ECHELON: MENACE OU MODELE POUR L'EUROPE

Mémoire de géopolitique du commandant Thierry Beylier

Dans le cadre du séminaire " Espace aérien et spatial européen "

Directeur : Monsieur Thierry Garçin

Mars 2007

FICHE DOCUMENTAIRE

1. Echelon: menace ou modèle pour l'Europe ?
2. 2007_mémoire_geop_Echelon_Beylier
3. Commandant, Armée de l'Air, BEYLIER Thierry, France
4. 12 mars 2007
5. Division C – groupe C1
6. Mémoire de géopolitique
7. Le réseau Echelon est un système unique d'interception des communications à l'échelle mondiale. Dirigé par les Etats-Unis, depuis 1947, cet outil de maîtrise globale de l'information a beaucoup évolué depuis sa création. Il a su s'adapter et profiter de la révolution des technologies de l'information et des communications pour resserer son emprise sur les réseaux. Depuis 2001, ses priorités opérationnelles ont été ré-orientées vers la guerre contre la terrorisme. Par son aptitude à espionner aussi bien les groupuscules terroristes que les entreprises européennes, ce système constitue t-il une menace ou seulement un risque dont nous sommes libres de nous protéger en développant nos moyens de cryptologie et en préservant nos réseaux nationaux comme un patrimoine stratégique ? Parallèlement, l'étude de ce système montre que c'est un modèle rare de construction d'un service multinational de renseignement, dont l'Union Européenne pourrait s'inspirer pour construire une Europe du renseignement qui fait tant défaut aujourd'hui. Seules la France et l'Allemagne disposent des capacités pour poser les bases solides d'un tel projet, baptisé « Eurechelon » par l'auteur.
8. Echelon, renseignement électronique, UKUSA, ROEM, SIGINT, Eurechelon

SYNTHESE DU MEMOIRE DU CDT BEYLIER

ECHELON : MENACE OU MODELE POUR L'EUROPE

Sous la direction de Monsieur Thierry Garçin, dans le cadre du séminaire « Espace aériens et spatial européen » de la 14° session du Collège interarmées de défense.

Les sujets relatifs à l'espionnage et aux « écoutes » constituent une thématique particulière sur laquelle les médias sont particulièrement prolixes en raison des phantasmes qu'ils génèrent et du mutisme traditionnel des autorités nationales. Le réseau Echelon n'échappe pas à cette règle : il en constitue même un des piliers car il s'assimile aisément dans l'imaginaire collectif à la vision du « big brother » d'Orson Welles.

Qui est donc Echelon ? Quelles sont les capacités avérées de ce système global d'interception des communications de tout type à l'échelle mondiale ? Quelles sont les limitations techniques d'un tel outil ? Rassemblant plusieurs pays anglo-saxons, ce réseau multinational de renseignement d'origine électromagnétique constitue-t-il une menace réelle pour les entreprises européennes en concurrence avec leurs homologues américains ? Enfin, à un moment où l'Europe envisage de se doter d'une capacité autonome d'appréciation de la situation, l'exemple d'Echelon est-il un modèle exportable de construction d'un service multinational de renseignement ?

Parmi les nombreuses publications parues sur l'existence du réseau Echelon, le rapport du parlement européen constitue un document de référence de premier ordre. Depuis sa publication en juillet 2001, plusieurs éléments majeurs sont intervenus et sont susceptibles d'amender l'analyse initiale des capacités de ce système. Les attentats du 11 septembre 2001 ont placé la guerre contre le terrorisme au cœur des priorités américaines et la révolution des technologies de l'information et des communications constitue un enjeu majeur auquel doit faire face un système d'interception.

L'objectif de ce mémoire est de proposer une nouvelle analyse des capacités du réseau et, a contrario, de montrer qu'il constitue un modèle pertinent pour la construction de l'Europe du renseignement.

Qui est Echelon ?

Même si certaines capacités du système sont seulement suspectées mais pas avérées, il est raisonnable d'estimer que les Etats-Unis, ainsi que plusieurs autres nations dont la Grande-Bretagne, ont mis en place à l'échelle mondiale un réseau global d'interception des communications. Ce système est composé de capacités visibles, notamment les nombreux centres d'écoute répartis dans le monde pour intercepter les liaisons descendantes des satellites géostationnaires de télécommunications, mais aussi d'un dispositif particulièrement redoutable de piégeage des routeurs de communications et des serveurs Internet. Ce système porterait le nom de Carnivore.

Toutefois, un service de renseignement peut intercepter une communication sans être capable de l'exploiter. Plusieurs barrières doivent être levées avant d'atteindre le contenu de la communication : le procédé de communication, le cryptage de la communication et la langue utilisée. Pour faire face à ces enjeux majeurs, le réseau Echelon s'intéresse d'avantage aux données techniques de communication, et non au contenu de cette communication : numéros appelé et appelant, lieu du routeur, etc. Ainsi, par ces éléments, le système tente de discriminer les communications suspectes ou douteuses parmi les milliards de celles qui circulent chaque minute sur les réseaux mondiaux.

Menace ou risque pour l'Europe ?

L'étude met en exergue l'importance du réseau Echelon dans la stratégie américaine de maîtrise globale de l'information. Elle met en lumière les capacités avérées d'interception des communications internationales qui peuvent être indifféremment orientées vers la lutte contre le terrorisme ou le renseignement économique. Face à ce risque bien identifié depuis plusieurs années, notamment à travers le rapport d'information du parlement français d'octobre 2000, les Européens sont libres de se protéger des interceptions en se dotant de moyens adaptés de cryptage pour sécuriser leurs communications.

