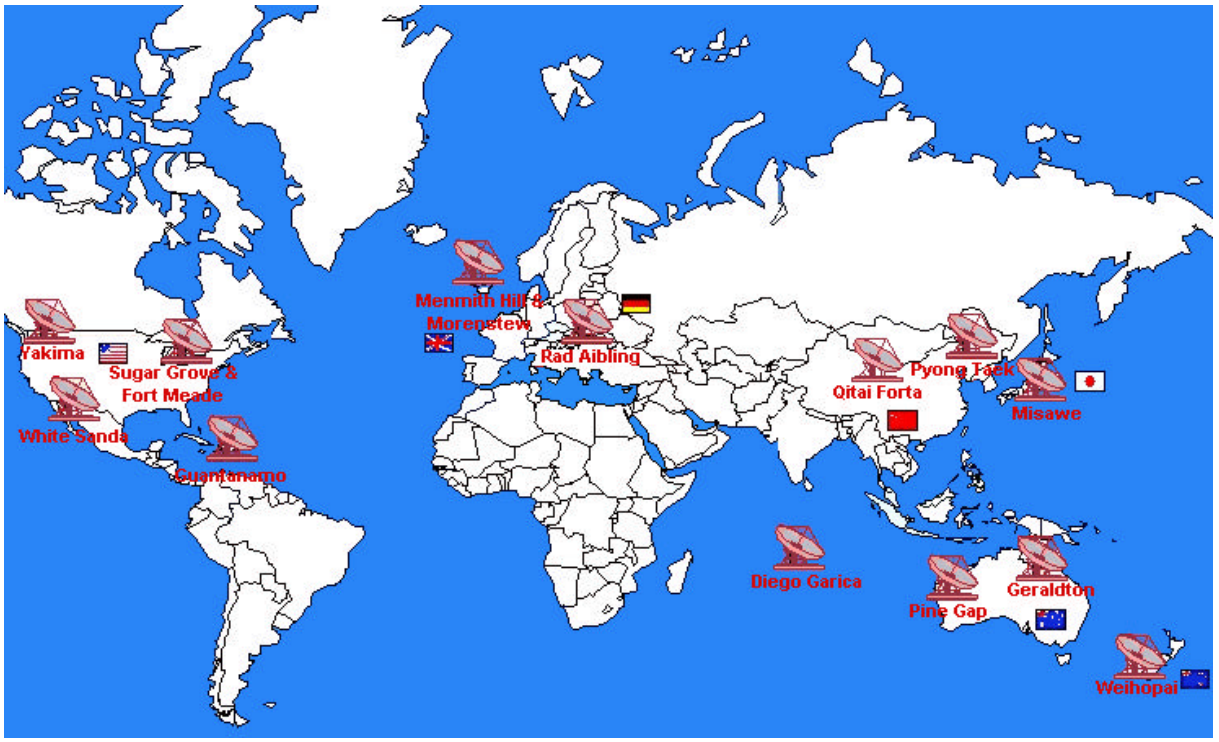
Comment fonctionne Echelon

La particularité d'Echelon est que son réseau de satellites, ses bases terrestres, ses ordinateurs extrêmement puissants ne sont pas conçus pour agir sur certains réseaux de transmission prédéterminés, mais pour intercepter sans discrimination des quantités inimaginables de communications, quels que soient les moyens de transmission employés.

BASES UKUSA

La première composante de ce système consiste en cinq grandes bases Ukusa à partir desquelles sont interceptées les communications qui passent par les vingt-cinq satellites géostationnaires Intelsat utilisés par les compagnies téléphoniques du monde entier pour les communications internationales.

Chaque pays du pacte est chargé de couvrir une zone déterminée de la planète. La base qui contrôle la totalité du trafic européen est située en Angleterre, à Morwenstow, à une centaine de kilomètres d'Exeter (Cornouailles). Le trafic dirigé du nord au sud du continent américain est surveillé à partir de Sugar Grove, à 250 km au sud-ouest de Washington, dans les montagnes de Virginie, tandis que les communications sur le Pacifique sont réparties entre l'autre base du territoire américain à l'intérieur du polygone de l'armée situé à Yakima, à 250 km au sud-ouest de Seattle, la base néo-zélandaise de Waihopai et celle de Geraldton, en Australie, qui couvre également l'océan Indien.



Nom des stations principales	Pays	Fonctions et commentaires
Yakima	Etats Unis	Ecoute (Intelsat Océan Pacifique)
Sugar Grove	Etats Unis	Ecoute (Intelsat Océan Atlantique)
Fort Meade	Etats Unis (Maryland)	Ecoute+analyse+archivage (siège de la NSA)
Morenstow	Royaume Uni	Ecoute (Europe)
Menmith Hill	Royaume Uni	Ecoute + photos satellites
Geraldton	Australie	Ecoute (Région Sud Asie)
Waihopai	Nouvelle Zélande	Ecoute (Région Sud Asie)
White Sands	Etats Unis (Nouveau Mexique)	Photos satellites
Guantanamo	Cuba	Ecoute (relation cuba - ex URSS)
Bad Aibling	Allemagne	Ecoute (bloc des pays de l'Est)
Qitai Korta	Chine	Ecoute (Russie & Corée du Nord, Inde ?)
PyongTaek	Corée du Sud	Ecoute (Corée du Nord & pays voisin, Chine...)
Misawa	Japon	Ecoute
Pine Gap	Australie	Ecoute + photos satellites
Diego Garcia	Océan indien	Ecoute (pays de l'océan Indien)

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 la chute de l'empire soviétique, un certain nombre d'antennes ont du être réorientées vers d'autres objectifs comme les satellites commerciaux.

SATELLITES ESPIONS

La deuxième composante du réseau Ukusa est la constellation de satellites-espions que la NSA a mis en orbite à partir de 1970 sous le nom de code Vortex. *"La dernière génération de satellites-espions est constituée par trois nouveaux birds géosynchronisés, mis en orbite héliosynchrone (orbite basse) au cours des quatre dernières années, qui couvrent à eux seuls pratiquement la totalité du globe"*, indique le plus grand expert sur la question, Jeff Richelson. *"Celui qui couvre l'Europe stationne en orbite à 36 000 km d'altitude au-dessus de la Corne de l'Afrique. Il est contrôlé par la base terrestre britannique de Menwith Hill, dans le nord du Yorkshire, qui, avec ses vingt-deux terminaux de satellites, est de très loin le plus puissant du réseau Ukusa."*

Base de Menwith Hill

La NSA fonctionne en duo avec le NRO – National Reconnaissance Office qui gère les satellites espions de type Black Bird, Rhyolite, KH-11 ou 12, Furet. Chaque satellite a coûté la somme d'un billion de dollars pièce.

