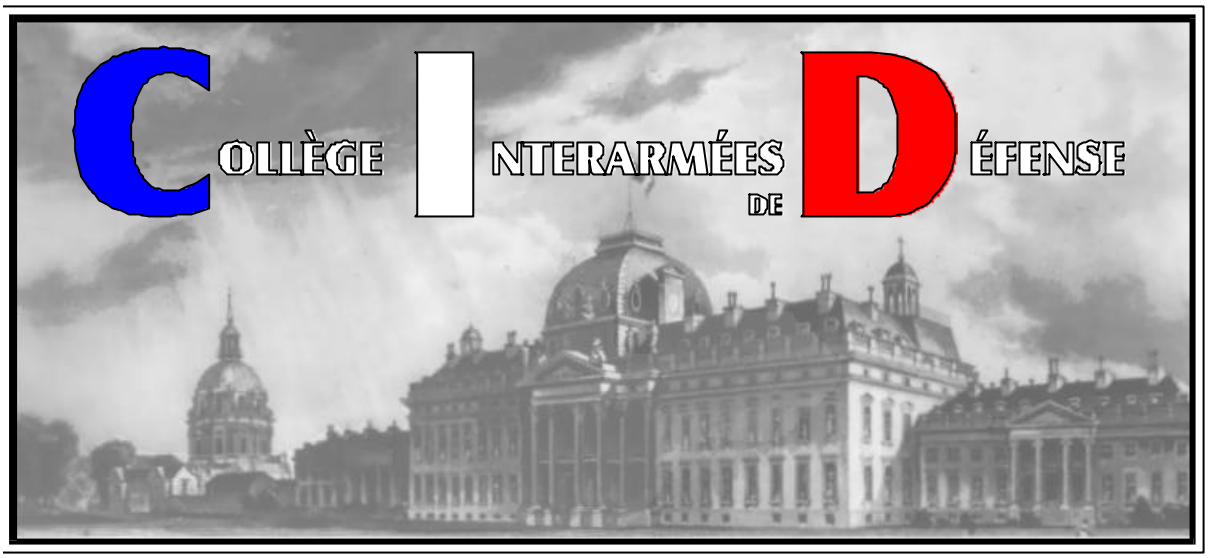
FICHE DE PRESENTATION

1. Le renseignement dans la stratégie des Etats-Unis : le « big brother » vis à vis de l'U.E.
2. CF Pier Federico BISCONTI, Marine Italienne
3. 15 Mars 2000
4. Division D
5. Mémoire de stratégie
6. Les Etats-Unis et quatre de leurs alliés privilégiés ont déployé depuis quarante ans un gigantesque réseau d'écoute électronique capable d'intercepter les télécommunications du monde entier. Depuis la fin de la guerre froide, ce dispositif ultra secret, connu sous le nom d'Echelon, est de plus en plus utilisé pour des opérations d'espionnage économique.

   Ce danger a été bien compris par le Parlement européen qui a récemment commandité une étude pour évaluer les technologies de contrôle politique, en particulier celles de surveillance électronique.

   George Orwell avait-il raison ? Ne sommes nous pas tous sous contrôle de « big brother » ? Les Européens peuvent-ils s'affranchir de cela ?
7. Mots clés : Echelon, Big Brother, renseignement, NSA, UkUsa



Le renseignement dans la stratégie des Etats-Unis : le « big brother » vis à vis de l'U.E.

Mémoire de Stratégie

Rédigé par le

Capitaine de Frégate **Pier Federico BISCONTI**

TABLES DES MATIERES

Introduction

Nous vivons à l'age de l'information. Elle est « mondialisée, globale, surabondante et numérisée (cf. Amiral Pierre LACOSTE) ». Les Etats-Unis ont bien compris que le monde « cybernétique » offre une foule de nouvelles opportunités.

Dans ce mémoire nous essaierons d'identifier l'importance des renseignements dans la stratégie des Etats-Unis vis a vis de l'UE (Union Européen).

Dans une première partie nous traiterons brièvement l'histoire du renseignement américain à partir de la Guerre du Golfe. Nous verrons ensuite la doctrine «intelligence » américaine et les liens avec le monde économique et enfin nous parlerons de la montée en puissance du renseignement économique vis à vis de l'UE et les démarches européennes pour s'opposer au « big brother ».

L'idée centrale de ce mémoire est que « les moyens modernes permettent de recueillir et de transmettre en temps réel des informations qui fournissent une connaissance parfaite du théâtre des opérations et éliminent donc l'une des composantes fondamentales de la stratégie traditionnelle : l'incertitude (Hervé Coutau-Bégarry) [i]».

Ce concept, bien compris par les Anglo-saxons, a été proposé a l'issue de la guerre au Kosovo : celui qui maîtrise l'information sait désormais quoi et où frapper.

Les Etats-Unis et quatre de leurs alliés privilégiés ont déployé depuis quarante ans un gigantesque réseau d'écoute électronique capable d'intercepter les télécommunications du monde entier. Depuis la fin de la guerre froide, ce dispositif ultra secret, connu sous le nom d'Echelon, est de plus en plus utilisé pour des opérations d'espionnage économique.

Ce danger a été bien compris par le Parlement européen qui a récemment commandité une étude pour évaluer les technologies de contrôle politique, en particulier celles de surveillance électronique.

George Orwell avait-il raison ? ne sommes nous pas tous sous contrôle de « big brother » ? Les Européens peuvent-ils s'affranchir de cela ?

1. Le renseignement aux Etats Unis

a. La doctrine

Selon la doctrine interarmées des Etats Unis, l'Intelligence est l'outil de renseignement et connaissance d'un adversaire, obtenu avec l'observation, l'investigation et l'analyse[ii].

Le "cycle intelligence" permet de transformer les informations en un produit fini, disponible pour l'utilisateur final et se développe en cinq phases (Figure 1) :

(1) la planification et la direction, avec la détermination du plan de recherche et la conduite des opérations;
(2) la recherche de renseignements;
(3) la valorisation, obtenue avec l'analyse et l'expérience;
(4) la production, de documents facilement employables par l'utilisateur;
(5) la diffusion aux utilisateurs qui ont la nécessité de savoir.

Comme on peut bien imaginer, les opérations de recherche des renseignements à des fins d'espionnage sont particulièrement importantes, même si souvent elles sont effectuées en dehors de la légalité.

Figure 1 : le « cycle intelligence »

On peut diviser ces opérations en cinq catégories, selon les sources ou le moyens employés: Humint (Human Intelligence), avec l'utilisation d'espions et des indicateurs, Imint (Imagery intelligence), avec l'étude des images, Masint (Measurement and Signature Intelligence), c'est à dire la mésure et l'étude des signaux, Osint (Open Source Intelligence), élaboration des données provenantes des sources ouvertes et, enfin, Sigint (Signal Intelligence).

Dans ce cas particulier, il s'agit d'une récolte de signaux electro-magnétiques émis intentionnellement par les Gouvernements ou les organisations dont on veut voler les secrets. Le Sigint se partage en Elint (Electronic Intelligence), interception d'émissions de non-communications (radar etc.) et Comint (Communication Intelligence) qui recueille, et éventuellement dechiffre, et analyse les signaux des communications (radio, téléphones etc.).

Les cibles du Comint sont devenues, à partir des années 60, outre les communications militaires et diplomatiques, celles commerciales et financières et celles liées au terrorisme, à la criminalité, aux trafics de drogue et d'armes et au blanchiment de l'argent.

Avec le developpement des télécommunications et de la télématique, ces activités sont devenues de plus en plus importantes.

b. La National Security Agency

Dans la communauté du renseignement américain, les opérations de collecte des renseignements sont confiées à la National Security Agency (NSA), la plus puissante structure « *Intelligence* » du monde.

Crée en 1952, cette agence est chargée de l'espionnage des télécommunications et de la mise au point des systèmes de codage et de cryptage destinés à garantir la confidentialité des messages envoyés par le gouvernement, les diplomates et les militaires américains (Figure 2).

Mais la NSA se doit de rester discrète, voire invisible. Pourtant, son budget est supérieur à celui de la CIA (*Central Intelligence Agency*). Elle coûte, selon certaines estimations, entre 4 et 6 milliards de dollars par an aux contribuables américains.

Figure 2 : La siège de la NSA à Fort Meade

A Fort Meade, à mi-chemin entre Washington et Baltimore, le quartier général de la NSA est à peine moins vaste que le Pentagone.

Environ 20.000 personnes y travaillent tandis que plusieurs milliers d'autres opèrent à partir des sites d'interception disséminés à travers la planète. Derrière les vitres miroir des bureaux, on s'active pour décoder, traduire, et analyser les messages captés par les satellites espions ou les installations au sol.

On trouve ici la plus forte concentration de mathématiciens de haut niveau au mètre carré. La NSA embauche chaque année entre 40 et 60 docteurs en mathématiques et elle multiplie les appels du pied en direction des étudiants américains de cette discipline pour qu'ils rejoignent ses rangs. Et l'agence a de quoi les attirer. Outre qu'elle leur propose de "participer à la défense des Etats-Unis", elle dispose de l'un des plus grands parcs de Superordinateurs : les fameux Cray qui font rêver tous les scientifiques de la planète pour leur phénoménale puissance de calcul. Mais pour entrer à la NSA, les candidats doivent accepter de signer un engagement formel : tout, absolument tout, de leurs activités devra rester secret, ils ne seront pas autorisés à en parler même une fois qu'ils auront atteint l'âge de la retraite.

c. De la Guerre du Golfe à nos jours

Les opérations menées par les Alliés durant la guerre du Golfe ont confirmé l'importance de disposer d'une structure de renseignement efficace et fiable et représentent pour les communautés de renseignement une étape fondamentale de leur histoire.

Jusqu'au déclenchement des opérations, tous les systèmes de recherche étaient conçus pour contraster une éventuelle menace d'invasion soviétique de l'Europe et les moyens disponibles étaient seulement de niveau stratégique. Très tôt ces types de renseignements se sont montrés insuffisants pour conduire une campagne aérienne

limitée dans l'espace mais à laquelle était demandée une précision sans précédent dans l'histoire des frappes aériennes et avec le souci fondamental de réduire au minimum les pertes humaines.

Il fallait donc disposer de moyens aptes à surveiller un champ de bataille, à tenir l'ennemi sous contrôle constant, à évaluer les données en temps réel. Les renseignements, donc, devaient passer du niveau stratégique au niveau opératif et, dans certains cas, ils devaient descendre jusqu'au niveau tactique.

Les Américains ont bien compris cela et ont reconfiguré leurs moyens et leurs doctrines, pour fournir aux combattants un outil performant et gagnant.[1]

Après la Guerre du Golfe, avec la fin de la guerre froide, les services de renseignement ont dû revoir leurs priorités. En tête de la liste des personnalités à écouter, la nomenklatura russe a laissé la place aux hommes forts du Moyen-Orient et des Balkans, aux groupes terroristes, aux trafiquants de drogue et aux hommes d'affaires européens ou japonais.

Les cibles ont changé mais l'objectif reste le même : fournir le maximum d'informations précises à l'administration américaine. Et elle n'a pas à s'en plaindre si l'on en croit le prédécesseur de Bill Clinton. Avant de passer le relais, George Bush a tenu à rendre hommage aux hommes de la NSA. Aux commandes de la Maison Blanche au moment de la chute du mur de Berlin, de l'invasion du Koweït puis de la guerre du Golfe, il a souligné publiquement ce jour là que « *les écoutes sont un facteur essentiel dans les décisions de politique internationale* ».

d. La révolution dans les affaires militaires (RMA)

Selon plusieurs analystes, les innovations techniques sont toujours à la base des transformations dans la manière de faire la guerre. Cette vision, appelée *Military Technical Revolution* (MTR), dénote le phénomène selon lequel les extrêmes transformations dans la guerre seraient le résultat de l'exploitation de la technologie pour obtenir des innovations dans le domaine opérationnel et de l'organisation. En bref, la MTR est un évent technologique qui modifie le cours de l'histoire militaire.

Une illustration claire des MTR qui se sont produites depuis le quatorzième siècle est fourni par Krepinevich[iii]:

- La révolution de l'infanterie, pendant la quelle les fantassins ont obtenu un rôle dominant sur la cavalerie ;
- La révolution de l'artillerie ;
- La révolution des forteresses, où apparurent des fortifications adaptées à l'artillerie ;
- La révolution de la poudre à canon, avec le développement des armes pour les fantassins ;
- La révolution napoléonienne, dans le domaine de la logistique et de l'organisation ;
- La révolution terrestre, en raison de puissance de feu, transports et communications ;
- La révolution navale du vapeur, de l'acier et des sous-marins ;
- La révolution du moyen aérien ;

[1] "Le succès de n'importe quel déploiement en cas de crise repose sur l'existence d'un system fiable de command et contrôle et sur un système de recueil, d'analyse et de diffusion des renseignements tactiques et stratégiques sûr et souple" – Général Norman SCHWARZKOPF, USA, USCINCENT, Opération DESERT STORM 1991

- La révolution Nucléaire.

Néanmoins, donner une puissance déterminante aux innovations technologiques semble être plutôt simpliste. Les innovations technologiques sont seulement l'un des processus dans lequel l'art de conduire la guerre évolue. La technologie ne peut pas révolutionner une entreprise (militaire ou non) qu'après avoir été reconnue, développée et, enfin, adoptée. Par exemple, l'emploi de l'artillerie a eu lieu en Europe à partir du XIV siècle, bien après l'invention de la poudre à canon (950 après J.C. environ) et dans un lieu complètement différent de celui où elle avait été inventé (la Chine).