Sur le fond, ces travaux ont montré que les réseaux nationaux de communication appartenaient au patrimoine stratégique d'une nation et que celle-ci avait le devoir de les protéger pour garantir son indépendance. Typiquement, le marché des opérateurs privés de

téléphonie ne doit pas être totalement débridé : la recherche permanente du moindre coût ne doit pas devenir une finalité lorsque l'on traite d'un secteur stratégique.

Modèle pour la construction de l'Europe du renseignement ?

Etudié en temps que modèle de construction d'un système multinational de renseignement, le réseau Echelon constitue un exemple rare de réussite, au même titre que le système Hélios ; ces deux systèmes ayant été construits sur des logiques similaires.

Certaines constances apparaissent : ces systèmes ont été définis sur la base d'une coopération bilatérale ou trilatérale entre pays, puis l'ouverture à d'autres membres a été progressive. Il est important de constater la présence systématique d'un pays « leader » qui assure la maitrise unilatérale du système, même lorsque le système s'ouvre à d'autres pays. Ce point n'est pas anodin car il donne une vision claire des grandes orientations du réseau : ce seront celles de la nation directrice Enfin, la définition d'un objectif stratégique clair est indispensable pour fédérer des énergies et mener à terme des projets si ambitieux dans des domaines qui se prêtent très peu, par nature, à la collaboration inter étatique.

Pour la construction de l'Europe du renseignement, le couple franco-allemand semble être la solution crédible pour initier une telle démarche. La France et l'Allemagne sont les seules nations à disposer d'une expertise dans le domaine du renseignement technique, qui puisse être mise à disposition d'un dessein européen. Une étude sur la définition d'une Europe du renseignement ne peut pas faire l'économie d'une réflexion sur la position britannique, tiraillée entre son engagement européen et sa relation privilégiée avec les Etats-Unis. Membre éminente du réseau Echelon, la Grande-Bretagne ne dispose pas des ressources pour dupliquer ses structures au profit d'un système européen de renseignement.

Synthèse

Finalement, le réseau Echelon constitue un dispositif unique de surveillance électronique mis en place par au moins cinq nations anglo-saxonnes, dont la Grande-Bretagne. Comme tous les dispositifs techniques, il possède plusieurs limitations majeures et des contraintes d'emploi assez lourdes. Toutefois, ce système a su s'adapter à la révolution des

technologies de l'information et des communications pour resserrer son dispositif sur l'ensemble des réseaux et augmenter largement le risque d'interception pour le *quidam*. Outre une menace, il est aussi un modèle pour la construction de l'Europe du renseignement. Paradoxalement, ce sera probablement en s'appuyant sur ce modèle d'organisation que l'Europe se dotera de capacités de renseignement d'origine électromagnétique.

« En Dieu nous croyons, le reste nous l'écoutons »

(Devise officieuse de la NSA)

ECHELON : MENACE OU MODELE POUR L'EUROPE

SOMMAIRE

PREMIERE PARTIE : QUI EST ECHELON ?

Le réseau Echelon : Est-ce un système global d'interception des télécommunications de tout type à l'échelle mondiale ? Quelles sont ses limites ? Quelles sont les capacités réelles du système ?

DEUXIEME PARTIE : MENACE OU MODELE ?

Constitue-t-il une menace ou seulement un risque pour l'Europe ? Est-ce un modèle de coopération réussie ? Quelles leçons pour la construction de l'Europe du renseignement ? Vers un « Eurechelon » ?

Introduction

Les sujets relatifs à l'espionnage et aux « écoutes » constituent une thématique particulière sur laquelle les médias sont particulièrement prolixes en raison des phantasmes qu'ils génèrent et du mutisme traditionnel des autorités nationales. Le réseau Echelon n'échappe pas à cette règle : il en constitue même un des piliers car il s'assimile aisément dans l'imaginaire collectif à la vision du « big brother » d'Orson Welles.

Qui est donc Echelon ? Quelles sont les capacités avérées de ce système global d'interception des communications de tout type à l'échelle mondiale ? Quelles sont les limitations techniques d'un tel outil ? Rassemblant plusieurs pays anglo-saxons, ce réseau multinational de renseignement d'origine électromagnétique constitue-t-il une menace réelle pour les sociétés européennes en concurrence avec leurs homologues américains ? Enfin, à un moment où l'Europe envisage de se doter d'une capacité autonome d'appréciation de la situation, l'exemple d'Echelon est-il un modèle exportable de construction d'un service multinational de renseignement ?

Parmi les nombreuses publications parues sur l'existence du réseau Echelon, le rapport du parlement européen constitue un document de référence de premier ordre. Depuis sa publication en juillet 2001, plusieurs éléments majeurs sont intervenus et sont susceptibles d'amender l'analyse initiale des capacités de ce système. Les attentats du 11 septembre 2001 ont placé la guerre contre le terrorisme au cœur des priorités américaines et la révolution des technologies de l'information et des communications constitue un enjeu majeur auquel doit faire face un système d'interception.

L'objectif de ce mémoire est de proposer une nouvelle analyse des capacités de ce réseau et, a contrario, de montrer qu'il constitue un modèle pertinent pour la construction de l'Europe du renseignement.