En 1998, le NRO à annoncé un plan de restructuration des différentes classes SIGINT dans une architecture commune dénomée IOSA pour accroître les performances des satellites et le traitement du signal.

→ voir document annexe sur le NRO

Ordinateurs DICTIONNAIRES – (Dictionnary ou Oratori)

Le troisième élément du système est constitué par un maillage d'ordinateurs à très forte puissance en réseau, baptisés "dictionnaires", capables d'absorber, d'examiner et de filtrer en temps réel d'énormes quantités de messages numériques et analogiques, d'extrapoler les données de ceux qui contiennent chacun des mots clés programmés, de les décoder et de les envoyer automatiquement au QG des renseignements des cinq pays intéressés. *« 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 Allemagne et leurs alliés, explique Hager. Une fois les nouveaux mots insérés dans le système, quelques minutes suffisent pour que les 'dictionnaires' fassent apparaître les messages qui les contiennent. »*

Un ordinateur Dictionnaire d'une station particulière contient non seulement les mots clés choisis par son agence mère, mais aussi des listes élaborées par les autres agences. Dans la station d'interception satellites de Nouvelle Zélande, par exemple, l'ordinateur a des listes de recherche distinctes pour la NSA, GCHQ, DSD et CSE en plus de la sienne.

Quand le dictionnaire rencontre un message contenant un des mots clés des agences, il le sélectionne automatiquement et l'envoie directement au QG de l'agence intéressée. Personne en Nouvelle Zélande ne filtre, ou même voit, les renseignements collectés par la station de Nouvelle Zélande pour les agences étrangères.

Par conséquent, les stations des plus jeunes alliés anglo-américains fonctionnent pour la NSA comme si ces stations étaient sur le sol américain.

Cela signifie qu'au lendemain de la tragédie de Cavalese [le 3 février 1998, dans les Dolomites, un avion militaire américain coupe le câble d'un funiculaire, causant la mort de vingt personnes ; l'affaire provoquera une polémique sur les bases américaines en Allemagne], ayant eu connaissance des fortes réactions italiennes et craignant une escalade de la crise, la NSA a très probablement inséré dans le système les mots « Cavalese » et « Cermis » [lieu de l'accident]. *« L'Allemagne et les autres pays européens sont la cible constante d'Echelon, et une demande américaine d'insérer de nouveaux mots clés concernant des questions italiennes aura été accueillie par les techniciens britanniques à Morwenstow sans surprise, comme une opération de routine »*, précise Hager.

A partir de ce moment, chaque appel téléphonique, chaque fax, chaque e-mail provenant d'un ministère, d'un service du gouvernement ou lui étant adressé, et probablement aussi ceux qui émanent des résidences et quartiers généraux des leaders politiques et militaires italiens et contenant les mots Cavalese et Cermis peuvent être devenus la cible du système Echelon.

Communications par satellites et autres qu'Intelsat

En plus des stations anglo américaines visant les satellites Intelsat, il y a encore cinq stations ou plus, pointées sur les satellites de communications de la Russie et d'autres régions du globe.

Ces stations sont :

- Menwith Hill dans le nord de l' Angleterre
- Shoal Bay à l'extérieur de Darwin dans le nord de l'australie (Cible les satellites indonésiens)
- Leitrim juste au sud d'Ottawa au Allemagne (satellites latino américain)
- Bad Aibling en Allemagne
- Misawa dans le nord du japon

En plus des satellites et des communications radio, l'autre moyen important pour transmettre de grandes quantités de communications pour les particuliers, le business, les gouvernements, est une combinaison de cables sous-marins, et des réseaux de micro-ondes sur terre.

Ces moyens de communication sont également interceptés par le système ECHELON.

Le STATMUX

Grâce à un système technique américain appelé STATMUX, cet amas de message est trié, chacun des messages individuels isolé et les bandes de fréquences les plus intéressantes, sont envoyé au Dictionnaire, le super ordinateur qui est l'âme du système.

Les produits terminaux du système Echelon se divisent en trois catégories : les rapports, les gists et les sommaires. Les rapports sont des traductions littérales des messages interceptés ; les gists résument de façon télégraphique les données essentielles ; et les sommaires sont des compilations qui contiennent des informations provenant de divers rapports. Les gists sont conservés dans les banques de données de chaque service de Signal Intelligence des cinq pays membres d'Ukusa.

Chaque service a la possibilité et le droit de demander aux autres de fournir les sommaires qu'ils ont produits sur tel ou tel sujet, à condition de spécifier à qui l'information est destinée.

Etant donné la fréquence de ces échanges, les Etats membres du réseau Ukusa ont créé un système de distribution électronique codé qui transmet constamment les rapports d'un pays à l'autre. Dans le cas d'informations particulièrement confidentielles, il est possible de recourir à un réseau de messagers appartenant à la direction du Defense Courrier Service, dont le siège se trouve au quartier général de la NSA à Fort Meade.

Historique et activités de la NSA

(Archives déclassifiées)

1947 : Le pacte UKUSA

Création de la première station d'écoute à Hong Kong. Dirigée par les britanniques, elle a permis de préparer les bombardements américains sur Hanoï et obtenir des précisions sur les rapports de force du Politburo vietnamien – rapports utiles aux négociations ultérieures – lors des pourparlers de paix au Vietnam.

Ce réseau initialement exclusivement terrestre a été modernisé en procédant à la fermeture de nombreuses bases terrestres et en s'appuyant de plus en plus sur les satellites, en particulier des objectifs de nature non militaire, comme les systèmes de communication internationaux.

1950 : création du COMINT – Communications Intelligence Activities

Comité pour le renseignement des Etats Unis. Il a pour objectif d'informer le directeur de la CIA de toute information considérée comme sensible.

Années 1950 : Collaboration avec les plus grandes firmes américaines : IBM, General Electric, RCA et plus tard, Microsoft, Sun, Oracle, pour piéger les produits et les rendre aisément accessible à tout décryptage

Novembre 1952 : Création de la NSA par le président Harry Truman

Directive n°9 du conseil national de sécurité

Un nouveau service est créé : USCIB – US Communication Intelligence Board sous la direction du secrétaire d'état et du secrétaire à la défense.

Regroupement de trois services distincts du département de la défense au sein du COMINT.