Aujourd'hui les militaires n'attendent plus les innovations technologiques mais sont à même de les proposer. Dans le XX siècle la claire (mais non décisive) relation entre la maîtrise technologique et la supériorité militaire a rendu l'innovation technologique un point clé de la planification et des dépenses militaires. A partir de cela, on peut donc envisager la MTR actuelle : la révolution des affaires militaires.

Ce concept n'est pas nouveau. On parlait déjà de « révolution militaire » durant la deuxième guerre mondiale. Sur le théâtre européen, les Allemands, les Français et les Britanniques disposaient des mêmes atouts de départ : expérience de la première guerre mondiale, connaissance des armes nouvelles qu'étaient avant tout l'avion et le char d'assaut. Seuls pourtant les Allemands furent à même d'exploiter ces technologies pour produire à leur avantage un bouleversement de l'art militaire. Ce bouleversement a consisté à inventer et mettre en œuvre les concepts opérationnels et les modes d'organisation les mieux à même de donner à ces armes leur plus grande efficacité militaire[iv].

Cependant le concept n'est adopté en tant que tel et ne devient un élément structurant du débat stratégique qu'après la guerre du Golfe. En effet le conflit du Moyen-Orient a illustré les possibilités des armes nouvelles développées dans le cadre de la doctrine *Airlandbattle*, au moment où, paradoxalement, avec la chute du mur de Berlin, s'effondraient le contexte international et le problème militaire pour lequel elles avaient été conçues.

De manière schématique, ce nouveau contexte peut être, partiellement, caractérisé par les paramètres suivants :

- disparition de l'ennemi désigné et profonde incertitude sur la nature de la menace à long terme ;
- rareté relative de la ressource budgétaire, affectée de préférence à la priorité économique et sociale ;
- évolution marquée dans un certain nombre de secteurs technologiques, notamment l'électronique, l'informatique, les télécommunications, affectant le vaste domaine de l'information, à l'impact probable mais encore difficile à évaluer précisément sur la forme générale des opérations militaires.

L'école de la RMA s'est répandue à partir des ouvrages des Töfflers[2], mais aussi de la réflexion d'un petit nombre de spécialistes groupés autour du *Strategic Studies Institute* du *Army war College* à Carlisle Barracks.

[2] TÖFFLER, Alvin & Heidi, produisent, depuis les années 70, des ouvrages de prospective, qui n'auraient guère d'importance si, depuis 1993, leur pensée n'était devenue partie intégrante de la pensée ordinaire du Pentagone. La "guerre de l'information" surgit, de l'irruption de l'électronique, comme révolution technologique, introduisant la troisième des "révolutions dans les affaires militaires" d'importance macro-historique (1. : La révolution agraire circa 4000 av. J.-C. ; 2. : la révolution industrielle circa 1800 ; 3 la révolution électronique circa 1970-2000). L'expansion de ce concept dans la littérature de Défense depuis 1993 accompagne le succès de leur dernier ouvrage, *War and antiwar.*

En avril 1994, la RMA est au centre d'un colloque comme un concept faisant l'objet d'un consensus interarmées, selon lequel on quitterait le paradigme du combat (*warfighting*) de la guerre de manœuvre, auquel se rattache encore la guerre du Golfe, pour un paradigme de la guerre de la connaissance (*knowledge warfare*) ou de l'information (*Information War*). Le concept de la RMA s'est depuis banalisé. Il signifie tout : la recherche de l'application des innovations technologiques aux inventions militaires ; la dérive de la pensée stratégique vers la guerre virtuelle et le cyberespace ; la recherche d'armes non létale destinées à maintenir l'ordre sans grandes tueries.

2. Le renseignement dans le contexte de la géostratégie américaine

a. La politique de l'administration Clinton

A la fin de la guerre froide les Etats Unis ont revu leur politique de sécurité. Les priorités américaines dans ce domaine peuvent être ainsi schématisées[v] :

(1) Jamais une autre superpuissance ne devra exercer une menace vitale similaire à celle que les armes nucléaires soviétiques ont posé pendant les dernières décennies aux Etats Unis ;
(2) Jamais les Etats Unis ne devront être engagés contre leur volonté dans un conflit mondial comme s'est passé, par la faute des Européens, deux fois dans ce siècle ;
(3) Le multilatéralisme n'est plus acceptable : l'ONU et les autres organisations internationales ne doivent plus échapper au contrôle des Etats Unis et ne doivent pas imposer quelque soit décision contraire aux intérêts nationaux ;
(4) Le modèle de la société, fondée sur le marché, la libre entreprise et la mondialisation, implique la défense et la promotion des intérêts économiques publics et particuliers américains dans le monde entier. La priorité stratégique passe donc du domaine militaire au domaine économique.

Le rôle des agences de renseignement américaines repose, donc, sur ces concepts.

La promotion des intérêts économiques américains a été codifiée sur la sécurité économique. Un de points clés de cette doctrine est la consolidation et l'augmentation de l'avance stratégique américaine dans le domaine des hautes technologies, civiles et militaires, avec, entre d'outre, une agressive politique commerciale d'exportation.

Pour cette raison a été crée le National Economic Council (NEC) pour coordonner les efforts de tous les ministères impliqués et donner des conseils au Président dans ces domaines. La politique d'exportation est suivie par un office du Département du Commerce, appelé, ceci n'est pas un hasard, *war room*.

Le Président Clinton a toujours poursuivi cette politique, bien convaincu de l'importance du pouvoir économique plus que du pouvoir des armes.

Dans un document de la Maison Blanche de 1994, le Président a clairement affirmé ce que son administration s'attendait par les services de renseignement en termes de protection et de poursuite des intérêts économiques des Etats Unis : « *Pour mieux prévoir les dangers futurs pour la démocratie et pour les intérêts économiques des Etats Unis, la communauté des renseignements doit tracer les lignes politiques, économiques, sociales et militaires de développement dans ces endroits où les intérêts des Etats Unis sont plus entraînés et où la récolte de renseignements par de sources ouvertes n'est pas adaptée* »[vi].

De plus, le Président Clinton a montré sa volonté de combattre toute menace économique de son pays en signant l'*Economic Espionage Act*. Il s'agit d'une loi qui protège le monde économique de toutes les formes d'espionnage provenant soit d'une nation étrangère soit d'une compagnie nationale ou étrangère. Dans son discours sur l'*Act*, le Président a affirmé : « l'espionnage économique et le vol de secrets commerciaux menacent la sécurité nationale et l'aisance économique ».[vii]

Cohérente à sa stratégie, le Président Clinton a réaffirmé son diktat dans un document de la Maison Blanche sur la Stratégie nationale dans le nouveau millénaire[viii] : « *Nos intérêts nationaux doivent rester clairs… Le premier regarde les intérêts vitaux, c'est à dire la sécurité du territoire et des citoyens et le bien-être économique de notre Nation. Nous ferons tout ce que nous pourrions pour défendre*

ces intérêts, en utilisant tous les moyens, même la force militaire » ; « *Un certain nombre d'Etats ont les capacités de menacer nos intérêts nationaux avec la coercition ou l'agression…* » et encore « *La menace d'espionnage par les services de renseignements étrangers est plus diversifiée et complexe que jamais, dans un mélange d'adversaires traditionnels et non-traditionnels, qui ont comme cibles les secrets militaires, diplomatiques, technologiques, économiques et commerciaux des Etats Unis* ».

Lors de son récent discours sur l'état de l'Union, enfin, M. Clinton a indiqué les lignes à suivre pour le nouveau millénaire, notamment sur la globalisation et la mondialisation du commerce, envisageant pour son Pays un rôle de « *centre de tous réseaux vitaux, comme un bon voisin et un bon partenaire* »[ix]. Dans le même document le Président envisage une étroite coopération entre les industriels américains de « *hi tec* », pour garder le monopole américain dans ce domaine hautement stratégique.

b. UkUsa

L'espionnage et le contre-espionnage électronique sont donc envisagés comme les moyens les plus « politiquement corrects » pour surveiller les concurrents économiques, thèse soutenue par l'ancien conseiller pour la sécurité nationale Brzezinski[x]. Quels sont donc les rapports entre les Etats Unis et l'Europe dans le domaine de l'espionnage électronique ?

Depuis quelques années la presse et quelques Organisations non-Gouvernementales (ONG) s'occupent du sujet, en affirmant que les Etats Unis et quatre leurs alliés auraient créé un système d'écoute globale de toutes les communications, appelé ECHELON.

Figure 3 : l'organisation UkUsa

L'origine historique de cette «infrastructure» remonte à 1947, époque de la guerre froide, où un accord UkUsa fut signé, avec comme objectif le renseignement militaire. La fin de la guerre froide a entraîné une mutation de cet objectif.

L'espionnage économique et politique est devenu la raison d'être de l'accord, qui vise aujourd'hui essentiellement des cibles non militaires : des gouvernements, des organisations et des entreprises. Les informations issues de ce système sont à la disposition des organismes de renseignements des cinq Etats signataires, soit, outre la NSA américaine le GCHQ (Government Communications Headquarters) du Royaume Unie, le CSE (Communications Security Establishment) canadien, le DSD (Defence Signals Directorate) australien et le GCSB (Government Communications Security Bureau) de la Nouvelle Zélande. (Figure 3).

L'existence de UkUsa a été récemment indirectement confirmée (mars 1999) par un fax envoyé par un dirigent du « *Defense Signal Directorate* », le service de renseignement australien, à un reporter du *Australian Sunday*, dans le quel est

clairement indiqué que le DSD travaille avec les autres services alliés dans le cadre de l'alliance (Figure 4).

Les partenaires de UkUsa dépendent strictement des Etats Unis pour ce qui concerne la haute technologie et, probablement, pour quelque aspect financier. Les rapports de force à l'intérieur de UkUsa sont bien étroits et les bases d'écoute, réparties géographiquement parmi les nations signataires, sont de souvent partagées avec les spécialistes américains.

Selon quelques auteurs[xi], la DSD écouterait les communications dans l'Océan Indien oriental, une partie du sud-est asiatique et le Pacifique occidental, le GCHQ écouterait l'Afrique et l'ancienne Union Soviétique jusqu'aux monts Ourals, le CSE s'occuperait du nord de l'ancienne Union Soviétique et de l'Europe, le GCSB d'une petite partie du sud Pacifique et la NSA, avec d'autres agences alliées, de tout le reste du monde.

Il existerait aussi d'autres « troisièmes parties » signataires, comme la Chine, qui, même si elles n'ont pas le droit de recevoir systématiquement les renseignements, auraient accepté d'installer des bases d'écoute sur leurs territoires. La NSA gérerait deux bases d'espionnage dans le Sin-Kiang (à Chi Tai et Korla)[xii] pour surveiller les communications et les expériences balistiques russes.


DEFENCE SIGNALS DIRECTORATE

Figure 4 : fax qui confirme l'existence de l'organisation UkUsa

UkUsa a donc une capacité de renseignement presque totale qui se sert d'un réseau d'écoute à haute technologie dans le monde entier et des bâtiments, des avions et surtout des satellites militaires américains.

c. ECHELON

Même si les Nations concernés n'ont jamais confirmé l'existence d'Echelon, plusieurs indications montrent la véridicité des rumeurs, notamment les déclarations d'un ancien agent des renseignements néo-zélandais, Nick Hager, qui dans son livre[xiii] dépeint le fonctionnement d'Echelon[3].

[3] Hager a interrogé plus de 50 personnes travaillant dans le renseignement pour découvrir un système de surveillance qui s'étend au monde entier pour former un système pointé sur tous les satellites clés Intelsat utilisés pour transmettre l'essentiel des communications téléphoniques, Internet, le courrier électronique, les télécopies et télex transmis par satellite dans le monde entier.

Ce système espionne toutes les nations qu'elles soient, ennemies ou alliées des puissances anglo-saxonnes, et les renseignements ressemblés ne concernent pas uniquement les domaines militaires mais aussi ceux diplomatique, commercial, financier, technologique, jusqu'à espionner, en certain cas, le simple citoyen d'un pays tiers. Mais les citoyens anglo-saxons ne sont pas eux même à l'abri : même si la loi des Etats Unis interdit d'espionner un citoyen américain sans l'ordre d'un juge, ça n'empêche pas au CSE canadien de le faire et de donner ces renseignements aux autorités américaines dans le cadre de l'alliance UkUsa.

Tout type de communications fait l'objet d'interception par Echelon : conversations téléphoniques et radio, fax, e-mail, Internet.

Même le Parlement européen a montré son inquiétude et, comme nous verrons après, plusieurs interpellations ont été posées par les députés, à tel point que des études ont été commandées pour bien évaluer les dangers et les éventuelles réponses.

Construis à partir des années 70 et mise à jour régulièrement, Echelon est constitué par une série de stations d'écoute dirigées surtout sur le trafic des satellites Intelsat. Selon M. Hager[xiv], les stations d'écoute des satellites Intelsat et Inmarsat seraient situées à Yakima (Pacifique de l'Ouest) et Sugar Grove (côte atlantique) aux Etats Unis, Morwenstow au Royaume Uni, Geralston en Australie (qui a implémenté les fonctions de la station GCHQ - DSD d'HongKong qui a été abandonnée) et Waihopai en Nouvelle Zélande.