Dans une première partie, nous étudierons les capacités du réseau Echelon en soulignant les limitations et ses contraintes. Dans une seconde partie, nous montrerons que ce système constitue une menace auquelle l'Europe est libre de se protéger ou pas. Enfin, si elle doit réduire ses vulnérabilités, l'Europe doit aussi se doter de capacités offensives pour faire face aux nouvelles menaces actuelles. Dans cette logique, le réseau Echelon, en

temps que système multinational de renseignement, constitue un modèle de construction pour l'Europe du renseignement.

PREMIERE PARTIE : QUI EST ECHELON ?

I. 1 Introduction

Dans cette première partie, nous allons montrer que les Etats-Unis disposent, de toute évidence, d'un système d'interceptions des télécommunications à l'échelle mondiale. Après avoir détaillé les procédés pour intercepter les différents supports de transmission, et mis en lumière les limitations techniques incontournables, nous évaluerons les capacités réelles du réseau Echelon avant de proposer quelques pistes pour réduire les vulnérabilités des Européens aux interceptions.

I. 2. Comment fonctionnent les télécommunications ?

Pour comprendre les méthodes d'interception d'une télécommunication, il est nécessaire de faire l'inventaire des différents supports de transmission et de les décrire sommairement en soulignant les contraintes techniques et physiques de chacun. Une analyse détaillée est présentée en annexe.[1]

I. 2.1 Les différents types de communications

Que ce soit un courrier électronique, un fax ou un appel téléphonique, une télécommunication transite toujours par une succession de supports de transmission de différentes natures :

- les liaisons hertziennes de proximité : ce sont traditionnellement les communications radio par onde directe utilisées par les forces armées et l'aviation civile, mais aussi les différentes solutions pour raccorder des équipements mobiles (téléphone mobile, sans fil, etc.) au réseau fixe,
- les faisceaux hertziens : ce sont des liaisons directives entre deux antennes positionnées en face en face à une distance de plusieurs

[1] Annexes A.1 à A.6

kilomètres. Elles sont utilisées dans les réseaux d'infrastructure pour s'affranchir de l'installation d'une liaison filaire,

- les liaisons HF[2] : ce sont des liaisons radio, en ondes décamétriques, permettant des communications à très longue distance, de l'ordre de plusieurs milliers de kilomètres,
- les câbles sous-marins : ils sont utilisés pour les liaisons intercontinentales,
- les liaisons filaires : elles regroupent l'ensemble des liaisons terrestres utilisant un support filaire : réseau en fibre optique, ligne téléphonique en cuivre, etc.,
- les liaisons par satellite : apparues au début des années 80, ce sont l'ensemble des liaisons qui utilisent un satellite pour assurer un relais de communication entre deux points sur Terre.

Enfin, il est important de citer les « routeurs » : ce sont les ordinateurs disposés aux nœuds du réseau et qui décident du transport des paquets de données.

I. 2.2 La circulation de l'information

Contrairement à l'idée reçue, une communication entre un point A et un point B ne transite pas par le chemin le plus court mais par le chemin le moins cher. En effet, les opérateurs de téléphonie obéissent à une logique financière de recherche systématique du trajet le plus économique. Pour une communication téléphonique utilisant les procédés traditionnels, par opposition à celle par Internet, le trajet effectué par la communication sera le même pendant toute sa durée. En revanche, pour un courrier électronique, l'opérateur gère dynamiquement les routeurs de manière à optimiser en temps réel le coût des télécommunications.

Dans cette logique, l'importance des câbles sous-marins est primordiale car ces supports, capables de très haut débit, sont largement sous-utilisés. Ainsi, par la loi de l'offre et de la demande, il peut être plus rentable pour un opérateur de faire transiter une communication

[2] HF : high frequency. La gamme HF recouvre les fréquences entre 3 et 30 Mhz

Alger-Londres par les Etats-Unis, via un câble sous-marin, que de passer par le réseau terrestre français.

En termes d'interception, cet état de fait pose deux difficultés majeures :

- il est très difficile de prédire le trajet que va emprunter une communication longue distante, sauf bien entendu s'il existe une solution unique pour joindre les deux points. Pour mener une interception, il est nécessaire de rechercher le support principal sur lequel circulent les communications de la « cible »,
- une communication entre deux points du territoire national peut transiter par l'étranger : cette possibilité, parfaitement réaliste, est contraire aux idées reçues et les précautions prises lors d'une communication internationale ne le sont pas sur une communication nationale, qui en fait présente aussi des risques d'interception.

Enfin, les communications par satellite étant d'un coût exorbitant par rapport à celles transitant par câbles sous-marin, elles sont principalement utilisées pour communiquer avec les régions les moins développées et celles en crise.

I. 2.3 Les évolutions en cours

Le monde des nouvelles technologies de l'information et des communications évolue sans cesse. Les principales évolutions en cours qui ont un impact majeur sur les interceptions sont la téléphonie par internet et la banalisation des faisceaux étroits, ou « spot beam[3] », pour les services mobiles.

La téléphonie par Internet :

Le principe repose sur une numérisation de la voix, appelée vocodage, et la transmission en temps réel des données numérisées. Ainsi, cette voix numérisée est décomposée en petits paquets de données, comme n'importe courrier électronique. Selon la logique propre

[3] Cf. Annexe A.6 sur les différents types de couverture

à Internet, chaque paquet de données suit son propre chemin, indépendamment des autres, pour atteindre le serveur cible. Comme nous l'avons rappelé précédemment, la seule logique qui guide le choix du trajet de chaque paquet est économique. Ainsi, dans une communication téléphonique par Internet, les propos échangés utilisent une multitude de trajets différents. La seule solution pour intercepter la totalité de la communication sera d'agir à proximité de l'un des deux correspondants ou, le cas échéant, sur un segment de liaison incontournable. En revanche, le trajet emprunté par une communication téléphonique classique est le même durant toute la durée de l'appel.