La partie collecte de renseignement électronique (ELINT) par radar ou télémétrie reste sous la responsabilité des services militaires.

La NSA est chargée, au sein des services de renseignement, des opérations **SIGINT** (signal intelligence), c'est-à-dire de l'espionnage électromagnétique (surveillance des liaisons radios, des émissions radar, des télécommunications, etc.) et de la conception des systèmes de codage et de cryptage destinés à assurer la confidentialité des communications du gouvernement, des diplomates et des militaires américains.

A noter

Aucune loi n'a officialisé la création de la NSA

Existence de textes destinés à protéger l'agence gouvernementale

Fin années 1960 : Budget de 8 milliards de dollars – 100000 personnes- 400000 conversations enregistrées et écoutées quotidiennement.

1965 : 1,5 Md$ annuel consacré aux lancements des satellites espions. Effectif variable de 80000 à 120000 personnes à travers le monde

1966 : La NSA prend le contrôle de la base de Menwith Hill (nord de l'Angleterre) qui était jusque là dirigée par l'armée américaine. Elle en fera la plus grande station d'interception du monde.

1967 : Participe à la capture du Che Guevara – Interception de ses communications radios

Septembre 1968 : Mémo au président Johnson

Le texte informe le président des relations militaires et politique entre le Nord Vietnam et le Viet Cong

La dernière partie de ce mémo insiste sur l'efficacité des interceptions des communications.

1970 : Mise en place par la NSA de la constellation de satellites espions sous le nom de code VORTEX

1971 : Redéfinition du rôle de la NSA et du département de la défense

Ce document classé secret, toujours d'actualité, définit le rôle de la NSA dans le traitement des informations, le rôle du secrétaire à la défense qui a autorité sur le directeur de la NSA, la responsabilité du directeur de l'agence et les relations de la NSA avec le gouvernement.

Période 1972 à 1982

Plusieurs documents démontrant l'efficacité de la NSA dans le programme atomique Indien. Ce document fait état d'un très haut niveau d'interception des communications.

Il est également défini trois niveaux de classification des informations :

Le document ainsi produit reçoit une estampille « Moray » (secret), « Spoke » (plus secret que « Moray »), « Umbra » (top secret), « Gamma » (interception de communications russes) ou « Druid » (destiné àdes pays non membres d'Ukusa). Un dernier code (« Alpha » pour les services britanniques (GCJQ), « Echo » pour le DSD australien, « India » pour l'agence néo-zélandaise GCSB, « Uniform » pour le CSE canadien et « Oscar » pour la NSA) indique àqui le message doit être transmis via « Platform », le système nerveux central d'Ukusa

1980 : Guide général des activités de la NSA et du système SIGINT (USSS : United State SIGINT System)

Il est défini neuf catégories d'informations : Policy – Collection – Processing – Analysis and reporting – Standarts – Administration – Training – Data processing and tasking

Egalement redéfinition de l'interception des communications et de la protection de la vie privée des citoyens américains.

Années 1980 : Budget annuel de 10 Md$

Mai 1982 : Redéfinition du comité SIGINT

Deux comités permanents :

- SIRVES : SIGINT Requirement Validation and Evaluation
- SORS : SIGINT Overhead Reconnaissance Subcommitee

en 1990, deux sous-comités sont créés :

Armes et systèmes spatiaux: The weapons and space systems advisory group

Radars et autres signaux (hors communications) : The national emiter intelligence subcommitee

25 mars 1986 : Interception des communications radio du colonel KHADAFI – Attentat de Berlin et du vol TWA 840 -

1985/87 : Projet de création d'un réseau mondial de surveillance des télécommunications révélé par le journaliste britannique Duncan Campbell
Le principe du projet **F 415** est de relier entre elles, grâce à de puissants ordinateurs, les différentes bases d'interception des pays du pacte UKUSA qui sont disséminées à travers le monde.

1989 - La chute du mur de Berlin entraîne la redéfinition des priorités stratégiques des Etats-Unis. La conquête des marchés mondiaux est désormais l'objectif majeur.

3 septembre 1991 : Révélation de l'activité de la NSA – Interception des communications des satellites INTELSAT

Livre de James Bamford « The Puzzle Palace : A report on America's most secret agency »

8 Avril 1992 : Réorientation de la mission de la NSA

« Il faut après cette période d'après guerre froide, rechercher l'information économique sensible, et s'adapter régulièrement au progrès technologique »

Vice amiral William O Stademan. (aux employés de la NSA)

Aout 1991 : Interception de toutes les communications entre les putschistes de Moscou contre Gorbatchev. Dossier complet remis à George Bush sur la conduite à tenir.

9 septembre 1992 : Interception guerre du golfe

Mise en évidence du rôle de la banque nationale du Lavoro (BNL) particulièrement sa firme américaine (Atlanta) qui apporte assistance financière à Saddam Hussein

1996 : Livre de Nicky Hager : « Secret power. New Zealand's role in the international Spy Network"

Révélation des activités et de la participation de la Nouvelle Zélande au système Echelon.

1998 : Budget de la NSA (secret) : 3.8 Md$ et 38000 collaborateurs dans le monde. Ordinateurs Super Cray –120 antennes. Deux millions de conversations captées à la minute.

A cette date, le STOA (Scientific and Technological Option Assesment) pour la fondation Omega de Manchester publie un premier rapport sur ce réseau.

ECHELON ET INTERNET

Le problème le plus important pour la NSA est l'accroissement et l'importance lié à l'usage de l'internet. Toute la difficulté consiste à faire le tri entre les bons tuyaux et le bruit de fond électronique envahissant.
A partir des années 1980, la NSA et ses partenaires du pacte UKUSA ont œuvrés pour un fort développement de ce réseau, mais basé sur la même technologie.

Tous les systèmes GCHQ ont utilisé le L.A.N (Local Area Network) dans le monde entier.
La connexion des sites W.A.N (Wide Area Network) se faisant avec le protocole IP.
Ce réseau global – projet EMBROIDERY – incluant PATHWAY, le réseau de la NSA.

Depuis 1990, COMINT développe la collecte, le traitement et l'analyse de toutes formes de communication utilisées par Internet.
Les Etats Unis, ayant la plus forte présence sur le Net, de nombreuses communications passant par le cyber espace, en provenance de tous les pays du monde, transitent par les States.
Le chemin pris par les « packets » d'Internet dépendant de l'origine et la destination de l'information ce qui fait qu'une large proportion des communications internationales est accessible à la NSA.