Les communications qui passent sur les satellites russes sont ressemblées par sept autres stations situées au Royaume Uni (la base NSA de Menwith Hill, qui gère, entre d'outre, le projet Moonpenny d'interception des satellites Raduga russes), en Canada (Leitrim), en Australie, en Allemagne, au Japon (Misawa, projet Ladylove pour espionner les satellites russes Molnya, Raduga e Gorizont), à Porto Rico (Sabana Seca) et aux Etats Unis (Rosman dans le Nord Carolina)(Figure 5) .

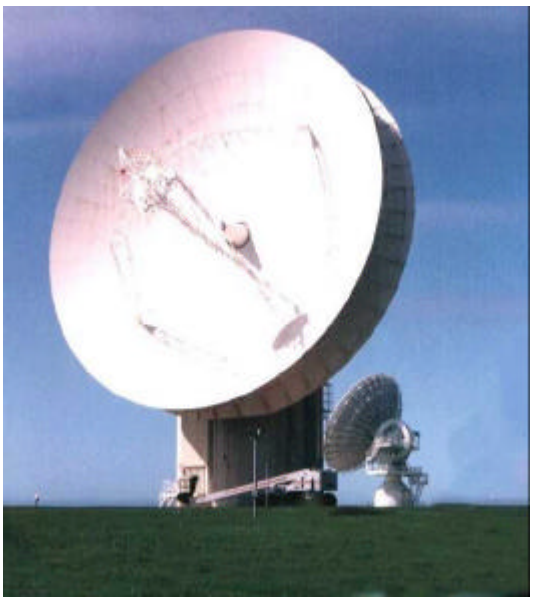


Figure 5 : les oreilles d'Echelon

D'autres stations dispersées partout (de l'Alaska à la Thaïlande) interceptent les communications radio et téléphoniques qui passent sur les câbles sous-marins. Pour faire cela on contrôle les relais côtiers qui branchent le câble au réseau téléphonique national, mais, en certain cas, on utilise des outils à induction magnétique posés sur les câbles mêmes. Pour les câbles en fibre optique, qui n'émettent aucun signal électromagnétique, on utilise les émissions des dispositifs utilisés pour renforcer le signal le long du parcours (Figure 6).

Les bases de Menwith Hill, Bad Aibling en Allemagne, Buckley en Colorado et Pine Gap en Australie servent de relais pour les satellites Sigint américains. Il s'agit de satellites de quelques tonnes en orbite géostationnaire, qui peuvent, avec leur antenne aussi grande qu'un champ de football, intercepter même les téléphones portables.

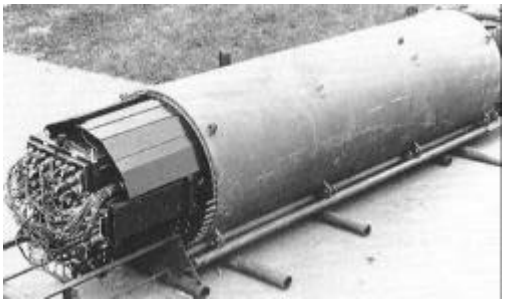


Figure 6 : Capteur électro-magnétique déposé par un soumarin américain au large de Kamchatka

Les Américains sont les seuls au monde à disposer de ce type de satellites : la tentative britannique d'envoyer dans l'espace le satellite Zircon a échoué à cause de problèmes budgétaires.

Enfin dans les Ambassades des Pays UkUsa, il y aurait des centres d'écoute qui fournissent d'autres renseignements.

Après le travail initial des satellites, un ensemble d'ordinateurs absorbe les millions d'informations qui circulent, avant de les filtrer en un temps record, le plus souvent grâce à un simple mot clé. Dans n'importe laquelle des cinq bases, il suffit qu'un ingénieur entre le mot «drogue» pour que toutes les conversations interceptées et au cours desquelles «drogue» a été prononcé soient fichées, puis classées en fonction de leur importance. «Cela va même bien plus loin», assure le journaliste Jean Guisnel, qui a étudié à fond le système Echelon[xv]. «*En réalité, les ordinateurs sont capables de saisir ce que l'on appelle l'information élaborée. Même pas la peine de prononcer le mot drogue, si la conversation tourne autour de la drogue, l'ordinateur comprend le contexte général et la sélectionne.*»

Le procédé est le même si on s'intéresse aux nouvelles technologies, à l'industrie du bâtiment ou à un possible contrat entre telle ou telle firme. «*Il est évident qu'Echelon a dû peser lourd dans l'obtention de marchés par certaines firmes américaines*», poursuit Jean Guisnel. Une fois les messages analysés, ils partent directement au quartier général de la NSA, dans le Maryland. Les Américains gardent ceux qui les intéressent et redistribuent le fruit des écoutes à leurs quatre partenaires.

d. Les grandes affaires

Malgré le culte du secret cultivé, le nom d'Echelon, toujours lié à celui de la NSA, apparaît parfois au cours d'affaires d'espionnage, mais la majeure partie des activités du réseau reste dans l'ombre. En particulier, selon plusieurs sources, notamment d'origine journalistique, dans les dix dernières années les actions suivantes auraient été effectuées:

1990 - Echelon intercepte les communications entre le fabricant japonais de satellites NEC et l'Indonésie pour la fourniture d'un contrat de 200 millions de dollars. Le président Bush intervient auprès de Djakarta. Le contrat sera partagé entre NEC et l'américain ATT.

1990 - Inauguration des nouveaux locaux de l'ambassade de Chine en Australie. Lors de la construction du bâtiment, des agents américains ont installé de multiples micros et des systèmes de surveillance des communications dans tous les murs. Les informations recueillies sont transmises directement par satellite au quartier général de la NSA dans le Maryland aux Etats-Unis.

1991 - Plus de 12 tonnes de cocaïne sont saisies grâce aux informations fournies par la NSA qui intercepte, à partir du Venezuela, toutes les communications des membres du cartel de Cali.

1992-93 - La NSA espionne les communications des officiels mexicains qui négocient l'ALENA (Accord de Libre-Échange Nord-Américain) avec les Etats-Unis et le Canada.

1993 - Au cours du sommet de l'APEC (forum de coopération Asie-Pacifique), la NSA et le FBI (Federal Bureau of Investigation) installent des équipements capables d'écouter les communications des 15 dirigeants des pays de la zone Asie-Pacifique conviés à Seattle aux Etats-Unis par Bill Clinton. Certaines informations collectées semblent avoir été transmises à des chefs d'entreprises qui ont financé la campagne électorale du président américain.

1994 - Lors du bras de fer entre les Etats-Unis et l'Union européenne dans les négociations du GATT (*General Agreement on Tariffs and Trade*), le réseau Echelon est utilisé par Washington pour connaître la position de chacun des 15 pays de l'UE et la stratégie de la Commission européenne. Des consignes seront données aux fonctionnaires de Bruxelles leur demandant de ne pas utiliser le courrier électronique, dont l'usage commence à se généraliser, pour transmettre des informations sensibles.

1994 - Interception des négociations entre le fabricant français de radars Thomson-CSF et les autorités brésiliennes. C'est finalement la firme américaine Raytheon qui décrochera le contrat pour assurer la couverture radar de l'Amazonie.

1994 - La NSA intercepte les coups de téléphone et les fax entre Airbus et les autorités saoudiennes. Le contrat de 6 milliards de dollars sera décroché par Boeing.

1998 - La NSA aurait infiltré des agents au sein de la mission de désarmement de l'ONU en Irak. Leur mission : installer de petits systèmes d'interception pour capter les communications de Saddam Hussein et de l'état-major irakien.

3. L'opposition

a. Le rôle des médias

La presse internationale joue un rôle très important dans les vicissitudes d'Echelon. Depuis quelques années tous les principaux journaux du monde ont dédié un espace à ce phénomène, en dénonçant les intrusions et les violations de la « *privacy* ». Une foule de « journalistes d'assaut » a étudié et décortiqué Echelon ; grâce à eux, plusieurs gouvernements ont revu leurs législations, notamment dans les domaines de la protection de la vie privée, des systèmes de communications et des bases de données « sensibles ».

C'est le cas en Italie, avec plusieurs dossiers sur les quotidiens et les journaux d'opinion, qui ont récemment provoqué la prise de position du Gouvernement face aux déclarations du chef des juges du parquet de Rome Carlo Sarzana. Dans une interview[xvi] il a dénoncé que « *nous sommes tous espionnés par un Big Brother étranger mais le Gouvernement ne fait rien du tout* ».

En France c'est surtout Jean Guisnel qui, des pages du Point[xvii], a dénoncé Echelon et ses tentacules, en montrant la puissance écrasante américaine dans ce domaine mais, comme nous le verrons après, en déclarant que la France elle aussi espionne ses alliés.

La presse russe s'intéresse à ce système : dans un article d'« *Izvestia* », Echelon est qualifié de « scandaleux » et on essaie d'en expliquer le fonctionnement[xviii].

Mais, paradoxalement, c'est surtout par les médias anglo-saxons qu'arrivent les attaques plus violentes. Le *New York Times*[xix], la *Tribune*[xx] et d'autres dénoncent le phénomène, vu comme une lourde ingérence sur la vie privée des concitoyens. Le Sunday Times[xxi] a relaté que par le passé les radômes de Menwith Hill dans le Nord du Yorkshire au Royaume-Uni, avaient eu pour tâche d'intercepter l'ensemble des communications commerciales ordinaires. Le personnel est passé de 400 personnes dans les années quatre-vingts à plus de 1400 aujourd'hui auxquelles s'ajoutent 370 personnes venues du ministère de la Défense.

Et sur Internet une foule de cybernautes se rebelle à l'idée d'être espionnée et contrôlée, en créant des forums de discussion et des sites « anarchiques » de dénonciation et de révolte. Selon Privacy International, le Royaume-Uni pourrait réaliser que ses « relations particulières » contreviennent aux obligations auxquelles il a souscrit en vertu du traité de Maastricht dans la mesure où le titre V du traité de Maastricht fait obligation aux États membres de s'informer mutuellement et de se concerter au sein du Conseil sur toute question de politique étrangère et de sécurité présentant un intérêt général, en vue d'assurer que leur influence combinée s'exerce de la manière la plus efficace par la convergence de leurs actions. Or, en vertu de sa relation particulière, la Grande-Bretagne ne peut s'engager à consulter librement ses autres partenaires européens.

b. Le siège à la base de Menwith Hill

Installée au nord de l'Angleterre, la base de Menwith Hill était située idéalement, du temps de la guerre froide, pour surveiller les activités de l'URSS et des pays communistes d'Europe. Ces dernières années, elle a pu facilement réorienter une partie de ses écoutes pour se concentrer désormais sur l'espionnage de l'Europe occidentale et des communications transatlantiques (Figure 7). Ce qui frappe le plus les visiteurs, ce

sont les immenses boules blanches qui semblent venues d'ailleurs. Les " balles de golf ", comme les appellent les habitants de la région, mesurent jusqu'à une vingtaine de mètres de diamètre. Il s'agit de radômes, autrement dit de structures creuses qui abritent des paraboles de réception satellitaire. Les 28 globes blancs protègent donc autant de paraboles contre les effets du vent, de la pluie et de la neige, mais aussi contre les regards indiscrets. Il est impossible pour les automobilistes qui longent la base de voir dans quelle direction sont pointées ces antennes-satellite. Impossible également de deviner ce qui se passe à l'intérieur du bâtiment à demi enterré où se trouvent les postes de commande et de contrôle de la base.

L'accès à la base de Menwith Hill de la RAF (Royal Air Force) est gardé par des policiers en arme et strictement contrôlé. Mais en dépit de sa dénomination officielle, la plupart des 2.000 personnes qui travaillent ici ne sont pas britanniques. Dans cette base, contrôlée depuis 1966 par la NSA, les plus nombreux sont les citoyens américains, civils et militaires.

Figure 7 : la station d'écoute de Menwith Hill

C'est d'ailleurs un officier de l'armée américaine qui commande ce site baptisé " base F83 " par les experts en renseignement électronique de la NSA.

Les activités précises de la base de Menwith Hill demeurent en grande partie mystérieuses. Quelques parlementaires britanniques ont bien tenté d'interpeller le gouvernement britannique pour connaître le statut et rôle de la base, mais la réponse a toujours été identique : *"nous ne pouvons pas répondre, c'est une question de sécurité nationale".*

Face à ce mutisme, une poignée de militants pacifistes a décidé d'en avoir le cœur net. Depuis le début des années 90, Lindis Percy et ses amis mènent une campagne de harcèlement avec les faibles moyens dont ils disposent. Ce n'est même pas David contre Goliath, c'est une piqûre de mouche sur le dos d'un éléphant.

Leur association, la CAAB (*Campaign for the Accountability of the American Bases*) multiplie les actions de protestations, les procédures devant les tribunaux et Lindis Percy effectue de multiples intrusions à l'intérieur du site pour tenter d'en savoir plus. Résultat de ce travail de fourmi : une partie des activités de Menwith Hill a été mise au jour. Ces militants ont mis en évidence l'existence de plusieurs programmes et ont décrypté leurs noms de code ésotériques .