Les évolutions sur les satellites géostationnaires de télécommunications mobiles:

Les récentes évolutions technologiques sur les antennes en bande L[4] permettent maintenant à un satellite de service mobile de générer simultanément près de deux cents lobes étroits, appelées « spot beam », de communications. Les premiers satellites à disposer d'une telle capacité sont ceux du système Thuraya. Elle est maintenant disponible sur la quatrième génération de satellite Inmarsat, dont deux sont déjà en orbite. La banalisation des zones de couverture étroite va imposer un problème structurel aux services d'interception. Par le passé, avec des satellites géostationnaires n'utilisant que des couvertures globales[5], un service devait disposer de trois ou quatre centres d'écoute bien repartis sur le globe pour intercepter la quasi-totalité des communications transitant par des satellites géostationnaires. Maintenant, avec la réduction de la taille des zones de couverture, il est nécessaire de multiplier les centres d'interception ou de se doter de satellites d'interception. Comme nous le verrons ultérieurement, cet état de fait pose singulièrement la question de l'avenir des grands centres fixes d'interception des communications mobiles par satellite.

I. 3 Un système d'interception à l'échelle mondiale ?

I. 3.1 Quelques contraintes de l'interception

L'explosion des nouvelles technologies de l'information et des communications a banalisé l'usage de systèmes civils reposant sur des procédés numériques de transmission

[4] Cf. Annexe A.6 sur les différentes gammes de fréquence
[5] Cf. Annexe A.6 sur les différents types de couverture

très variés et d'une grande complexité technique, qui n'a parfois rien à envier aux techniques de cryptage. L'interception de ces nouveaux types de communication exige de disposer d'une expertise de haut niveau pour décortiquer ces procédés complexes et programmer rapidement les outils adaptés d'écoute. Un tel savoir-faire ne s'acquiert qu'au prix d'un investissement humain et financier important et continu, que seules quelques nations peuvent s'offrir.

Le développement d'Internet et des nouveaux modes d'échanges a amené les états à libéraliser progressivement les logiciels de cryptage, jusqu'alors réservés aux usages gouvernementaux. La banalisation de l'emploi de ces outils constitue certainement le second défi majeur auquel les services de renseignement électronique doivent faire face. En effet, cette déréglementation a eu un effet de boite de Pandore puisqu'une multitude d'applications, notamment en accès libre sur Internet, est rapidement apparue. La plupart des systèmes civils offre maintenant des fonctions de sécurité pour garantir la protection des informations. La banalisation du cryptage impose donc aux services de renseignement de disposer d'une capacité de décryptage pour "casser" ces algorithmes et accéder au contenu des communications interceptées.

En théorie, par son statut d'extra-territorialité, une ambassade pourrait être une plate-forme accueillant des moyens d'écoute pour les communications à courte distante et les faisceaux hertziens. Toutefois, il est important de souligner qu'une ambassade constituant un élément de représentativité, il est très difficile d'y installer un tel dispositif pour plusieurs raisons :

- un dispositif d'interception est souvent visible. De plus, il est nécessaire d'y adjoindre des moyens de communications supplémentaires pour rapatrier les données interceptées vers un centre d'analyse,
- un tel dispositif, s'il était détecté, constituerait une manœuvre agressive à l'égard du pays hôte,
- seules les émissions transitant à proximité de l'ambassade peuvent être interceptées. Les possibilités d'interception sont, de fait, assez réduites. Pour la nation hôte, ce serait une grave erreur que de faire passer un faisceau hertzien stratégique au dessus d'une ambassade,
- un tel dispositif peut aisément être brouillé par la nation hôte.

Enfin, le problème de la traduction est crucial, notamment dans les langues rares (persan-farsi, Wolof, dari-pachto, dialectes arabes, etc.). Cela exige des services de renseignement d'avoir une véritable politique de ressources humaines en matière de linguistes en langue rare, tout en prenant en compte les contraintes de sécurité (risque d'infiltration, fiabilité, etc.).

I. 3.2 l'interception des liaisons hertziennes de proximité

L'interception de ce type de communication de courte portée exige que le dispositif d'écoute soit dans la zone de réception de l'émetteur, c'est-à-dire à moins de 100 km dans le meilleur des cas. La seule possibilité technique est de mener une interception depuis le territoire adverse ou depuis la frontière (ou les eaux territoriales) : A l'exception des possibilités offertes par une ambassade, dont les limitations ont déjà été soulignées, seul un bateau en limite des eaux territoriales, un avion ou un drone de guerre électronique ou un satellite en orbite basse peut mener une telle opération, par essence ponctuelle.

Dans ce cas, seules quelques interceptions sur des objectifs bien ciblés et dans des zones adaptées sont possibles. En conclusion, l'existence d'un système mondial d'interception capable de prendre en compte l'ensemble des liaisons hertziennes de proximité n'est pas techniquement possible.

I. 3.3 l'interception des faisceaux hertziens

L'interception d'un faisceau hertzien (FH) exige que le dispositif d'écoute soit installé à proximité de la liaison. De plus, les FH étant généralement destiné à faire transiter des débits très élevés, l'intercepteur devra assurer, en toute discrétion, le rapatriement des données interceptées. La problématique de ce type d'interception est finalement assez proche de celle des liaisons hertziennes de proximité : s'approcher de l'émetteur puis retransmettre les données recueillies.