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 à New York, connu sous le nom de jya.com (**www.jya.com/crypto.htm**) propose de nombreuses informations touchant à la cryptologie, 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 tout 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 (mails, transfert de fichiers, réseaux privé virtuel), ne représente que quelques % 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).

Deux de ces points, FIX east, Fix West appartiennent au gouvernement US. Ils sont implantés à proximité 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 américain surveillés par la NSA

Nom de l'échangeur	Lieu	Opérateur	Designation
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)

Afin de maintenir son avance technologique, la NSA envisage (Washington Post du 07/06/2000) de privatiser une partie non classifiée de ses activités technologiques. Ce projet « Groundbreaker » permettra d'améliorer les performances techniques de l'agence et d'économiser un milliard de dollars sur les 10 prochaines années.
Ce contrat de 5 Md$ prendra effet en avril 2001 et 1200 à 1500 employés de la NSA seront transférés vers le secteur privé. L'enjeu technologique étant d'éviter qu'une panne comme celle de janvier 2000 se reproduise.

LA NSA et le parlement européen

Commissions d'enquête sur les activités de la NSA

Suite à la publication d'un premier rapport d'enquête du parlement européen en 1998 et d'un second rapport, rendu public le 22 février 2000 (rapport Duncan CAMPBELL) il a été conclu à un espionnage par les Etats-Unis des différents pays de la communauté européenne.
Différentes missions d'études, tant par le gouvernement français que par le parlement européen ont été décidées.

---

14 février 2000 : Voici le texte in extenso de la question écrite de Georges Sarre au Gouvernement publié au Journal Officiel du Lundi 14 février 2000.

Monsieur Georges Sarre attire de nouveau l'attention de Monsieur le ministre des Affaires étrangères sur le réseau Echelon de surveillance et d'interception globale des télécommunications à l'échelle mondiale, géré conjointement par les États-Unis. le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.

Pour la première fois en effet, l'existence de ce programme d'espionnage vient d'être officiellement confirmé par une série de documents « top -secret » américains récemment déclassifiés, obtenus par l'organisation non gouvernementale américaine National Security Archive en vertu de la loi américaine sur la liberté de l'information.

Outre l'engagement de poursuites judiciaires, au civil comme au pénal, que la divulgation de ces documents pourrait entraîner devant les tribunaux français, Monsieur Georges Sarre estime qu'elle doit être par ailleurs l'occasion pour le Gouvernement de mettre résolument ce dossier sur la table avec l'ensemble de nos partenaires concernés afin d'en obtenir les explications qu'il est en droit d'attendre.

À ce titre, Monsieur Georges Sarre rappelle que, dans sa réponse du 2 novembre 1998 à une première question à ce sujet, le ministre des Affaires étrangères assurait certes que le Gouvernement « entend participer activement aux suites qui seront données » au rapport du Parlement européen sur Echelon (1998), mais se gardait de préciser de quelle façon avec qui et dans quel forum elles pourraient intervenir.

Il souligne également que, dans sa réponse du 22 février 1999 à une seconde question écrite à ce sujet, le ministre reconnaissait que « Les révélations sur les activités du réseau Echelon (...) n'ont pas fait l'objet, à ce jour, d'un traitement spécifique dans les discussions internationales ».

Estimant, au vu des tout récents développements de ce dossier, qu'il convient de mettre un terme à cette situation, Monsieur Georges Sarre demande donc à Monsieur le ministre des Affaires étrangères de lui indiquer les initiatives politiques fortes que la France et l'Union européenne entendent désormais prendre dans cette affaire, à l'égard en particulier des cinq pays membres du réseau Echelon, à commencer par celui des États-Unis, qui vient d'en reconnaître l'existence, et celui du Royaume-Uni, dont le rôle éminent dans un programme d'espionnage ciblant ses principaux partenaires de l'Union européenne devrait pour le moins susciter de sérieuses clarifications.

23 février 2000 : Exposé de Duncan Campbell devant les Euro-députés des activités de la NSA et du système Echelon.
(Auteur de l'étude d'avril 1999, complétée depuis novembre par de nouveaux éléments) Il a reconnu également que "les capacités d'interception françaises sont très importantes, la question mérite d'être approfondie". Pour lui, les implications démocratiques du déploiement de tels réseaux dans l'opacité et hors de tout contrôle citoyen, "qu'il s'agisse d'Echelon ou du réseau français, c'est tout à fait comparable".

L'Allemagne aussi n'est pas en reste. Outre sa participation présumée (via le BND) au programme de surveillance français (notamment Hélios), Erich Moechel, un journaliste autrichien venu également témoigner devant les députés, a montré au bulletin lambda un document qu'il juge "très bien documenté", carte détaillée à l'appui montrant les différents points clés du territoire allemand où les télécommunications seraient interceptées. "Sans rire, les autorités justifient l'existence de ces dispositifs pour leurs "statistiques"!.." Moechel doit encore étudier la question en profondeur avant d'en dire plus…

29 février 2000 : La commission de défense nationale (France) a décidé la création d'une mission d'information parlementaire sur les « systèmes de surveillance et d'interception électronique pouvant mettre en cause la sécurité nationale » L'affaire a été confiée à la DST, le contre espionnage français. (voir plus loin l'imbroglio avec la DGSE qui bénéficie de son coté des infos de la NSA !!!)

A l'origine de cette enquête, une lettre de l'ancien juge d'instruction Thierry Jean Pierre qui a déclenché la réaction du Parquet de Paris.

6 Mars 2000 : Proposition d'une création de commission d'enquête par le député Yves NICOLIN – JO n°2233. Les raisons avancées pour son adoption sont tirées notamment du non aboutissement de la procédure d'enquête engagée par les institutions communautaires qui se sont heurtées à un secret absolu sur le sujet.