Par exemple :

- « Silkworth » désigne un système de satellites positionnés au-dessus de pays-cibles et qui captent les communications micro-ondes qui servent notamment de relais à l'extrémité des câbles sous-marins à haut débit ;
- « Moonpenny » désigne un programme d'interception de certains satellites de télécommunication non-américains ;
- « Runway » reçoit les informations captées par les satellites espions Vortex qui écoutent les télécommunications relayées par Intelsat ;

- « Steeplebush I et II » sont des systèmes informatiques sophistiqués qui rassemblent toutes les données recueillies par les différents programmes ;

Cependant les activités de la base ne tournent pas seulement autour de l'espionnage au sens où on l'entend habituellement. Lors de la guerre du Golfe par exemple, les installations de Menwith Hill ont servi à détecter les tirs de missiles Scud Irakiens contre l'Arabie Saoudite et Israël. Et ce sont les informations collectées par les grandes boules blanches du Yorkshire du nord qui permettaient ensuite de guider les missiles antimissiles Patriot.

Menwith Hill est la plus grande base d'espionnage du monde, mais elle n'est pas la seule. A Pine Gap, en Australie, une installation du même type a été mise en place par la NSA pour surveiller les télécommunications dans l'hémisphère sud.

c. Le sénateur BARR

Un attaque probablement inattendu par les hommes de la NSA a été conduit récemment par un sénateur américain, Bob Barr.

Le Sénateur Barr (Figure 8) est un ancien juge et analyste de la *Central Intelligence Agency* (CIA), qui sert dans les comités judiciaires, des réformes et des banques du Congrès américain.

Figure 8 : Le sénateur Barr

Le 13 mai du 1999 le sénateur Barr a proposé un amendement au « *Foreign Intelligence Authorization Act for FY 2000* », adopté par le Gouvernement américain, en parlant officiellement pour la première fois du projet Echelon.

« *Si les agences de renseignement des Etats Unis interceptent, reçoivent ou diffusent des communications qui regardent nos citoyens sans l'autorisation de l'autorité légale, elles le font au dehors de la constitution. Si le projet Echelon existe, tous les Américains qui ont à cœur l'intégrité de la Constitution sont concernés* » a-t-il déclaré.

« *J'encourage la communauté de renseignement* » il a poursuivi « *à préparer un rapport détaillé sur le sujet. Seulement un rapport public pourra redonner assurance à nos concitoyens que leurs vies privées ne sont pas à risque d'intrusion* » [xxii].

Son attaque n'a pas eu l'effet désiré, aucun rapport officiel n'a été fourni jusqu'à maintenant par la NSA sur le projet Echelon. Les intérêts en jeu sont trop grands et les acteurs sont probablement trop puissants.

Mais le sénateur Barr n'a pas perdu son âme. Le 17 novembre 1999 a envisagé la surveillance d'Echelon en créant un site sur Internet mis à jour par des organisations pour les libertés civiles, notamment la *American Civil Liberties Union* (ACLU), l'*Electronic Privacy Information Center* (EPIC), et le *British Omega Foundation*, Ce

site doit servir comme « *fond commun d'information sur le projet Echelon* »[xxiii] a-t-il affirmé.

4. Echelon et l'Europe

a. Inquiétude au Parlement Européen

Les révélations sur les potentialités d'Echelon ont pressé le Parlement Européen à commander au STOA (*Scientific and Technological options assessment*)[4] une première étude sur le sujet, suivi par une deuxième plus approfondie (« *Une évaluation des techniques de contrôle politique* », 6 Janvier 1998, suivi par « *Développement des techniques de surveillance et risque d'abuse des renseignements économiques* », Avril 1999, présenté au Parlement Européen le 23 février 2000).

La prédominance américaine dans le Sigint est perçue avec une intolérance de plus en plus grande de côté Européen. L'explosion d'Internet, dominé par des technologies « *made in USA* » et dont les nœuds de communication sont contrôlés par Washington pose d'autres interrogations aux gouvernements et aux industries européennes.

Plusieurs interpellations parlementaires ont été posées depuis les deux dernières années, par tous le groupes politiques, notamment par les députés Esko Seppänen[xxiv], Giuseppe Rauti[xxv], Paul Lannoye, Olivier Deleuze et Jean Luc Robert.

Ces trois derniers, en particulier, parlent avec une certaine inquiétude des nombreux problèmes politiques que pose Echelon à l'Union européenne. Notamment :

- un problème de sécurité politique : le fait que les Etats membres, les hommes politiques, les syndicalistes, les activistes d'organisations non gouvernementales, tous ceux qui peuvent apparaître comme subversifs ou gênants à l'égard de certains groupes d'intérêt, soient susceptibles d'être espionnés constitue une menace grave pour les libertés publiques et l'exercice de la citoyenneté ;
- un problème de sécurité économique : l'espionnage économique menace la compétitivité des entreprises qui en sont potentiellement victimes ; les entreprises européennes souffrent donc d'un désavantage compétitif à l'égard des entreprises américaines ... et britanniques ;
- un problème de confiance à l'égard d'un Etat membre et de respect des traités : le sentiment, dans l'ensemble de l'Union, d'être grugés par un partenaire (le Royaume-Uni) compromet l'indispensable confiance au sein de l'Union.

La réponse donnée à ces interpellations par le commissaire Bangemann au nom de la Commission Européenne le 14 septembre 1998 fut aussi lénifiante qu'embarrassée. Le commissaire met en doute l'existence même d'Echelon «*nous n'avons pas le moindre indice venant d'un Etat membre montrant que quelqu'un (citoyen, entreprise,...) se trouve lésé dans ses droits et montrant que ce système existe réellement*».

On peut s'étonner d'une telle réponse alors qu'au sein même de la Commission, il semble bien que de hauts fonctionnaires s'inquiètent des risques d'interception de communications importantes émanant de leurs services. Le président Santer lui-même aurait pris l'initiative d'alerter les principaux responsables de l'institution... [xxvi]

b. « Une évaluation des techniques de contrôle politique »

[4] Il s'agit d'un organisme de la Division Générale de recherche du Parlement européen, avec siège à Strasbourg, qui a le but de fournir un support de connaissance technico-scientifique aux travaux du Parlement

Cette première étude, commandée par le Parlement européen au STOA, a été rédigée par la Fondation Omega de Manchester et présentée au mois de septembre 1998 au Parlement européen.

L'étude a été conçue pour répondre aux objectifs-clés suivants:

- fournir aux membres du Parlement européen un guide de référence concis sur les récents progrès réalisés en matière de techniques de contrôle politique;
- identifier et décrire l'état actuel des développements les plus importants, en précisant davantage et en mettant à jour les éléments de l'étude qui ont suscité l'intérêt et les commentaires les plus importants du public;
- présenter aux eurodéputés un résumé des tendances actuelles en Europe et dans le monde;
- proposer des options politiques couvrant des stratégies réglementaires pour le contrôle et la gestion future de ces techniques.

Selon le rapport il existe globalement deux systèmes distincts d'interception:

- Le système anglo-américain couvrant les activités de services de renseignement militaires tels que NSA-CIA aux États-Unis englobant le GCHQ et MI6 britannique qui opèrent un système connu sous le nom d'ECHELON;
- le système UE-FBI qui assure la liaison entre divers services répressifs, tels que le FBI, la police, les douanes, les services de l'immigration et ceux de la sécurité intérieure.

(1) L'interception NSA de toutes les télécommunications de l'U.E.

L'étude confirme tous les bruits donc on vient de parler. Toutes les communications électroniques, téléphoniques et par fax en Europe seraient quotidiennement interceptées par la NSA et ses alliées , qui transfèrent toutes les informations provenant du continent européen via le centre stratégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York Moors au Royaume-Uni.

Le système ECHELON fonctionne en interceptant sans distinction de très grandes quantités d'informations puis en en triant les éléments intéressants à l'aide de systèmes d'intelligence artificielle comme Memex, à la recherche de mots-clés (Figure 9).

Chacune des cinq Nations partenaires fournit aux quatre autres des « dictionnaires » de mots-clés, de phrases, de personnes et de lieux pour "l'identification" et le message intercepté ainsi identifié est transmis directement au pays demandeur.

Le rapport cite Nick Hager[xxvii], selon le quel les principales priorités du système, et de loin, continuent à être le renseignement militaire et politique

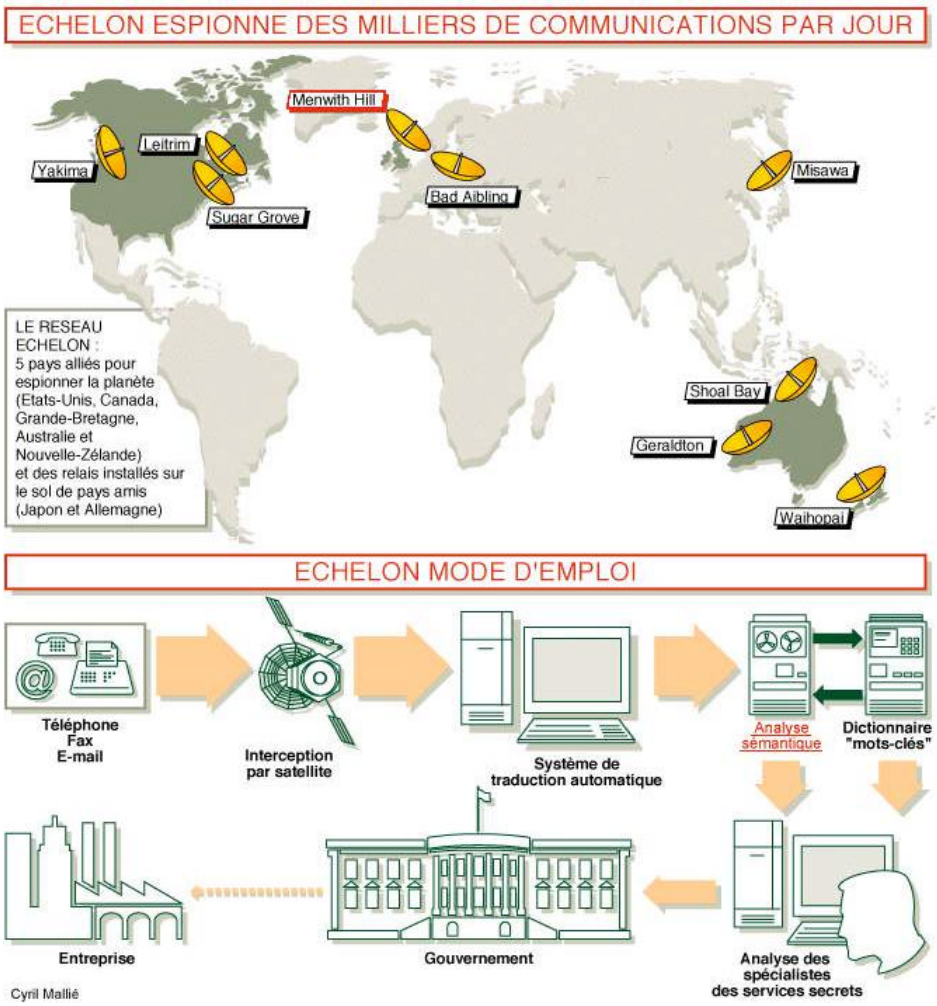


Figure 9 : le fonctionnement d'Echelon

correspondant aux principaux centres d'intérêt des partenaires du système.

Hager cite des agents de renseignements très haut placés qui se sont exprimés dans l'Observer de Londres. « *Nous estimons ne pas pouvoir nous taire plus longtemps sur ce que nous considérons comme une incurie et une négligence grossières de la part des institutions pour lesquelles nous travaillons* ». Ils ont cité pour exemple l'interception par GCHQ des communications de trois organisations bénévoles, y compris Amnesty International et Christian Aid. Selon cette source du GCHQ: « *à tout moment GCHQ est en mesure d'écouter leurs communications pour répondre à une demande ciblée de routine* ». Dans le cas d'écoutes téléphoniques, la procédure est connue sous le nom de Mantis. Pour les télex, elle a pour nom Mayfly. Lorsque l'on tape un code relatif à l'aide au tiers monde, la source est en mesure de se positionner sur les télex des trois organisations.

En l'absence de système de contrôle, il est difficile de découvrir les critères qui déterminent ce qui échappe à ce criblage. «*Les mots-clés identifiés par les experts américains incluent les noms d'organisations intergouvernementales et de consortiums d'affaires en concurrence avec des entreprises américaines. Le mot "bloc" est sur la liste pour identifier les communications sur les ressources pétrolières offshores dans des régions où le fond de la mer doit encore être divisé en blocs d'exploration* ».

(2) Le système global de surveillance des télécommunications UE-FBI

L'essentiel des informations et de la recherche nécessaire pour faire connaître au public l'histoire, la structure, le rôle et la fonction de la convention passée entre l'UE et le FBI visant à légitimer la surveillance électronique globale, est l'œuvre de Statewatch, une organisation de surveillance et de recherche sur les libertés publiques, basée au Royaume-Uni et qui fait autorité en la matière.