En conclusion, à l'instar du cas des liaisons hertziennes de proximité, l'existence d'un système mondial d'interception capable de prendre en compte l'ensemble des faisceaux hertziens n'est techniquement pas possible.

I. 3.4 l'interception des liaisons HF

Par constitution, les liaisons HF sont destinées à transmettre à très longue distance, plusieurs milliers de kms. Certes, l'émission est directive mais sur de telles distances, le cône de dispersion devient très important.

En conséquence, à partir de quelques centres fixes d'écoute bien repartis dans le monde, il est techniquement possible de disposer d'un système mondial d'interception des liaisons HF.

I. 3.5 l'interception des câbles sous-marins

A l'époque des câbles électriques, il était techniquement possible, par induction, d'interception les signaux morses transitant sur ces supports. De nombreuses informations circulent dans la presse sur une interception menée à partir d'un sous-marin américain sur un câble russe. Toutefois, le problème du rapatriement des données se pose de manière assez cruciale si l'interception est menée depuis un sous-marin.

Maintenant, les câbles sous-marins sont constitués de fibre optique et les répétiteurs sont en laser à l'erbium. Dans l'état actuel des connaissances sur l'interception des fibres optiques, il n'est pas possible de mener une telle opération. La seule solution pour intercepter un câble sous-marin moderne est de disposer d'un accès à l'opérateur. Dans ce cas, il s'agit d'une interception de sécurité, car le support de transmission est coopératif.

En conséquence, l'existence d'un système mondial d'interception capable de prendre en compte, de façon non coopérative, l'ensemble des câbles sous-marins n'est pas techniquement possible. En revanche, par un accès autorisé, son intégration dans un système complet est parfaitement envisageable.

I. 3.6 l'interception des liaisons filaires

L'interception non-coopérative d'une liaison filaire exige d'utiliser des moyens clandestins très difficiles à mettre en œuvre et qui ne peuvent, bien entendu, pas être généralisés.

En conséquence, l'interception systématique des liaisons filaires exige de bénéficier d'un cadre juridique adapté dans chaque pays. Toutefois, il est important de souligner qu'un système qui permet d'intercepter systématiquement les communications d'un pays, permet aussi d'intercepter les communications transitant seulement par ce pays.

Toutefois, l'arrivée des opérateurs privés de téléphonie et les principes de la libre concurrence pourraient constituer une nouvelle faille. Ces opérateurs sont tenus par des exigences de service. Ainsi, rien ne peut les interdire de vouloir faire transiter les communications dont ils ont la charge par un pays tiers disposant d'une législation permettant une interception systématique des communications.

I. 3.7 l'interception des liaisons par satellite

Une communication transitant par satellite entre deux individus A et B est composée de quatre liaisons : une liaison montante et une descendante entre A et le satellite et autant entre B et le satellite. Toutefois, en termes de renseignement, les propos émis par A peuvent être indifféremment interceptés sur la liaison montante entre A et le satellite ou sur la liaison descendante entre le satellite et B.

Il est aisé de comprendre qu'il est techniquement beaucoup plus simple d'intercepter une liaison descendante qu'une liaison montante. Pour la liaison descendante, il suffit de se situer dans la zone de couverture. L'interception de la liaison montante exige soit de se situer à proximité de l'antenne d'émission, ce qui pose de nombreuses contraintes de sécurité, soit de disposer d'un satellite d'écoute. En conséquence, pour intercepter les deux sens d'une communication entre A et B, il est nécessaire d'intercepter les deux liaisons descendantes. Si ces liaisons transitent par des faisceaux satellitaires différents, qui n'ont pas la même zone couverture, il peut être nécessaire d'utiliser deux centres d'écoute.

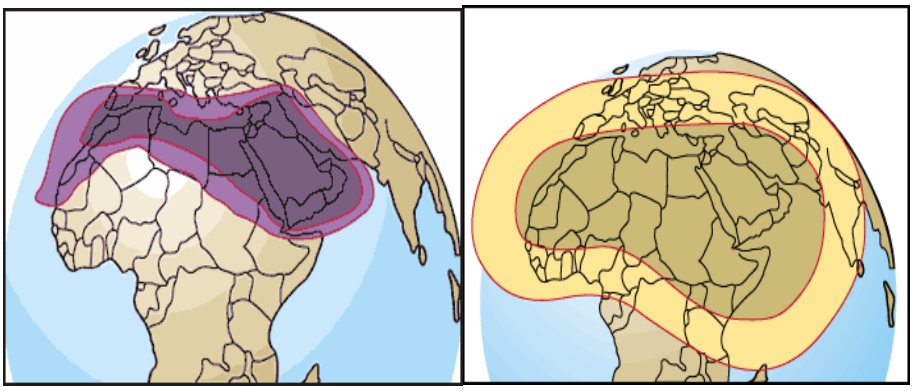

Figure : couverture Arabsat 2B (bande Ku à gauche, bande C à droite).

Site www.arabsat.com

Toutefois, il n'est pas indispensable de se situer exactement dans la zone de réception pour intercepter la liaison. En effet, en s'écartant progressivement de cette zone, la puissance du signal, appelée Puissance isotrope rayonnée équivalente (PIRE), diminue. Elle n'est plus suffisante pour être utilisée avec l'antenne de réception fournie par le distributeur. En revanche, la baisse de puissance peut être compensée par l'augmentation de la taille de l'antenne d'interception. C'est pour cette raison que les antennes paraboliques d'interception sont généralement de très grand diamètre.