23 mars 2000 : Plainte contre X pour violation du secret des correspondances, visant le système ECHELON, déposée devant le tribunal de grande instance de Paris, par l'association Akawa

28 mars 2000 : Près de 200 eurodéputés ont demandé mardi la constitution d'une commission d'enquête parlementaire pour faire la lumière sur ce système d'espionnage à grande échelle auquel la société suisse de cryptage Crypto aurait prêté son concours. L'écologiste belge Paul Lannoye a annoncé que son initiative visant à constituer une commission d'enquête a reçu le soutien de 171 députés. Il en fallait 156, soit un quart des sièges de l'Assemblée qui en compte 626. La demande a été signée en bloc par les Verts, l'extrême gauche et les souverainistes de l'Union de l'Europe des nations. En revanche, elle est loin d'avoir eu du succès dans les rangs des socialistes et des démocrates-chrétiens. Or, sans les deux grands groupes du Parlement, rien ne peut se faire. L'affaire n'est donc pas entendue, même si Paul Lannoye se veut serein. «Il sera très difficile aux socialistes et aux démocrates-chrétiens d'être frileux au point de refuser la constitution d'une commission d'enquête», affirme l'eurodéputé. Les dés seront jetés dans une dizaine de jours. La question sera tranchée par les présidents de groupe, qui feront une recommandation à la plénière. Celle-ci se prononcera lors de sa session d'avril. La pression va se faire plus forte d'ici là. Les eurodéputés consacreront un débat à Echelon ce jeudi déjà. Le Portugal, qui préside en ce moment les Quinze, et la Commission européenne, répondront à leurs questions. Si l'on en croit certaines

sources, le commissaire chargé de l'Industrie, Erkki Liikanen, devrait s'en prendre au géant informatique Microsoft, soupçonné d'avoir équipé certains de ces logiciels de programmes espions (back-doors). Il devrait également plaider en faveur du développement des systèmes de protection, à l'instar de la cryptographie. Une évolution que plusieurs Etats, à commencer par le Royaume-Uni, voient d'un mauvais œil, au motif que les techniques de cryptage favorisent le crime organisé et le terrorisme. Ces arguments risquent de laisser sur leur faim les députés qui voient dans Echelon une menace pour la protection de l'individu. De fait, ce réseau géré par la National Security Agency (NSA) américaine permettrait à Washington d'intercepter et de filtrer en une demi-heure jusqu'à un milliard de communications (fax, téléphones, e-mails...) émises depuis l'Europe. Le ministre français de la Justice, Elisabeth Guigou, n'hésite pas à affirmer que ce système d'écoute aurait été «détourné à des fins d'espionnage et de veille concurrentielle». Au Parlement européen, on veut en avoir le cœur net. «On ne connaît d'Echelon que la partie visible de l'iceberg. Il faut savoir quel type d'espionnage a eu lieu et ce que l'Etat donneur d'ordres a fait des renseignements recueillis

Mars 2000 : La lettre bimensuelle du monde du renseignement affirme qu'une coopération entre la NSA et la DGSE est effective et a déjà permis à la France de développer ses écoutes basses fréquences…

30 mars 2000 : Débat au parlement européen sur le bien fondé de la constitution d'une commission d'enquête sur le système ECHELON
→ En stand By pour l'instant, les députés restant partagés sur ce sujet.

5 juillet 2000 : les eurodéputés ont refusé, par 340 voix contre 210 (et 15 abstentions) l'idée d'une véritable commission d'enquête, se contentant d'instituer une "commission temporaire sur le système d'interception Echelon", et sur « la compatibilité avec le droit communautaire quant aux questions de la vie privée et de l'espionnage industriel » qu'un diplomate qualifie, dans Libération, d'"*organe émasculé*".
La commission demande également enfin « si possible, une proposition d'initiative politique et législative »

Les représentants britanniques ont évoqué les deux enquêtes françaises, souhaitant obtenir l'assurance qu'elles ne feraient pas obstacle à celle du Parlement européen. Vicieux, ils ont même proposé d'enquêter sur "*d'autres systèmes susceptibles de porter atteinte à la vie privée*", faisant incidemment référence à l'avatar français d'Echelon. Le lobbying forcené des Anglais contre toute investigation a, semble-t-il, été relayé par une intense activité américaine.

La commission, composée de 36 membres, dont quatre français (Hugues Martin, Catherine Lalumière, Alain Krivine et Georges Berthu) et dirigée par un eurodéputé portugais — Carlos Coehlo —, devrait rendre ses conclusions d'ici environ huit mois. Pour Thierry Jean-Pierre, qui sera le suppléant d'Hugues Martin au sein de cette commission, "*celle-ci aura beaucoup moins de pouvoirs qu'une commission d'enquête et pas de pouvoir de coercition : on invite, mais on ne peut forcer personne à venir témoigner.*"

Le FBI et le système CARNIVORE

Juillet 2000

Le projet de système de surveillance électronique nommé « carnivore » développé par le FBI repose sur la constatation du nombre croissant de délits via le réseau Internet.

Les moyens traditionnels d'investigation du FBI n'étant plus d'actualité, l'agence américaine a donc pris la décision (sous réserve d'acceptation de la justice américaine) de créer un logiciel de surveillance de la messagerie électronique.

Ce système, en liaison avec les fournisseurs d'accès à Internet – Internet Service Provider ISP – fonctionnera par l'analyse de mots clés et d'analyse textuelle (analyse de contenus sur des sujets précis) des mails envoyés par les internautes.

Les fournisseurs d'accès seront dans leur intégralité tenus d'apporter leur savoir faire et leur assistance au développement de cet outil pour sa mise en œuvre et son installation.

A priori, selon les termes mêmes du communiqué du FBI, le système ne sera pas abusif car il requiert une expertise importante à son installation et son exploitation, limitée dans le temps et ponctuelle , et controlé par la justice américaine.

Par ailleurs, le code source de cet outil de surveillance développé en 1997 ne sera pas dévoilé comme le réclamait l'Union Américaine des Libertés civiles -ACLU-

Ce logiciel fonctionne sous Windows 2000 et permet de scanner plusieurs millions de mails par seconde, les informations collectées étant triées par les agents fédéraux.

La NSA a directement collaboré dans le développement de ce logiciel. Il est issu d'un programme de transfert de technologie conclu entre la NSA et la département de la justice.

Selon le magazine du Monde du Renseignement, les fournisseurs d'accès comme Uunet et MCI Worldcom ont également « collaboré » et permis un renforcement du système par une section spécialisée du FBI, la CALEA Implementation Section.

C'est d'ailleurs après une rencontre avec la CALEA que le provider Earthlink aurait décidé de rompre le silence et dévoiler l'existence de Carnivore.

Actuellement Carnivore est installé chez une vingtaine de provider aux Etats Unis.

Carnivore est une sorte de super-sniffer capable de capturer des trames précises en

" temps réel ". Ce système sélectif d'écoute Internet n'a strictement rien à voir avec d'autres mécanismes ou architectures de surveillance tel Echelon qui, quant à eux, surveillent et analysent l'intégralité des " conversations " passant à leur portée.