Statewatch a longuement décrit la signature du calendrier transatlantique à Madrid lors du sommet UE-US du 3 décembre 1995, dont faisait partie le « Plan d'action conjoint UE-US », et a analysé par la suite ces efforts comme une tentative de redéfinition de l'Alliance transatlantique dans l'après-guerre froide, un thème de plus en plus utilisé pour justifier les efforts déployés par les services de sécurité interne pour conforter leur rôle de maintien de l'ordre en Europe. Statewatch note que le premier plan de surveillance « hors zone » de l'action conjointe n'a pas été inscrit à l'ordre du jour de la réunion des ministres de la justice et des affaires intérieures mais a été adopté sans discussion, sous forme de point A (sans débat) par, ô combien surprenant, le Conseil de la pêche du 20 décembre 1996.

En février 1997, Statewatch indiquait que l'UE avait secrètement accepté la création d'un réseau international d'écoutes téléphoniques via un réseau secret de commissions créées dans le cadre du « troisième pilier » du traité de Maastricht couvrant la coopération dans les domaines juridiques et du maintien de l'ordre. Les principaux points de ce plan sont soulignés dans un protocole d'accord, signé par les États de l'Union européenne en 1995 (ENFOPOL)[xxviii], qui est toujours classé secret. Selon *The Guardian* du 25.2.97, il reflète la crainte exprimée par les services de renseignements européens que les technologies modernes les empêchent d'écouter les communications privées.

Les pays de l'UE, selon ce journal, devraient convenir de normes internationales en matière d'interception, fixées à un niveau permettant le décodage ou l'interprétation des mots brouillés par les services gouvernementaux. Des rapports officiels indiquent que les gouvernements de l'UE ont convenu de coopérer étroitement avec le FBI à Washington. Or, des procès-verbaux antérieurs à ces réunions semblent indiquer que l'initiative est venue de Washington. Selon Statewatch, les fournisseurs de réseaux et de services au sein de l'UE seront tenus d'installer des systèmes « écoutables » et de placer sous surveillance toute personne ou groupe lorsqu'ils se verront présenter une demande d'interception.

Ces projets n'ont jamais été soumis au contrôle d'un gouvernement européen, quel qu'il soit, ni à la commission des libertés publiques du Parlement européen, en dépit des aspects évidents de libertés publiques soulevés par ce type de système non contrôlé. Le feu vert a simplement été donné secrètement par «écrit » sous forme d'un échange de télex entre les gouvernements des 15 États membres de l'UE. Statewatch précise que le plan global de surveillance UE-FBI se développe désormais « *en dehors du troisième pilier* ». En clair, cela signifie que ce plan est développé par un groupe de vingt pays, les 15 États membres de l'UE plus les États-Unis, l'Australie, le Canada, la Norvège et la Nouvelle-Zélande. Ce groupe de vingt pays ne rend aucun compte de ses travaux au Conseil des ministres de la justice et des affaires intérieures, ni au Parlement européen ou aux parlements nationaux. Rien n'est dit sur le financement du système mais un rapport émanant

du gouvernement allemand estime que la part du projet concernant les téléphones portables s'élève, à elle seule, à 4 milliards de DM.

Statewatch en conclut que c'est l'interface entre le système ECHELON et son évolution potentielle sur les communications téléphoniques, combinée à la normalisation de centres et d'équipements permettant l'écoute des communications, bénéficiant du soutien de l'Union européenne et des États- Unis qui présente une véritable menace globale sur laquelle ne s'exerce aucun contrôle juridique ou démocratique[xxix]. À maints égards, nous assistons à des réunions d'agents d'une nouvelle puissance mondiale militaire et du renseignement. Il est très difficile pour quiconque d'avoir un tableau d'ensemble de ce qui se décide lors de ces réunions au sommet qui élaborent cet « Agenda transatlantique ».

c. *« Développement des techniques de surveillance et risque d'abuse des renseignements économiques »*

Cette étude a été confiée à Duncan Campbell, un journaliste indépendant anglais qui travaille depuis plus de 20 ans sur les questions liées à l'utilisation des nouvelles technologies par les services de renseignement. En 1988, il fut le premier à détailler le projet américano-britannique de réseau mondial d'espionnage des télécommunications.

Il fait une analyse très ponctuelle et exacte des systèmes de renseignements dont dispose Echelon, en particulier des systèmes satellitaires. J'en propose un extrait très intéressant dans l'annexe technique à ce mémoire.

Comme ses prédécesseurs de la fondation Omega, Campbell aussi arrive à démontrer l'existence d'Echelon.

Mais tandis que le premier rapport Echelon décrit un scénario « *Orwellien* », avec un *Big Brother* qui peut tout intercepter et, en utilisant des « dictionnaires » de mots-clés, tout espionner, au contraire Duncan Campbell ramène à des justes proportions le réseau, qui ne serait pas capable d'analyser les mots des conversations téléphoniques. Echelon aurait les mêmes problèmes que ceux des moteurs de recherche d'Internet : des montagnes de donnés archivées sans aucun critère d'ordre, où chercher un renseignement est comme chercher une aiguille dans une botte de foin.

Campbell soutien aussi que le futur d'Echelon est condamné: le développement des communications et des messages voie téléphone portable, du réseau Internet et des techniques de cryptographie des données, l'emploi de plus en plus fréquent des fibres optiques et des câbles sous-marins ont mis hors jeu une grande partie du réseau d'espionnage. Si les communications intercontinentales des années '70 pouvaient être interceptées par deux stations terrestres syntonisées sur « Intelsat », aujourd'hui cette technologie n'est plus suffisante.

Pour cette raison Echelon est en train de chercher à remédier avec deux stratégies : la mise à jour des technologies d'espionnage et les fortes pressions sur les politiques et les législateurs, pour que les nouveaux moyens de communications soient réalisés en utilisant des technologies plus « faibles », pour en permettre une interception plus facile.

Dans le premier cas, Echelon peut se fier à quelques industries américaines retenues «amies », qui produisent ce qu'il faut pour se mettre à jour. La Ast, par exemple, produit pour le « *Big Brother* » le « *transponder* » pour intercepter les nouveaux satellites, le « *snapper* » pour analyser les bandes magnétiques et enregistrer les données et l'unité « *Acquisition data* » pour les analyser. Il s'agit d'instruments qui

peuvent gérer des données équivalentes à 40.000 conversations téléphoniques contemporaines.

Plus dangereuses et frauduleuses seraient, selon Campbell, les pressions sur administrations, sociétés, gouvernements et institutions dans le monde entier. Une loi des Etats Unis, par exemple, empêche l'exportation de systèmes de cryptographie « forte », au détriment de Netscape, Microsoft et Lotus qui ont dû réduire les capacités de leurs produits destinés aux marchés étrangers. Dans le même point de vue, on peut aussi regarder les pressions diplomatiques du Gouvernement américain vis à vis des pays européens pour un accord mondial dans le domaine des interceptions, qui prévoirait l'emploi de technologies et de standards de cryptographie produits aux Etats Unis et contrôlés par les services de renseignements américains.

5. L'Europe se défend

La suprématie américaine dans le domaine du Sigint est vue de plus en plus avec intolérance par l'Union européenne. La diffusion d'Internet, dominé par de technologies « made in USA », dont les nœuds principaux sont contrôlés par Washington, pose d'autres questions aux Gouvernements européens.

Face au refus américain de permettre la vente à l'étranger de systèmes de cryptographie « forte » (avec une clé supérieure à 56 bits), l'Europe cherche à développer ses systèmes.

La France a récemment libéralisé la vente de ces technologies, en passant sur les objections qu'elles puissent favoriser l'activité criminelle[xxx]. La priorité est devenue la défense des entreprises françaises contre l'espionnage électronique étranger. En tout cas, Paris continue à adhérer à la réglementation internationale (accords de Wassenaar) inspirée par les Etats Unis, qui interdit l'exportation de systèmes avec une clé supérieure à 56 bits. Ceci signifie que les pays du troisième monde n'ont aucune défense contre l'espionnage des pays plus forts et pas seulement occidentaux.

En Italie l'Institut de recherche et communications sociales (IRCS) de Turin a développé Ermes, un système qui peut cacher un fichier sur Internet. En pratique l'information pourra rejoindre n'importe quel pays en restant cachée dans un « micro-point » numérique du texte envoyé sur le Web[xxxi]

A savoir qu'il n'existe pas une politique communautaire en ce domaine même si, en ce qui concerne l'espionnage satellitaire dans le domaine des images (Imint) a été créé le centre de Torrejon, en Espagne, qui appartient à l'Union européenne.

Les pays européens, enfin, ont eux aussi des services qui font du Sigint. Mais, exception faite du Royaume Uni, ils n'ont pas une agence exclusivement dédiée au Sigint. En général, ces activités sont effectuées par les départements techniques des services d'espionnage étranger.

a. La France

Le président de la République, Jacques Chirac, dans son discours aux ambassadeurs, a dit, je cite, "*dans un monde en transformation permanente, la France a besoin, aux quatre coins de la planète, des meilleures analyses pour lui fournir en temps réel l'information approfondie, sélectionnée et pondérée sur laquelle elle pourra fonder ses jugements et ses décisions*". Pour assurer ces analyses, la France dispose de la gamme la plus complète possible de "capteurs".

(1) La DGSE

En France la «*Direction Générale de la Sécurité Extérieure* » (DGSE) est chargée du Sigint stratégique.

Service de renseignement extérieur de la France, subordonné au Ministère de la Défense, la Direction Générale de la Sécurité Extérieure est issue de l'intégration des différents services de renseignements français issus de la seconde guerre mondiale.

La DGSE s'occupe du renseignement militaire ainsi que du renseignement stratégique, des écoutes électroniques et est responsable du contre-espionnage hors des frontières de l'Etat. Officiellement son personnel militaire est affecté au 44e Régiment d'Infanterie basée a Orléans, à Cercottes ou comme le surnomme les agents, Tristus-city. Ses agents sont appelés des *honorables correspondants.*

Elle dépend du ministère de la Défense mais surtout de Matignon (1er Ministre).

Les liens traditionnels de la France avec le continent africain et le Proche-Orient ont contribué à faire de la DGSE l'un des services de renseignement occidentaux les plus performants dans ces régions. Le renseignement en direction de l'Asie ou de l'Amérique (centrale et latine) est plus faible.

La France est à l'origine de plusieurs alliances de coopération entre services. Il s'agit, entre autres du:

- « *Safari Club* », crée en septembre 1976 et qui rassemble la France, le Maroc, L'Iran, l'Arabie Saoudite, l'Égypte et le Zaïre ;
- « *Club Méditerranée* » ou « *MIDI-club* », créé à Rome en 1982, qui regroupe la France, l'Espagne, l'Italie, la Tunisie, l'Algérie et le Maroc, et dont les plus importants objectifs sont la lutte contre le fondamentalisme islamique et le crime organisé.

Dès 1981, la DGSE a placé une priorité plus élevée dans l'acquisition de renseignements technologiques. Le Directeur Général d'alors, Pierre Marion, a mis sur pied une cellule de 20 hommes spécialisés dans ce domaine. En 1991, le FBI a dévoilé les tentatives d'infiltrations de certaines entreprises américaines (notamment Texas Instruments et IBM) par la DGSE. L'acquisition de technologie par la France dans les autres pays de l'OTAN a suscité de vives critiques. Au printemps 1993, la firme américaine Hugues annonçait qu'elle n'aurait pas participé au Salon du Bourget en raison de l'espionnage technologique dont elle faisait l'objet de la part de la DGSE.

La DGSE serait aussi impliquée dans les opérations *Barracuda*, qui en septembre 1979 ont eu pour objet le remplacement de l'empereur Bokassa de la République Centrafricaine par le président David Dacko, et *Satanique*, durant laquelle le Rainbow Warrior, bateau de l'organisation « éco-térroriste » Greenpeace, a été coulé, le 10 Juillet 1985, à 23h38, dans le port d'Auckland (Nouvelle-Zélande) par les membres des services spéciaux de la DGSE, provoquant la mort du photographe et néanmoins « éco-terroriste » Fernando Peira.

La DGSE gère, par sa Division technique, un système d'interception des communications satellitaires par les stations placées en Dordogne (à Domme), en Nouvelle Calédonie et, grâce à un accord avec les autorités locales (très bonnes clientes de l'industrie des armements française…), dans les Emirats Arabes Unis. Ces deux installations interceptent les satellites qui couvrent la zone de l'Océan Indien et Pacifique et celle du moyen orient. Enfin, la station de Kourou, en Guyane française, couvre la zone américaine. Cette dernière station serait gérée avec le service de renseignement allemand (« Bundesnachrichtendienst BND »).

D'autres centres d'écoute se trouvent à Djibouti, en République Centrafricaine (mais cette station aurait été récemment fermée), en Guadeloupe et à la Réunion. L'ancienne base du Plateau d'Albion, en Haute Provence, a été transformée en une ultérieure station Sigint, gérée par une cinquantaine de spécialistes de la DGSE. L'Armée de l'Air française y a aussi installé un centre d'observation satellitaire.

La DGSE a intensifié durant ces dernières années la surveillance de l'Algérie, en utilisant des structures dans des pays voisins et le bateau espion *Berry*, récemment remplacé par le *Bougainville*, rentré de la Polynésie.[xxxii]

(2) La DRM

La « *Direction du Renseignement Militaire* » (DRM) gère les activités Sigint militaires et dispose, entre autre, du centre « *top secret* » de Mutzig, nommé « *Centre de Guerre Electronique* » (CGE)[xxxiii].

Le décret de fondation de la DRM date de juin 1992. Le phénomène "déclenchant" sa création a été l'inadaptation du renseignement français d'intérêt militaire apparue de façon très nette lors de la guerre du Golfe. Auparavant, chaque état-major d'armée disposait de son propre bureau RENS.