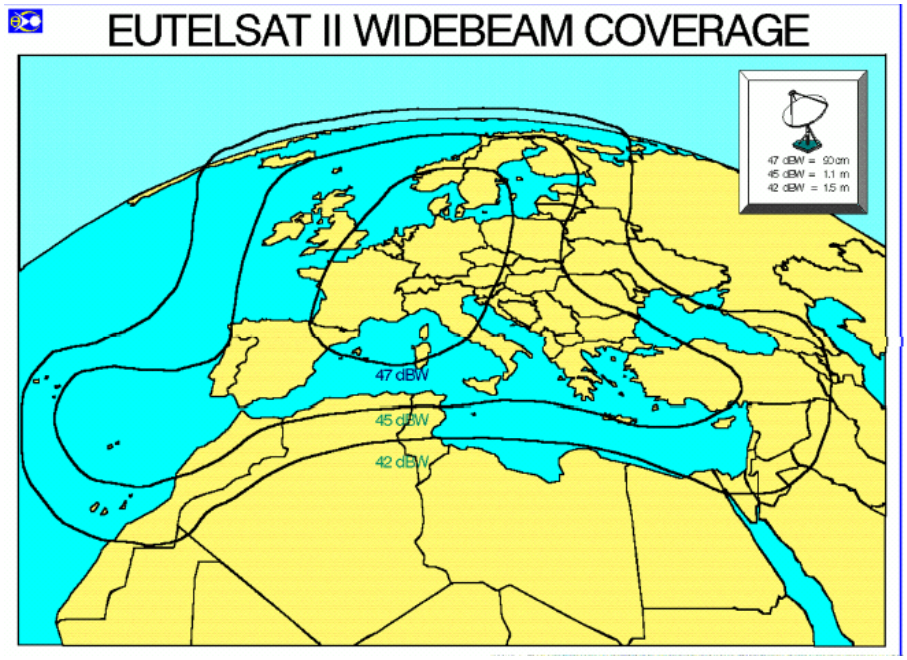

Figure : elle montre le lien entre la diminution de la puissance du signal (exprimée en dB) et le diamètre de l'antenne de réception (dans le cadre en haut à droite du schéma)

Site www.eutelsat.com

Parallèlement, les zones de couverture des satellites se réduisent afin de concentrer les signaux sur la région concernée. Typiquement, l'évolution de la couverture de la liaison en bande L[6] du système Inmarsat illustre bien cette règle :

- les satellites de 2° génération avaient une couverture globale,
- les satellites de 3° génération ont une couverture zonale (5 à 6 faisceaux),
- les satellites de 4° génération utilisent des « spot beam » (près de 200 par satellite)

En termes d'interception, cela signifie qu'il était nécessaire de disposer d'un seul centre d'écoute pour intercepter un satellite de 2° génération. Il en faut 2 ou 3 pour un satellite de 3° génération (Cf. figure). Il faudra certainement une dizaine pour la 4° génération (deux satellites de ce type sont déjà en service).

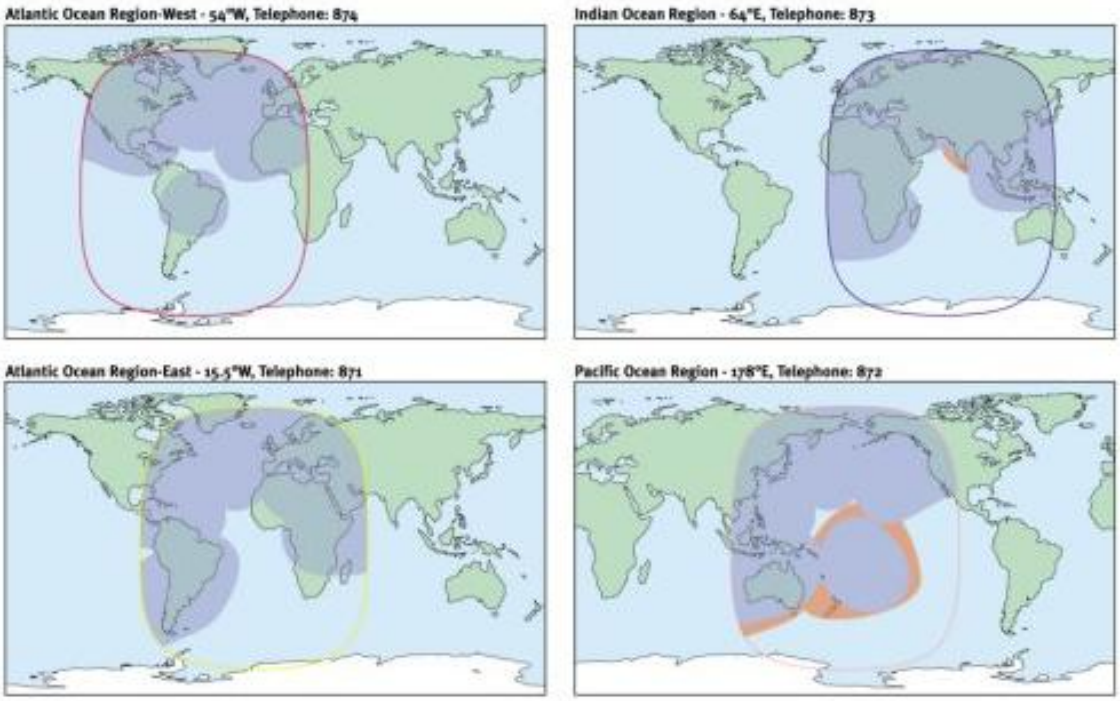

Figure : En bleu foncé, pour chaque satellite de 3°génération, sont représentées les zones de réception des valises Inmarsat. Elles sont l'union des 5 ou 6 couvertures zonales.
Site www.inmarsat.com

[6] La liaison en bande L relie le mobile au satellite. La liaison entre la station terrestre fixe et le satellite s'effectue en bande C.