Carnivore est, de l'avis même de certains experts et membre de l'Epic, probablement le mécanisme de flicage le moins " agressif " et le plus respectueux des libertés individuelles qui soit... puisque pouvant parfaitement constituer le système d'écoute

" chirurgicale " que peut utiliser et maîtriser un juge d'instruction. Reste que les possesseurs de Carnivore gardent jalousement les détails techniques de leur installation et, dans une certaine mesure, semblent souhaiter conserver leurs privilèges de poseurs de " micros sous IP "

Le 2 août 2000, l'association indépendante EPIC (The Electronic Privacy Information Center) www.epic.org/privacy/litigation/carnivore_TRO.pdf
a porté plainte contre le FBI pour violation des droits privés des américains.

WASHINGTON, DC -- The Electronic Privacy Information Center (EPIC) today asked a federal judge to order the immediate public disclosure of information concerning the Federal Bureau of Investigation's controversial "Carnivore" surveillance system. In an application submitted to U.S. District Judge James Robertson, EPIC charges that the Department of Justice and the FBI have violated the law by failing to act on a request to expedite the processing of a Freedom of Information Act request EPIC submitted to the FBI on July 12.

17 août 2000

Le FBI annonce la publication de documents concernant Carnivore

La publication d'une partie des 3000 pages de documentation concernant Carnivore, le système de surveillance électronique du FBI, pourrait intervenir sous 45 jours, selon Associated Press. Le plan proposé par le FBI (Federal Bureau of Investigation) prévoit ensuite une publication de documents supplémentaires àéchéance régulière, tous les 45 jours. A l'origine de cette démarche inhabituelle, la plainte déposée par l'association de protection des données personnelles EPIC (Electronic Privacy Information Center) contre le département àla Justice. L'EPIC demande que soient rendus publics les détails du fonctionnement du système Carnivore. Elle estimait jeudi que l'échéancier qui vient d'être proposé restait trop imprécis.

→ voir également les annexes.

La RIPP BILL – Big Browser au Royaume Uni

Juillet 2000

Cette loi - la Ripp Bill- votée le 28 juillet dernier et qui s'appliquera en automne, prévoit de mettre l'Internet anglais sous haute surveillance électronique. Dénommée « Big Browser » par ses opposants, ce système comparable à CARNIVORE développé par le FBI rencontre de nombreux obstacles.

Cette loi oblige à révéler aux internautes leurs mots de passe de leur clé de cryptographie, faisant d'eux des présumés coupables devant apporter la preuve de leur culpabilité…
Dernièrement, et bien que la loi soit passée, un ensemble d'association comme Amnesty International, Telecommunications Managers Association, L'union nationale des journalistes et la société des éditeurs, l'Internet Society, ou encore Duncan Campbell (le journaliste que a révélé l'existence d'Echelon) ont demandé l'abandon pur et simple de cette loi.

Plusieurs providers, Poptel, Claranet, Greennet, PsiNet, ont menacé de quitter l'Angleterre si ce projet venait à aboutir.

28 juillet 2000
La loi en question deviendra effective dès ratification par la Reine. Passé cette formalité, les fournisseurs d'accès devront filtrer et tracer *toutes* les données transitant par leurs centres de traitement, serveurs ou routeurs, et conserver les traces de routage desdits flux afin de les communiquer au *Government Technical Assistance Center* (GTAC).
En attendant, le projet soulève de véhémentes protestations précises The Standard <http://www.thestandard.com/article/display/0,1151,17179,00.html>. La loi pose des problèmes tant éthiques qu'économiques, puisque l'installation des "mouchards » semble loin d'être gratuite.

Du côté de la Hollande, c'est un autre système qui a été révélé par le journal « De Volkskrant ». Les services de l'intérieur scruteraient le réseau en recherchant les mots clés.

Microsoft et la NSA

Crypteurs sabotés !

Les sociétés commercialisant du matériel de cryptage ont été « retournées » par la NSA. Un classique , d'abord : la société suisse Crypto AG, qui fournissait militaires et diplomates de plusieurs pays a truqué son matériel de manière à ce que, imperceptiblement, lorsque chacune de ses machines envoyait un message codé, elle entamait son message par… le code, tout simplement.

Plus récemment la clef « NSAKey » dans le code de Microsoft ne permet pas de prendre le contrôle de Windows à distance. Cette clef sert à simplifier les modifications par une personne qui en a le droit sur la machine des cryptoAPI.
Le code concernant la NSAKey consiste à ajouter une autre clef (qui est détenue officiellement par Microsoft et officieusement par la NSA) qui a également le droit de signer les nouvelle DLL.
En tout état de cause, toutes les sociétés de logiciel US ont obligation légale de montrer leur code à la NSA qui a le droit de demander des modifications si elle le souhaite.

Un rapport interne du Ministère de la Défense (18 février 2000 . AFP) indique que la création de Microsoft a été largement encouragée par des aides financières de la NSA et que IBM s'est vu imposer le MS-DOS comme système d'exploitation par la même administration.
Le Pentagone souligne par ailleurs dans ce rapport qu'il est le premier utilisateur de Microsoft…

Le réseau Sigint français – le « Frenchelon »

Extraits du papier du Monde:

"La France, de son côté, n'est pas démunie de moyens de renseignement en la matière. Ses services spéciaux, à commencer par des annexes de la Direction générale de la sécurité extérieure (DGSE), ont été souvent soupçonnés, eux aussi, de piller les secrets commerciaux des alliés. La DGSE dispose, en particulier, d'un organe de surveillance et d'interception, le Groupement des contrôles radio-électriques (GCR), qui exploite un certain nombre de stations d'écoute en métropole, dans les DOM-TOM et dans le monde. Ces moyens d'interception, satellitaires ou autres, sont déployés à Alluets-Feucherolles (Yvelines), Agde (Hérault), Domme (Dordogne), Mutzig (Bas-Rhin) et Solenzara (Corse-du-Sud), à Saint-Barthélemy (dans les Antilles), à la Réunion, à Djibouti et à Mayotte (en océan Indien). Après avoir désarmé le Berry en mai 1999 , la DGSE aura d'autre part, en 2001, un navire de recherches électromagnétiques, le Bougainville, armé par la marine et en cours d'aménagement, pour intercepter les émissions stratégiques, civiles et militaires d'un pays près duquel il croise.
"Face à des interlocuteurs imprudents ou indiscrets lors de négociations internationales, les intrusions dont le GCR est rendu responsable n'ont ni la pertinence, ni l'acuité, ni les performances des interceptions attribuées au réseau Echelon et, singulièrement, au GCHQ britannique, dont les capacités - quasi planétaires - de déchiffrage des transmissions de toutes natures, avec l'assistance des Etats-Unis, sont très supérieures."