Le chef d'Etat-major des armées avait directement sous son autorité le Centre d'Etude du Renseignement Militaire (CERM), qui était primus inter pares. Pourtant, des questions de fond restaient traitées par des bureaux distincts et une meilleure mise en commun des connaissances est apparue nécessaire pour améliorer la qualité du service rendu aux armées.

La DRM, placée directement aux ordres du CEMA, est un organisme central qui regroupe cinq sous-directions fonctionnelles. La sous-direction "recherche" organise, dirige et coordonne la recherche du renseignement par moyens humains et techniques. La sous-direction "exploitation", chargée du suivi et de l'analyse des capacités militaires des forces de l'ensemble de la planète. Outre l'organisation des forces armées, les ordres de bataille, les tactiques et déploiements, elle s'intéresse aux politiques de défense et aux personnalités militaires des divers pays. La sous-direction "prolifération et armement" a le même métier, mais pour ce qui concerne les armements, les vecteurs et les systèmes d'armes étrangers. Elle surveille, en particulier, l'évolution des menaces liées aux activités de prolifération. La sous-direction "technique", participe à la mise à disposition des moyens matériels, définit les besoins et suit les réalisations. C'est elle qui travaille sur les affaires satellitaires, les drones, les moyens d'écoute futurs, etc. Enfin la sous-direction "ressources humaines" chargée de satisfaire les besoins en personnel de la DRM en liaison avec les diverses directions du personnel du ministère.

Par ailleurs, la DRM dispose d'organismes extérieurs qui lui sont rattachés. Il s'agit de l'EIREL (Ecole Interarmées du Renseignement et Etudes Linguistiques) de Strasbourg, et des formations et moyens de recherche et d'exploitation des renseignements d'origine humaine, spatiale, photographique, électromagnétique, et radiogoniométrique. On peut citer, entre autres, le CF3I (Centre de Formation Interarmées à l'Interprétation de l'Imagerie).

(3) L'exploitation

Comme les services de renseignements anglo-saxons, les services français emploient de puissants ordinateurs et des agents de traitement automatisé de l'information pour l'analyse des émissions interceptées.

Il s'agit de logiciels capables d'explorer les banques de données informatiques afin d'en tirer les informations pertinentes et de les adresser aux personnels concernés

En particulier le logiciel Taïga (*Traitement Automatique de l'Information Géopolitique d'Actualités*) est un outil très sophistiqué de gestion de l'information. Taïga avait pour fonction de puiser des renseignements dans les bases de données russes après la chute du régime soviétique.

C'est le linguiste et informaticien Christian Krumeich qui en 1987 chez Thomson, a mis au point ce formidable logiciel.

A la différence des autres logiciels dédiés à l'exploitation des renseignements, Taïga travaille sur une base sémantique, c'est à dire qu'il analyse la racine du mot, alors que d'autres logiciels s'appuient sur des mots clés. Taïga est capable de rechercher n'importe quelle information venant d'une dépêche de presse et serait maintenant capable d'analyser les *newsgroup* d'autant plus que Taïga comprends toutes les langues. On estime à une trentaine d'exemplaire le nombre de postes présents à la DGSE. Mais il y en aurait à la DRM et dans de grandes entreprises françaises, comme Thomson et, surtout chez Madicia, l'entreprise qui prend maintenant en charge le logiciel.

D'autres logiciels permettent l'exploitation des renseignements, en particulier pour la recherche sur Internet. Les plus importants sont:

- *Spirit*: Développé par le CEA, il permet d'indexer automatiquement d'énormes quantités de textes «on line» et de repérer dans les bases de données ainsi «consultées» les mots nouveaux qui apparaissent, ceux qui disparaissent ou ceux qui évoluent. Ce qui donne ensuite la possibilité aux chercheurs de «cibler» les technologies et procédures émergentes.
- *Topic*: c'est l'un des plus communément utilisés dans le monde. Verity, la société qui l'exploite et le développe, affirme que plus de 10 000 entreprises l'emploient actuellement; des expertises indépendantes parlent de 15 à 20% du marché... Créé à l'origine par la CIA, c'est un logiciel «intelligent» de recherche documentaire en texte intégral qui utilise la technologie de recherche par concept (les «*Topics*»). Topic permet d'associer des images et des liens hypertextes aux documents recherchés. La version temps réel assure aussi la diffusion sélective «au fil de l'eau» des informations, qu'elles soient d'origine interne ou externe.
- *Semiomap*: mis au point par Claude Vogel du Laboratoire de sémiotique informatique du pôle Léonard de Vinci, ce logiciel indexe l'ensemble des pages Web sur le monde et sur cette base fournit une sorte de «carte sémantique» sous la forme de diagramme montrant les liens entre un événement, un mot (ou un nom) et les mots (ou concepts) qui lui sont associés. En tapant le mot recherché, le logiciel fait donc apparaître sur l'écran une carte avec des vignettes de couleurs différentes, chacune représentant un «agrégat» statistique de mots qui apparaissent régulièrement ensemble dans le même contexte. On a alors une vision synthétique du contenu des pages. Ce logiciel recherche mais surtout, présente l'information. La même équipe développe aussi *Semioscan* qui permet à l'utilisateur d'identifier sur son diagramme, via un changement des couleurs, ce qui s'est transformé depuis sa dernière visite: nouveaux produits, nouvel acteur sur le marché, etc.
- *Dataview*: mis au point par l'équipe du professeur Henri Dou du Centre de recherches rétrospectives de Marseille, ce logiciel permet de repérer, dans le fouillis exponentiel des bases de données spécialisées (notamment scientifiques), les équipes de chercheurs les plus en pointe, développant la même approche, dans des domaines proches. On imagine aisément le profit qu'un laboratoire pharmaceutique pourrait tirer de l'utilisation d'un tel programme.
- *Tétralogie* : Le logiciel Tétralogie a été mis au point par Bernard Rousset de l'IRIT (Institut Régional d'Information Technologique) et recherche les sites les plus pertinents sur Internet. Il permet d'obtenir les noms des chercheurs actifs (et donc sensibles) dans les domaines recherchés et d'établir des collèges invisibles mettant en relation les chercheurs.

- *Messie* : Le logiciel Messie a été mis au point par la société Langage Naturel pour les besoins du Ministère de l'Intérieur. Il analyse l'information qu'on lui fournit avant de l'adresser aux destinataires concernés. L'avantage de Messie est qu'il se met à jour facilement en fonction des domaines qu'on lui demande d'analyser à l'aide de dictionnaires spécialisés.
- *L4U*: il s'agit d'un développement de Taïga *(voir ci-dessous)* créé par deux ingénieurs formés à l'origine dans le giron de la société détentrice de Taïga. Language For You (L4U) est multilingue, et quoique s'appuyant sur une analyse sémantique (comme Taïga) il intègre une analyse syntaxique. L'objectif de ce logiciel est de filtrer, sans risque d'erreur ou d'oubli, une information stratégique non redondante. Par exemple: détecter dans un newsgroup l'annonce d'un nouveau produit par un concurrent.
- *Périclès*: c'est une équipe d'ingénieurs ayant longtemps travaillé pour la Marine Nationale qui a créé la société Datops dont le dernier-né est ce logiciel destiné aux entreprises. Décrit comme un «système d'information virtuel», il permet l'élaboration et la diffusion de l'information économique stratégique. Fondé sur une analyse des besoins, sélectionnés à partir des activités et de la culture spécifique de l'entreprise utilisatrice, Périclès crée des agents ayant une durée de vie prédéfinie qui vont avoir la charge de localiser des données (à l'extérieur comme à l'intérieur de l'entreprise). Ceux-ci fournissent une *«veille stratégique par l'analyse des changements, des évolutions et des tendances de l'information recueillie»*. Les informations recueillies sont réparties en deux catégories: l'information «pertinente» (rapatriée sur le serveur de l'entreprise et stockée au format HTML) et l'information «intéressante» (dont l'adresse est conservée dans une base de données spécifique). Six moteurs de recherche offrent des capacités d'interrogation simultanées de ces sources hétérogènes. De plus, Périclès envoie par messagerie des dossiers «tactiques» (destinés aux échelons opérationnels) ou «stratégiques» (pour le management). Datops aurait ces derniers mois développé un «outil de détection des signaux sémantiques faibles» qui aurait permis à la Délégation générale de l'alimentation de détecter, quelques mois avant qu'elle n'éclate, la crise de la «vache folle». Et évite à un de ses clients d'investir dans une société spécialisée dans le soja génétiquement diversifié, trois semaines avant qu'un bateau transportant ce type de soja en provenance des USA soit refoulé de Grande-Bretagne.

b. Les autres pays européens

En Italie le Sigint est confié au service de renseignement militaire (« *Servizio Informativo Sicurezza Militare, SISMI »*) et au nouveau service interarmées *(« Reparto Informazioni e Sicurezza, RIS* ») de l'EMA, qui remplace les ancien Services de renseignement spécifiques d'armée.

L'Allemagne, voir ci dessus, coopère soit avec la NSA américaine soit avec la DGSE et ses activités Sigint stratégiques sont fournies par l'agence fédérale pour la Sécurité des renseignements (BSI, qui constitue aussi le département 62 du BND).

Le BND, toutefois, est plutôt lié à l'agence américaine qu'à celle française. Des renseignements recueillis par la station d'écoute franco-allemande de Kourou, en effet, sont passés par le BND à la NSA, tandis que le service allemand coopère dans la gestion d'une centrale d'écoute américaine à Taiwan pour espionner, probablement, les services commerciaux chinois, partenaire économique très important du pays d'outre Rhin.

La coopération américo-allemande dans le domaine de l'espionnage a des racines historiques car le BND est l'héritier de l'organisation Gehlen, une structure semi-officielle financé par la CIA qui recyclait les espions du Troisième Reich. La récente controverse entre Etats Unis et Allemagne sur la possibilité pour cette dernière d'accéder aux archives de la Stasi, la police sécrète de l'ancien RDA, acquises par la CIA depuis quelques années, démontre, en outre, une certaine dépendance allemande face à la contrepartie américaine.

La Suisse, territoire neutre dont se servent les services secrets et quelques organisations légales et illégales[xxxiv] pour leurs transactions financières couvertes[5], est l'une des cibles prioritaires[xxxv] de la surveillance électronique[6].

La confédération, de son côté, s'est équipée pour surveiller ses voisins. Le « Groupe Renseignement » (GR) gère deux stations d'écoute à Merihausen et à Ruthi et les données sont analysées près de Zimmerwald. A cette station seront reliés deux systèmes basés à Berne et Valais pour l'espionnage satellitaire qui deviendront opérationnels à partir du 2004. Il s'agira de systèmes pour l'écoute des réseaux Iridium et Globalstar et des satellites de communications employés par la France, l'Italie et l'Allemagne.

Les services suisses cherchent à obtenir des renseignements importants à échanger avec les autres services étrangers. Avec Echelon ? Peut être. Le monde du renseignement est une auberge espagnole, dans laquelle personne ne donne rien pour rien. Dans cette optique, le système Iridium est particulièrement important car il a une bande très étroite et la NSA sera obligée d'utiliser d'autres Nations en dehors de UkUsa.

[5] Le Mossad, le service de renseignement israélien, par exemple, s'est servi pour des années de la Banque de Crédit Internationale de Genève et la Zimex Aviation de Zurich était sa compagnie aérienne clandestine.

[6] La NSA emploi pour cette raison les bases de Ramstein, Augsbourg, Bad Aibling en Allemagne et Sorico en Italie.

6. Conclusion

La façon la meilleure pour devenir une cible d'Echelon est d'encoder ses propres communications. La NSA a une capacité très développé de casser les codes inconnus[7] même si les dernières technologies peuvent leur poser des difficultés. Pour cette raison, la NSA cherche à exercer un contrôle étroit sur les producteurs américains, en prétendant installer une « *back door* » sur les logiciels et les « *chips* » destinés aux marchés étrangers. IBM, Microsoft, Sun, tous les explorateurs et moteurs de recherche d'Internet auraient une possibilité d'accès connue seulement par la NSA : tous les producteurs de logiciels américains se sont dépêchés de démentir cette affirmation, mais leur démentie semble plutôt une confirmation[xxxvi].

En outre la NSA réalise une pression continue sur les gouvernements pour imposer, ou influencer, leurs choix dans le domaine de la cryptographie. La preuve est un message, récemment declassifié par le « *Freedom of Information act* », un organisme du Département d'Etat américain, émis par l'Ambassade américaine à Rome qui suggère le moyen, les gens et le meilleur instant pour influencer le Gouvernement italien sur des choix liés à la cryptographie[xxxvii].

Y a-t-il une manière de s'affranchir de cela ? Non, apparemment. Un Pays ou une industrie conscient de ces risques cherchera à éviter d'acheter des produits occidentaux ou bien russes et s'adressera plutôt à un Pays neutre, comme la Suisse. Mais le principal producteur de machines à chiffrer est accusé d'être, en réalité, d'accord avec la NSA. La Crypto AG est soupçonnée d'avoir depuis des années un rapport de collaboration très étroit avec la NSA[xxxviii].