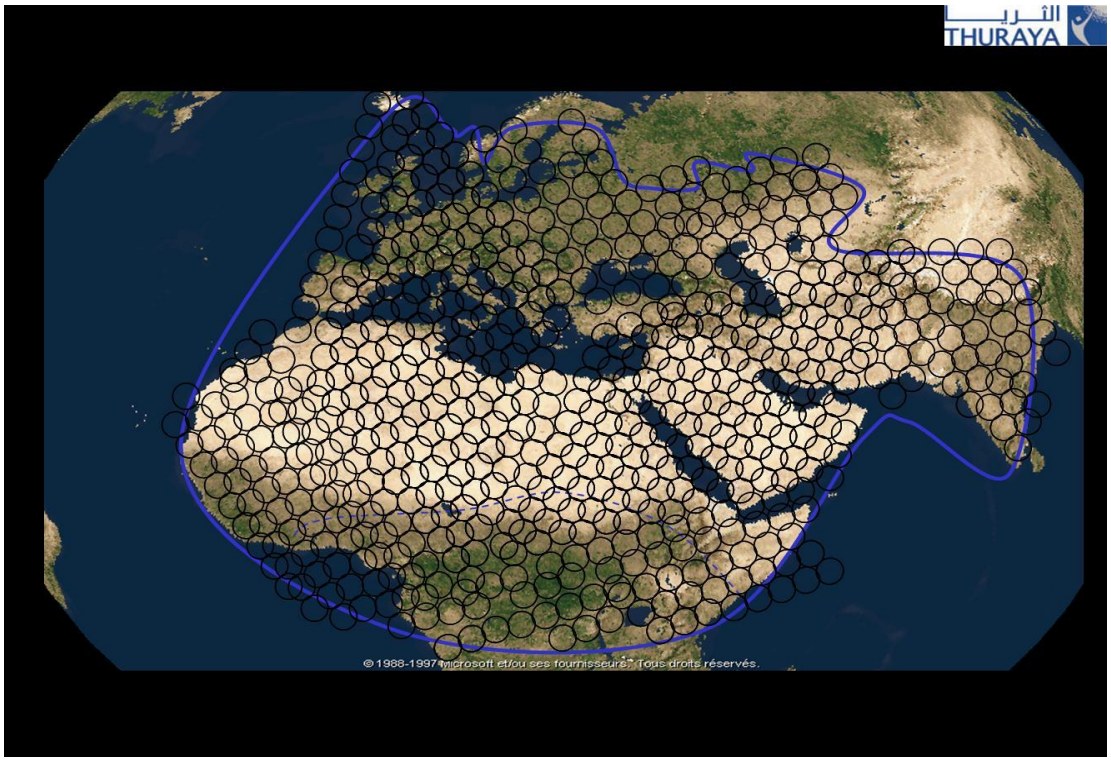

Figure : Les « spot beam » de Thuraya. Chaque cellule a un diamètre de l'ordre de 200km. Site www.thuraya.com

Enfin, une dernière alternative existe pour intercepter les communications par satellite : le satellite d'écoute. Schématiquement, un tel satellite est composé d'une ou plusieurs antennes d'interception des liaisons satellitaires montantes et d'une antenne de rediffusion des données interceptées vers une station sol. Au regard du coût et des contraintes de maintien à poste d'un satellite, quel est l'intérêt d'une telle solution par rapport à un centre d'écoute ? Typiquement, si la zone de couverture des liaisons descendantes n'est pas accessible pour y installer un centre d'écoute ou si ce satellite génère un nombre trop important de lobes étroits (« spot beam »), un satellite d'écoute, positionné à proximité d'un satellite de télécommunication, peut être la seule solution pour intercepter les communications que celui-ci fait transiter.

En conséquence, l'existence d'un système mondial d'interception capable de prendre en compte l'ensemble des communications transitant par satellite est techniquement possible, sous réserve de disposer des points d'appui (centres d'écoute judicieusement réparti sur la terre) ou de satellites d'interception. Toutefois, en raison de l'évolution des capacités des satellites de téléphonie mobile, un tel système aura deux alternatives pour assurer sa pérennité : multiplier rapidement le nombre de centre d'écoute et développer des capacités

mobiles d'interception pour se rapprocher des « cibles » ou se doter de capacités spatiales d'interception. A défaut, un accès autorisé, par interception coopérative, à ces réseaux mobiles permettrait de résoudre cette problématique.

I. 3.8 l'interception sur les routeurs et les serveurs Internet

L'installation de dispositifs adaptés d'interceptions systématiques des données transitant sur un réseau pourrait constituer un pilier central d'un système de surveillance à l'échelle mondiale. La mise en place d'un tel dispositif ne constitue pas un défi majeur technique, comme le montre le nombre de sociétés qui exposent chaque année, lors du salon MILIPOL de la sécurité, des dispositifs d'interception coopérative à installer sur les nœuds des réseaux.