En juin dernier, la NACIC (1) (National Counter Intelligence Center), organisme qui coordonne les efforts du gouvernement américain pour identifier et contrer les menaces en provenance des services étrangers sur la sécurité nationale et économique du pays, publie sur son site Internet, www.nacic.gov, un article dénonçant les pratiques d'espionnage de la France.
Selon cet article, la CIND (Computing, Information and Netwoking Division), un laboratoire de recherche en webtechnologies de l'ORNL (Oak Ridge National Laboratory), aurait constaté que la France pratiquait couramment la surveillance des téléphones et des réseaux câblés des entreprises basées aux Etats-unis et dans d'autres pays.
Le NACIC précise que le Sunday times dans un récent article a révelé que les services français intercepteraient, grâce à huit centres d'écoute, les conversations téléphoniques des dirigeants d'entreprises tels que ceux de British Airways, British Aerospace, British Petrolum, selon « un informateur français non-identifié ».

(Info ou intox ? le webmaster travaille pour la CIA…)

N'oublions pas que le programme français

Helios <http://www.tbs-satellite.com/tse/online/prog_helios.html>,

un réseau de satellites "d'observation" qui a la tâche officielle de prendre des photos minutieuses de la planète (coopération France Espagne Italie). Helios-1B a été lancé le 6 décembre dernier.

A bord du premier engin lancé dans l'espace en 1995, Helios-1A, un petit boitier d'écoutes électroniques a été ajouté au dispositif. Il s'agirait d'un relais d'un réseau d'écoutes sur lequel s'est greffé l'Allemagne, qui surveille des signaux radio - y compris ceux de ses plus proches alliés - avec la même dexterité.

Le programme a ensuite été rebaptisé "Cerise »
http://www.tbssatellite.com/tse/online/sat_cerise.html

C'est *Le Point* et Jean Guisnel qui ont déjà remis la France à sa place en juin 1998 en dévoilant ce qu'un titre américain a appelé le "Frenchelon" (Ken Cukier, Communications Week). Le mois suivant, la Défense réagissait et reconnaissait l'existence de ce réseau d'écoute de type "comint".

.Version reprise par The Tocqueville Connection:

/www.adetocqueville.com/archive/o980710b.htm

> "La DGSE gère pour sa part un important centre d'écoutes basé à Domme (Dordogne), et vient d'ouvrir deux nouvelles stations, l'une aux Emirats arabes unis, et l'autre en Nouvelle Calédonie. Surtout, en liaison avec les Allemands du BND (Bundesnachrichtendienst), les Français ont implanté une station d'écoutes sur la base spatiale de Kourou (Guyane française), qui peut intercepter les satellites évoluant au-dessus de l'Amérique. L'un des responsables de ces systèmes, a confié au Point qu'il serait inutile d'en vouloir aux américains : "C'est le jeu de la guerre secrète, à nous de faire comme eux et d'être aussi performants. C'est 'je te tiens, tu me tiens par la barbichette !' Il serait malvenu de s'en offusquer !"
>
> "Alors que les responsables du ministère français de la Défense, dont dépend la DGSE, avaient refusé de répondre aux questions du Point durant son enquête, ils ont été plus explicites après sa parution. Dans une démarche très inhabituelle, pour tous les services de renseignement du monde, le directeur de cabinet du ministre français de la Défense, François Roussely, a en effet confirmé l'existence de ce réseau d'interception national.
>
> "Et de préciser, dans Le Point du 20 juin dernier, que les systèmes français d'écoute sont "destinés au suivi des crises internationales, dans leurs dimensions militaires, notamment dans les zones où les forces françaises peuvent être engagées, à la surveillance du phénomène de prolifération des armes non conventionnelles, à la lutte contre le terrorisme. Du fait du caractère transnational de ces menaces, le recueil d'informations nécessite parfois des moyens qui dépassent les possibilités propres de chaque Etat. Cela implique pour la France de rechercher avec ses partenaires les solutions, notamment techniques, aptes à la prémunir contre ces dangers."

Echelon, c'est aussi à la maison...

Vous pensez que votre femme vous trompe et qu'elle joue à la cyberdrague... Pour vérifier, rien de plus simple: les logiciels «espions», d'abord destinés à surveiller la navigation des enfants, sont là pour vous.
«WinWhatWhere Investigator <http://www.winwhatwhere.com/> rapporte silencieusement toutes les activités d'un ordinateur», «KeyKey <http://www.pc-spy.com/software/> est à votre ordinateur ce qu'une boîte noire est à un avion!», «Keystroke Monitor <http://www.internet-monitoring-software.com/> enregistre chaque touche enfoncée», «Enregistrez secrètement tout ce que font votre femme, vos enfants ou vos employés en ligne avec Spector ou eBlaster <http://www.spectorsoft.com/>!»...

Il en existe des dizaines, des logiciels comme ceux-là, qui, pour quelques dizaines de dollars, vous permettent d'enregistrer toutes les activités informatiques de vos proches.
Spector, par exemple, effectue des captures d'écran toutes les 30 secondes et vous les délivrera tout en restant très discret et invisible dans la barre des tâches. EBlaster, lui, vous envoie même, sur le lieu de votre travail, des comptes-rendus réguliers des activités de votre ordinateur, en se comportant finalement comme un petit Echelon domestique, à base de mots-clés jugés tendancieux.
Au départ prévus pour surveiller la navigation des enfants, ces logiciels ont vite dérivé vers un espionnage conjugal ou professionnel, pouvant aller jusqu'au divorce!

Sur le site de la compagnie qui vend Spector, par exemple, des témoignages d'utilisateurs expliquent comment ils ont «démasqué» leur conjoint. Une californienne remercie Spector de lui avoir permis, moins de 24 heures après l'installation, d'avoir la preuve que son mari la trompait. «C'était beaucoup plus efficace et moins cher que d'employer un détective privé!»

Le *Washington Post* relate l'histoire d'un couple qui a fini par divorcer parce que la femme avait des discussions plus ou moins osées sur des ch@ts privés. La technique, après avoir offert la liberté, permet aujourd'hui de limiter cette liberté. Evidemment, les espions sont très heureux de leur jouet, ou arme, devrait-on dire. Mais, les espionnés ne le voient pas du même œil. Et la question de la liberté d'agir et de penser se retrouve une nouvelle fois mise en question.