En outre récemment il est apparu que l'Allemagne participe aussi à cette opération. Selon un article de « *Covert Action Quarterly* »,[xxxix] la Crypto AG serait gérée par la NSA et par le BND avec Siemens et Motorola, deux usines qui produisent des systèmes cryptographiques pour les Gouvernements américain et allemand. Parmi les témoignages recueillis près des techniciens de l'usine suisse, il apparaît que tous les produits nouveaux, avant d'être introduits sur le marché, seraient envoyés en Allemagne ou aux Etats Unis, où les techniciens de ces Pays suggéreraient des modifications à apporter pour rendre facilement déchiffrables les messages envoyés par ces machines. En pratique, dans toutes les machines, serait introduit un système qui envoie clandestinement la clé avant du message chiffré : seule la NSA pourraient recevoir ce message, connaître la clé et, donc, déchiffrer le message.

La dernière frontière de la NSA est la surveillance d'Internet, qui se passe surtout en espionnant les nœuds stratégiques qui passent par les Etats Unis, en particulier ceux de la NASA à Sunnivale en Californie et de College Park au Maryland. Une étude française[xl] sur l'espionnage économique met en garde les entreprises françaises à faire trop de confiance au Web et propose à l'Etat le développement et l'emploi de systèmes de sécurité exclusivement français.

Nous sommes donc tous espionnés par un grand frère ? Echelon peut-il vraiment entrer chez nous et contrôler notre vie ? La chose n'est pas si évident et la présomption d'être espionné est devenue plus une mode ou une ambition qu'une réalité. Que dire alors : Echelon existe-t-il vraiment ?

[7] D'après un récent calcul les super ordinateurs de la NSA occuperaient un espace de onze hectares dans une enceinte souterraine près de la siège centrale de l'agence à Fort Meade. La NSA est le deuxième utilisateurs de super ordinateurs du monde.

Le premier rapport commandé par le Parlement Européen a fait du bruit et la communauté internationale s'est indignée face à cette possibilité. D'après sa présentation, les journaux du monde entier, comme nous avons vu, ont commencé à parler d'Echelon. Aucun journal, toutefois, trouve une piste originale ou une preuve directe de ce qu'il écrit. La preuve est toujours et seulement le rapport STOA.

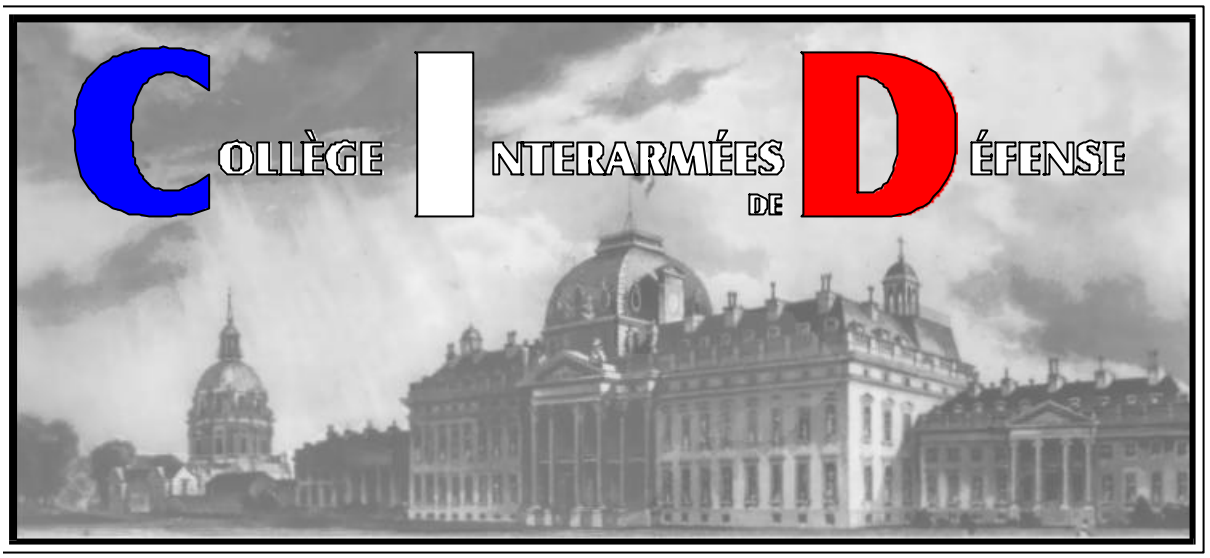
Mais aucune source du rapport est une source directe : l'existence d'Echelon est citée dans un livre et dans une enquête journalistique. Quand Steve Wright de la fondation Omega affirme que «*toutes les communications sont interceptées par la NSA* », il ne s'appui que sur « *Somebody's listening* (enquête du 1981 par Duncan Campbell) », sur le livre « *Secret power* » de Nick Hager et sur « *The Puzzle Palace* » (du journaliste américain James Bamford). Les autres sources sont la *Reuter*, le *Telegraph* , le *Times*, le *Guardian*, les dénonciations d'*Amnesty International*, de *Privacy International* ou de *Statewatch*. Les sources sont donc toutes indirectes : Echelon existe parce que *Reuter* et *Nick Hager* l'ont dit. Et les journaux, de leur coté, ont la preuve qu'Echelon existe parce que c'est écrit dans le rapport STOA !

Pourrons nous jamais savoir la vérité sur Echelon ? S'il existe ou s'il s'agit d'une fantaisie d'écrivains, de journalistes et des activistes politiques ?

Ni les Etats Unis ni la Grande Bretagne n'ont jamais démenti l'existence d'Echelon. Et l'absence de démentie devrait suffire. En plus, les bases d'écoute sont une réalité. Et la réticence de la NSA au Sénat des Etats Unis démontre, à mon avis, encore une fois que vraiment le « *big brother* » existe.

Si la moitié seulement de ces informations est exacte, le Parlement européen doit agir pour s'assurer que ces puissants systèmes de surveillance opèrent de façon plus démocratique dès lors qu'il a été mis fin à la guerre froide. Certes, les politiques transatlantiques des États membres de l'Union européenne ne coïncident pas toujours avec celles des États-Unis et, en termes de commerce, l'espionnage reste ce qu'il est. Aucune autorité digne de ce nom aux États-Unis n'autoriserait qu'un tel système d'espionnage européen opère à partir du sol américain sans strictes limitations, si tant est qu'elle le fasse.

Mais alors, même si le Parlement Européen s'indigne, pourquoi les Nations ne le suivent pas ? La raison est éclatante : « *cosí fan tutte* (tout le monde fait la même chose) », en paraphrasant le célèbre opéra de Mozart. Toutes les Nations européennes disposent de moyens plus ou moins sophistiqués pour l'interception et l'écoute et toutes emploient cet instrument pour leurs intérêts nationaux. Les performances de la NSA sont certainement impossibles à atteindre par les autres acteurs, mais ils n'ont pas besoin de performances globales et aussi sophistiquées. Pour revenir à l'introduction de ce mémoire et au professeur Coutau-Bégarry, celui qui dispose des renseignements plus précis et mis à jour, dans n'importe quel domaine, est maître de la situation. Cette possibilité représente un facteur de puissance et de dissuasion supérieur à l'arme nucléaire : les renseignements peuvent être employés en temps de paix et de guerre, dans le domaine militaire et économique, et donnent la puissance de la décision et de l'initiative à celui qui les maîtrise.



Annexe technique au mémoire de stratégie:

« Le renseignement dans la stratégie des Etats-Unis : le big brother vis à vis de l'U.E. »

Rédigé par le

Capitaine de Frégate **Pier Federico BISCONTI**

TABLES DES MATIERES

Introduction

Cette annexe technique est un résumé du rapport présenté le 23 février 2000 par Duncan Campbell au Parlement européen[8]. Il s'agit d'un document très détaillé sur les moyens et les capacités dont dispose le système global d'interception américano-britannique, appelé communément Echelon.

M. Campbell, journaliste britannique qui s'occupe d'Echelon depuis des années, dénonce une ingérence du Gouvernement américain dans les affaires européennes, notamment dans le domaine économique.

Selon M. Campbell la *National Security Agency* (NSA), l'agence américaine pour la collecte et l'évaluation de renseignement d'origine Sigint, intercepterait toutes les communications du monde politique, diplomatique et financier européen au profit de l'industrie américaine. « ITD » serait ainsi une communication diplomatique italienne, « FRD » une communication en provenance d'une ambassade française. Ces exemples montrent comment la NSA et ses partenaires du pacte UkUsa cataloguent les communications interceptées. Les deux premières lettres indiquent la nation de provenance de la communication, la troisième en définit le contenu: D pour les messages diplomatiques, P pour les communications entre les corps de police, C pour les renseignements commerciaux.

Le « *big brother* » intercepte, catalogue et diffuse les renseignements à ses demandeurs: Ministres, politiciens, militaires, entreprises.

Le but de cette annexe est de donner une idée sur les techniques d'interception utilisées par Echelon, en mettant en évidence que si aujourd'hui aucune communication ne peut échapper à l'interception, dans le proche futur le grand frère sera confronté à des technologies de communication de plus en plus avancées et perfectionnées.

[8] Duncan Campbell, « *Interception capabilities 2000* »

1. L'interception des communications internationales

La plupart des nations du monde s'appuient, pour les communications internationales, aux agences nationales de télécommunications ou à des compagnies privées. Dans les deux cas les systèmes utilisés pour communiquer sont très différenciés. Les organisations Comint emploient l'acronyme «ILC » (*International leased carrier*) quand elles parlent d'interception du trafic commercial d'un pays.

Les communications peuvent être différenciées selon leur nature.

a. Communications radio à haute fréquence

Elles ont été le moyen le plus commun de transmission entre Etats jusqu'en 1960. La caractéristique de ces ondes à haute fréquence est celle d'être réfléchies par la ionosphère et par la surface terrestre, en permettant des communications de quelques milliers de kilomètres. Cela facilite la communication mais aussi l'interception qui est, donc, relativement simple. Parmi les années 1945 et 1980 la NSA et le GCHQ ont effectué l'interception HF de communications ILC européennes à partir d'une base d'écoute en Ecosse.

Durant cette période le système d'écoute le plus performant était constitué par le AN/FLR-9, un système d'antennes de plus de 400 mètres de diamètre qui permettait l'interception et indiquait la direction de la source en même temps. En 1964 ces antennes étaient placées près des bases NSA de San Vito dei Normanni (Italie), Chicksands (Royaume Uni) et Karamursel (Turquie) et étaient destinées à l'écoute de l'Armée de l'Air soviétique. Après 1966 la station de Chicksands fut transformée pour intercepter et collecter les communications ILC européennes et les communications NDC (*non-US diplomatic communications*), notamment celles du type FRD (*French diplomatic Communications*).

b. Communications à ondes courtes

Elles furent introduites dans les années 50 pour fournir une grande capacité de communications entre villes pour la téléphonie, la télégraphie et, ultérieurement, pour la télévision. Il s'agit de communications directionnelles employant des puissances de transmissions réduites et des antennes paraboliques, placées, à cause de la courbure terrestre, sur les sommets des collines et des immeubles. Une station relais est donc nécessaire tous les 30-50 kilomètres.

Néanmoins, seulement une petite partie du signal transmis rejoint les stations relais. Le restant dépasse l'horizon et se perd dans l'espace.

Dès 1960 on a imaginé d'exploiter ce phénomène en faveur du Comint, en interceptant les communications par des moyens spatiaux. L'expérience démontra que la place la meilleure pour les satellites n'était pas sur la verticale du pays victime mais décalée d'environ 80 degrés de longitude.

Le premier satellite Comint américain fut le CANYON, lancé en août 1968. Ce satellite fut suivi bientôt par d'autres : sept satellites CANYON furent placés en orbite quasi géostationnaire entre les années 1968 et 1977. Leur but principal était les communications soviétiques, appuyées essentiellement sur des réseaux à ondes courtes.

Le succès des satellites CANYON convainquit les Américains d'envoyer dans l'espace d'autres satellites Comint. Les premiers deux satellites CHALET furent lancés en juin 1978 et octobre 1979 et contrôlés par une base terrestre placée à Menwith Hill, en Angleterre. Quand le nom CHALET fut diffusé par la presse, les satellites furent renommés VORTEX. En 1982 la NSA reçut l'autorisation par le

parlement d'opérer sur quatre satellites VORTEX en même temps. Une fois encore, quand la presse diffusa le nom VORTEX, les satellites furent renommés MERCURY.

Dès 1985 les satellites MERCURY sont employés pour l'écoute des communications au Moyen Orient. La base de Menwith Hill a eu donc un rôle fondamental durant la guerre du Golfe. Aujourd'hui Menwith Hill est la plus grande base américaine d'écoute, employée aussi à l'égard d'Israël, ami traditionnel des Américains. Enfin Menwith Hill a été récemment agrandie pour évaluer les donnés qui proviennent de la nouvelle famille de satellites Comint américains, placés en orbite entre 1994 et 1995 et dont le nom est encore inconnu.

Entre 1967 et 1985 la CIA aussi a placé en orbite une série de satellites SIGINT, avec des capacités complémentaires à celles des satellites de la NSA. Connus d'abord avec le nom de RHYOLITE, puis de AQUACADE, ces satellites peuvent intercepter les communications dans les bandes de fréquence UHF et VHF. Une deuxième série, connue d'abord comme MAGNUM et puis comme ORION, a été récemment lancée dans l'espace, avec le but d'intercepter les communications des téléphones portables. Une troisième série de satellites, enfin, appelés JUMPSET d'abord et TRUMPET ensuite, travaille dans une orbite polaire et permet la couverture des communications effectuées aux hautes latitudes et l'interception des signaux envoyés aux satellites russes de communication.