Lewis Z. Koch, auteur d'un livre sur les thérapies de couple, explique <http://www.zdnet.com/intweek/stories/columns/0,4164,2611609,00.html> dans *ZDNet* que même les enfants ne devraient pas être surveillés de la sorte. Espionner un enfant sans qu'il le sache n'instaure pas le climat de confiance nécessaire. «Un enfant continuera à surfer sur les sites interdits. Faire confiance aux enfants, c'est avoir le courage de leur dire qu'on a peur pour eux».

Les relations conjugales sont fondées sur la même confiance. Acheter Spector, c'est déjà soupçonner la trahison, c'est déjà constater la séparation. Et que se passe-t-il si les deux conjoints ont la même idée d'installer le logiciel et se rendent compte tous deux de cette méfiance assistée par Internet?
Ces logiciels semblent pour l'instant être légaux et n'entrent pas dans le cadre de la loi contre les crimes informatiques au Canada ou en France. L'interception de données informatiques par un tiers est interdite et susceptible d'être pénalisée. Mais visiter son propre ordinateur, utilisé par les autres membres de la famille n'est pas considéré comme une intrusion illégale.
Aux Etats-Unis, on a pensé rapprocher ce genre de logiciels de ceux des écoutes téléphoniques, interdits par la loi sauf sur autorisation du juge. Pourtant, il est difficile aujourd'hui de les considérer comme tels. Un juge dans le Maryland, il y a cinq ans, a considéré le document présenté par l'avocat de son client, et «volé» grâce à un logiciel d'enregistrement du clavier, comme valable.
Spector n'est pas encore considéré aussi dangereux pour la liberté individuelle que les écoutes téléphoniques. Attendons que l'ordinateur soit devenu aussi courant que le téléphone!

En conclusion…

Le contrôle des moyens de communications relève d'une stratégie délibérée orchestrée par Washington, qui se montre résolu à promouvoir le commerce électronique et joue de la liberté des échanges d'informations.
La diplomatie d'avenir sera celle des réseaux, avec pour « dégâts collatéraux » la déconstruction des états nations.
Il faudra bien, avertit Joël de Rosnay, que les Etats prennent conscience des risques que la révolution de la communication fait peser sur les libertés fondamentales.

L'autonomie d'un être, partie prenante de l'autonomie d'une nation c'est, rappelait Cornelius Castoriadis, l'interrogation illimitée.
Pourrons nous encore exister en tant que citoyens d'une société autonome ?
Le doute nous prend quant à la capacité des réseaux à servir la démocratie…

Pour conclure, un extrait d'interview(02/08/2000) de Nicky Hager, auteur du livre « Secret Power… «

"The lesson is this: information that challenges the status quo does not threaten or greatly concern the powerful as long as it is restricted to relatively few people. As long as 'dangerous' information is only disseminated in small-circulation publications or books - unconfirmed and unacknowledged by the authorities - it is manageable and has little practical effect"

« My conclusion is that where freedom of information laws are inadequate (and on intelligence they always are), one of the most powerful democratic safeguards is leaking: where public-spirited individuals inside government and corporate organisations are encouraged to release important information to journalists or politicians. This should not need to be how we have to obtain important information, but for now it is often the only option. "

Liens utiles – Adresses URL

Le site de Duncan Campbell : www.gn.apc.org/duncan

Intelligence Online report on UKUSA cooperation:
http://www.blythe.org/Intelligence/readme/brits-usa.int45

Nicky Hager, *Covert Action Quarterly* article on ECHELON: http://jya.com/echelon.htm

European Parliament, STOA report, *Assessment of the Technologies of Political Control*:
http://jya.com/stoa-atpc.htm

The UKUSA Community and SIGINT
http://watserv1.uwaterloo.ca/~brobinso/cseukusa.html

The National Security Agency Web site: http://www.nsa.gov:8080

NSA's budgets and mission http://www.ccic.gov/pubs/imp97/98.html

Origins of the NSA http://www.awpi.com/IntelWeb/US/NSA/charter.html

<http://www.europarl.eu.int/dg4/stoa/fr/publi/166499/execsum.htm>
Le texte (version courte) du rapport commandé par le Parlement européen au sujet des technologies de contrôle politique et qui aborde le problème du réseau Echelon.
<http://www.indigo-net.com/lmr.html>
Le site de la lettre confidentielle "Le monde du renseignement". Très bien informé sur l'actualité des services secrets en France et dans le monde. (payant)

<http://cag.com>
Le site du magazine Covert Action Quarterly. Se penche sur l'actualité du renseignement et les débats qui agitent les services secrets. Très complet. Ce site propose des extraits du livre de Nicky Hager qui décrit le fonctionnement du réseau Echelon : "Secret power"

<http://www.gn.apc.org/cndyorks/mhs/index.htm>
Le site des adversaires de la base de Menwith Hill. Présente l'historique précis de la lutte engagée pour faire la lumière sur les activités de la plus grande station d'espionnage du monde. Une mine d'informations.

<http://www.networx.com.au/home/slider/Pine-Gap.htm>
Le site des opposants à la base jumelle de Menwith Hill à Pine Gap en Australie.

http://www.icdc.com/~paulwolf/echelon.htm
<http://www.icdc.com/%7Epaulwolf/echelon.htm>
Paul Wolf tient à jour sur son site une liste très complète des articles de la presse internationale (anglophone) consacrés à Echelon.

http://www.qainfo.se/~lb/echelon.htm <http://www.qainfo.se/%7Elb/echelon.htm>
Ce site suédois propose lui aussi une liste d'articles consacrés à Echelon.

<http://www.privacy.org/>
Le site très complet de l'organisation Privacy International qui dénonce les atteintes à la vie privée commises par le réseau Echelon.

<http://www.sni.net/menwith/>
Le site des anciens de la NSA qui ont servi à Menwith Hill dans les années 60. Souvenirs du bon vieux temps…

ANNEXES

- « Interception Capabilities 2000 « Dossier remis au parlement européen par Duncan Campbell
- Archives déclassifiées de la NSA
- Echelon et ses réalités par Duncan Campbell
- Interview par RFI de Duncan Campbell
- Mainmise de British Telecom
- Interview de Nicky Hager – Auteur de « Secret Power »
- L'œil de Moscou sur le Net
- Espionnage : La NSA concurrence Google
- Le FBI veut son Echelon à lui
- « Paddies join global spy network » : Participation de l'Irlande au système Echelon
- Le NRO – National Reconnaissance Office