Aucune autre nation au monde ne dispose de capacités aussi développées pour l'écoute avec des moyens satellitaires. Les Britanniques (projet ZIRCON) et les Français (projet ZENON) ont dû renoncer à cause de problèmes budgétaires.

c. Câbles sous-marins

Les câbles sous-marins ont représenté pendant des années la plus grande ressource de communications internationales. Les premiers systèmes se limitaient à quelques centaines de canaux téléphoniques en même temps. Les actuels systèmes en fibre optique permettent la transmission en même temps de 5 Gbps (gigabits par seconde) de renseignements numériques, l'équivalent de 60000 canaux téléphoniques simultanés.

Contrairement à ce qu'on peut croire, même les communications sur les câbles sous-marins ne peuvent échapper à l'interception, y compris les câbles en fibre optique.

En 1971 – 1972 un sous-marin américain, l'Halibut, expérimenta avec succès une technique nouvelle. Il s'agissait de déposer un outil à proximité d'un câble sous-marin, pour en tirer les émissions électromagnétiques. La technique se révéla bien adaptée et l'interception fut déclenchée pour une décennie dans la Mer d'Okhotsk, à l'est de l'URSS, par trois sous-marins différents. En 1979 le sous-marin USS Parche traversa la calotte polaire vers la Mer de Barents pour déposer un système d'interception près de Mourmansk.

En 1982 un ancien agent NSA vendit des renseignements sur ces systèmes, dont le nom de code était IVY BELLS, aux Soviétiques. Cependant les interceptions dans la Mer de Barents furent poursuivies au moins jusqu'à 1992.

En 1985 les opérations d'espionnage furent étendues aux câbles sous-marins entre l'Europe et l'Afrique occidentale.

Les missions continuent encore aujourd'hui. Le USS Parche a été modernisé et ses missions restent toujours hautement confidentielles.

L'interception sur les câbles en fibre optique, qui ne relâchent aucune émission électromagnétique, est très difficile. Ceci dit, on peut la faire sur des câbles très longs,

en plaçant des outils à proximité des dispositifs d'amplification du signal qui, au contraire, émettent des ondes électromagnétiques interceptables.

d. Communications satellitaires

Les micro-ondes ne sont pas réfléchies par la ionosphère et passent directement dans l'espace. Cette propriété à été exploitée pour communiquer avec le monde entier mais aussi par les services de renseignement pour intercepter les communications, dans l'espace ou à terre. La plus grande constellation de satellites de communications (COMSAT) est gérée par une organisation internationale qui s'appelle Intelsat (*International communications satellites*). Les satellites sont placés dans une orbite géostationnaire, pour être toujours visibles par la station terrestre. Le premier satellite géostationnaire fut placé en orbite en 1967. En 1999 Intelsat gérait 19 satellites de la 5ème à la 8ème génération, avec la possibilité de transmission numérique de plus de 99000 canaux téléphoniques, fac-similés, télex ou de télévision en même temps.

L'interception et la collecte systématique des communications satellitaires commence en 1971. Deux stations européennes furent construites dans ce but. La première à Morwenstow, en Cornouaille, pour intercepter les satellites Intelsat sur l'Océan indien et atlantique, l'autre à Yakima, Etats Unis, pour intercepter les satellites sur l'Océan pacifique. Entre 1980 et 1995 la NSA a créé de nombreux centres d'écoute des communications satellitaires ILC dans les territoires UkUsa et ailleurs.

En comptant les antennes disponibles dans les bases d'écoute, on déduit que UkUsa a la possibilité d'écouter au moins 120 satellites.

e. Techniques de communications

Jusqu'au 1970 la plupart des communications employaient de techniques analogiques. Depuis 1990 toutes les communications sont numériques, à haut débit. Les plus modernes systèmes de communication pour Internet permettent la transmission de 155 Mbs (mégabits par seconde), l'équivalent de 3 millions de mots par seconde, c'est à dire le texte de mille livres par seconde.

A partir de 1990, des systèmes Comint ont été développés pour collecter, filtrer et analyser l'ensemble de communications numériques employées sur Internet.

Les messages sur Internet sont composés par des paquets de données nommés « *datagrams* », qui contiennent des nombres (appelés adresses IP) qui représentent l'envoyeur et le destinataire du message. Ces nombres sont uniques pour chaque ordinateur branché et indiquent, entre outre, la nationalité et les sites d'origine et de destination.

L'interception du trafic Internet peut se faire en écoutant les systèmes de communication employés par les fournisseurs des services Internet ou bien directement sur le réseau, en faisant un control sur les échanges. Les deux systèmes ont leurs avantages : le premier est plus discret, l'interception reste clandestine, le deuxième a l'avantage de pouvoir accéder plus facilement à un nombre plus grand de données.

La NSA emploie pour les recherches sur le réseau des logiciels qui fonctionnent avec la même logique que les moteurs de recherche. Les sites d'intérêts sont quotidiennement visités par les ordinateurs du *National Computer Security Center*, pour trouver des nouveaux documents et en faire des copies.

2. Les capacités Comint après les années 2000

A partir des années 90 les agences de renseignements ont commencé à éprouver des grosses difficultés dans le domaine du Comint. Ces difficultés seront encore majeures dans les années à venir. La raison principale est le passage à des communications employant des fibres optiques à grande capacité. Pour l'interception sera alors nécessaire un accès physique au câble, en plaçant des outils directement sur le territoire cible. Ces limitations empêcheront de fait l'interception de la plupart des réseaux terrestres.

Même dans le Comsat, où l'accès est relativement facile, la prolifération des nouveaux systèmes limitera l'interception, soit pour des contraintes budgétaires, soit parce que quelques systèmes (par exemple Iridium) ne peuvent pas encore être interceptés par les systèmes actuels.

Les organisations Comint reconnaissent en outre que la guerre contre la cryptographie civile et commerciale est perdue. Une foule d'universitaires et d'industriels sont particulièrement experts dans ce domaine et le marché virtuel a créé un libre change de renseignement, systèmes et logiciels.

Le futur développement du Comint prévoira probablement une réduction des dépenses dans les moyens spatiaux et un emploi d'agents humains plus grand qu'auparavant pour installer des outils de collecte de renseignement ou pour obtenir des codes. Un effort toujours plus grand sera enfin fait pour attaquer les systèmes étrangers d'ordinateurs, employant Internet ou d'autres moyens (notamment pour accéder au renseignement avant qu'il ne soit chiffré).

Un récent propos d'un fonctionnaire de la CIA, John Millis, chef du « *House representatives permanent select committee on Intelligence* » américain, illustre bien ce point de vue : « Le Sigint est en crise… Dans les derniers 50 ans la technique a été amie de la NSA mais dans les derniers quatre ou cinq elle en est devenue ennemie. Les communications ne sont plus *Sigint friendly* comme elles l'ont été par le passé… Le chiffrage est désormais à la portée de tout le monde et se développe rapidement… Il sera nécessaire d'investir beaucoup d'argent sur le Sigint pour obtenir les renseignements dont nous avons encore besoin pour notre politique ».

Glossaire

ACLU	American Civil Liberties Union
ALENA	Accord de Libre-Échange Nord-Américain
APEC	Asie-Pacific Economic Conference
BND	Bundesnachrichtendienst
CAAB	Campaign for the Accountability of the American Bases
CEMA	Chef d'Etat Majeur des Armées
CERM	Centre d'Etude du Renseignement Militaire
CF3I	Centre de Formation Interarmées à l'Interprétation de l'Imagerie
CGE	Centre de Guerre Electronique
CIA	Central Intelligence Agency
Comint	Communication Intelligence
CSE	Communications Security Establishment – Canada
DGSE	Direction Général de la Sécurité Extérieure
DRM	Direction de Renseignement Militaire
DSD	Defence Signals Directorate – Australia
EIREL	Ecole Interarmées du Renseignement et Etudes Linguistiques
Elint	Electronic Intelligence
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
FY	Fiscal Year
GATT	General Agreement on Tariffs and Trade
GCHQ	Government Communications Headquarters – GB
GCSB	GCSB Government Communications Security Bureau – Nouvelle Zélande
GR	Groupe Renseignement – Suisse
Humint	Human Intelligence
Imint	Imagery Intelligence
IRCS	Istituto di Ricerca e Comunicazione Sociale – Torino
IRIT	Institut Régional d'Information Technologique
IW	Information Warfare
Masint	Measure and Signature Intelligence
MTR	Military Technical Revolution
NEC	National Economic Council
NSA	National Security Agency
ONG	Organisations Non Gouvernementales
Osint	Open source Intelligence
RAF	Royal Air Force
RDA	République Démocratique d'Allemagne
RIS	Reparto Informazioni e sicurezza – Italie
RMA	Revolution on Military Affaires
Sigint	Signal Intelligence
SISMI	Servizio Informativo Sicurezza Militare – Italie
STOA	Scientific and Technological Options Assessment
TAIGA	Traitement Automatique de l'Information Géopolitique d'Actualités
UE	Union Européenne
UkUsa	United Kingdom – United States of America

Bibliographie

[i] Hervé Coutau-Bégarie – Editorial au n° 69 de la Revue Stratégique - "Stratégie, information, communication"
[ii] Joint Pub 2-0 – Joint Doctrine for Intelligence support to operations, 5 Mai 1995
[iii] Andrew Krepinevich, "Révolution dans les conflicts: une perspective américaine" in "Les cahiers du CREST", n° 12 1993
[iv] Christian Malis, *Signification historique et portée d'un phénomène américain :La révolution dans les affaires militaires, http://stratisc.org/Malis_RMA.html*
[v] Pierre Lacoste, *Une nouvelle stratégie pour le renseignement?*, "Politique Étrangère" n1 1997
[vi] White House Office of the Press Secretary, May 4, 1994 , www.whitehouse.gov
[vii] Clinton, William J. (1996 October 15). Statement on the Economic Espionage Act. U.S. Newswire, www.whitehouse.gov
[viii] A national security strategy for a new century, The White House, December 1999, www.whitehouse.gov
[ix] President William J. Clinton, State of the Union Address, U.S. Capitol Washington, D.C. Release January 27, 2000, www.whitehouse.gov
[x] Vincent Jauvert, *"Nous avons fait le choix de tout savoir"*, "Le Nouvel Observateur 16 décembre 1998
[xi] Desmond Ball et Jeffrey Richelson, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, Allen & Unwin, Sydney 1988
[xii] Mario De Arcangelis, *La storia dello spionaggio elettronico*, Milano, 1987
[xiii] Nick Hager - Secret Power – New Zealand's role in the International Spy Network
[xiv] Nick Hager – œuvre citée
[xv] Jean Guisnel, Guerres dans le cyberespace, Services Secret et Internet, La Decouverte
[xvi] Le "Messaggero" de Rome, 21 Janvier 1999
[xvii] Le point, 6 Juin 1998, Jean Guisnel.
[xviii] Izvestia, 25 Septembre 1998 'Scandalous "ECHELON" par Elmar Gusseinov
[xix] The New York Times, 24 Février 998, European Study Paints a Chilling Portrait of Technology's Uses, by Bruno Giussani
[xx] The Tribune, 13 Janvier 1998, Watching all over the World, by Glyn Ford
[xxi] The Sunday Times, 11 mai 1998
[xxii] http://www.house.gov/barr
[xxiii] www.echelonwatch.org
[xxiv] Interrogation écrite (1999/C 14 /003) P 1894/98 - 9 juin 1998 « Participation de l'Union Européenne aux interceptions électroniques
[xxv] Interrogation écrite (1999/C 341/132) E- 337/99 -23 février 1999 « Système d'espionnage USA en Europe »
[xxvi] Interrogation écrite (1999/C 135/187) P 3014/98 – 28 septembre 1998 « Système Echelon »
[xxvii] Nick Hager – œuvre citée
[xxviii] ENFOPOL 112 10037/95, 25.10.95
[xxix] Statewatch, Communiqué de presse du 25.2.1997
[xxx] « Le Monde » 21 janvier 1999, Eric Icyan, « L'espionnage électronique priorité de sécurité informatique »
[xxxi] « Famiglia Cristiana », 25 avril 1999. A savoir que cet article est apparu sur Internet la même semaine, traduit en anglais par la CIA (http://jya.com/echelon-ermes.htm)
[xxxii] Le point, 6 Juin 1998, Jean Guisnel.
[xxxiii] Jean – Pierre Husson, *La Brigade de Renseignement et de Guerre Electronique*, « Panorama Défense » décembre 1998.
[xxxiv] R. T. Naylor, *Denaro che scotta*, Milano, 1986
[xxxv] J. Ziegler, *La Svizzera lava più bianco*, Milano, 1990
[xxxvi] Panorama Difesa n° 170 – Novembre 1999
[xxxvii] www.foia.state.gov/52fa.pdf
[xxxviii] James Bamford *The Puzzle Palace: A Report on America's Most Secret Agency*, Penguin Books, 1983
[xxxix] Wayne Madsen, *Crypto AG: NSA's Trojan Whore?*, "Covert Action Quarterly", Hiver 1998
[xl] AAVV, Economie et sécurité: de l'industrie de défense et l'intelligence économique, Paris 1996