En contrôlant des routeurs majeurs ou les principaux centres serveurs Internet, un pays dispose d'une capacité de surveillance de l'ensemble des communications régionales. Dans un souci de réduction des coûts, certains opérateurs installent leur serveur à l'étranger. Ainsi, de nombreux pays ne disposent pas de centres serveurs majeurs, ce qui signifie que l'ensemble de la messagerie émise depuis ces pays transitent systématiquement par l'étranger. Dans ce domaine, il est important de constater que les Etats-Unis hébergent près de 80%[7] des centres serveurs Internet.

Enfin, il est important de signaler que ce type d'interception est particulièrement redoutable pour plusieurs raisons :

- les interceptions sont systématiques,
- ces dispositifs ne sont pas physiquement visibles, contrairement aux centres d'écoute,
- ils permettent d'obtenir la maitrise quasi complète de l'information sur une zone donnée,
- ils ne sont pas aisément détectables.

[7] Source UIT (Union internationale des télécommunications)

I. 3.9 les difficultés de l'exploitation

Comme cela a été décrit au paragraphe I.3.1, il est important de séparer l'interception de l'analyse. Un service de renseignement peut intercepter une communication sans être capable de l'exploiter. Plusieurs barrières doivent être levées avant d'atteindre le contenu de la communication :

- le procédé de transmission : la modulation utilisée pour transmettre les données. Elles deviennent de plus en plus complexes à décortiquer,
- le cryptage des informations : de plus en plus de systèmes civils de téléphonie cryptent les communications afin de se protéger des interceptions clandestines,
- la langue et les dialectes.

Ce dernier élément reste un point bloquant à la mise en place d'un système global d'interception et d'analyse des communications à l'échelle mondiale. La traduction systématique des communications vocales interceptées n'est pas concevable, faute de systèmes automatiques fiables. Il est donc encore nécessaire de faire appel à l'Homme. En revanche, il est techniquement concevable d'imaginer des logiciels automatiques de tri des courriers électronique, filtrant les messages selon les mots utilisés.

Toutefois, il reste encore possible de tirer de nombreux renseignements de l'interception d'une communication sans nécessairement la décrypter ou la traduire. En effet, l'analyse des données techniques de transmission est particulièrement intéressante : les numéros de téléphone appelé et appelant, ou les adresses électroniques le cas échéant, le lieu de l'appel (ou du routeur le plus près), la date, etc. L'exploitation de ces éléments permet de définir le cercle des relations professionnelles et personnelles de l'intéressé, de savoir qui dialogue avec qui, quand, etc.

Un système global d'interception des communications, s'il existe, serait composé de deux volets : une analyse systématique des paramètres techniques de toutes les communications interceptées et une analyse approfondie (décryptage, traduction, exploitation) des communications classées « douteuses » ou « hostiles »[8].

[8] Pour reprendre la classification utilisée dans le cadre de la sûreté aérienne.

I. 3.10 Synthèse sur la possibilité technique d'un système global d'interception

Ainsi, la possibilité technique d'un système mondial d'interception des communications au profit d'un ou plusieurs pays est avérée pour celles transitant par satellite ou en gamme HF, sous réserve de disposer des emprises géographiques ou de capacités spatiales de recueil.

Un tel système ne peut techniquement pas mener des interceptions non-coopératives sur les liaisons hertziennes de proximité, les câbles sous-marins, les faisceaux hertziens ou les liaisons filaires. L'accès aux communications transitant par ces supports exige de pouvoir accéder physiquement à ces réseaux. Un pays maitrisant ses réseaux nationaux de communication peut se prémunir aisément de ce type d'interception par un pays tiers.

Enfin, en raison de la quantité pharaonique de communications à analyser, seul un système d'analyse automatisée des paramètres techniques de communication est envisageable ; seules les communications téléphoniques répondant à certains critères de risque (numéros surveillés, etc.) étant traduites.

I. 4 Qui est Echelon ?

I. 4.1 Un système multinational COMINT[9]

L'origine du réseau Echelon est le pacte secret « UKUSA agreement » signé en 1947 par les Etats-Unis et la Grande-Bretagne puis élargi ultérieurement au Canada, la Nouvelle-Zélande et l'Australie. L'objectif premier de ce pacte était de mettre en place un réseau de recueil COMINT tourné vers le Pacte de Varsovie.

Ce pacte a survécu à l'effondrement du bloc de l'est. D'un objectif militaire bien ciblé, ce réseau a évolué vers un système de recueil stratégique face aux nouvelles menaces. De plus, il semblerait que de nouveaux pays aient rejoint le réseau Echelon. Le cas de la

[9] COMINT (Communication intelligence) : renseignement tiré de l'interception des communications

Pologne est cité, notamment par Monsieur Alain Juillet, Haute autorité chargée de l'intelligence économique auprès du Secrétariat général de la Défense nationale (SGDN).

Cependant, peu d'informations fiables circulent sur le fonctionnement du réseau et notamment le degré de collaboration entre les états membres. L'hypothèse la plus probable serait une maitrise unilatérale du réseau par les Etats-Unis. Les autres pays membres seraient répartis en deux catégories :

- *les nations de « premier cercle » :* ce sont certainement les pays anglo-saxons liés par une « special relationship » à l'instar des Britanniques. Ces pays mènent eux-mêmes leurs interceptions, probablement avec du matériel américain, et alimentent le réseau Echelon. En retour, le réseau leur fournit les interceptions menées par les autres pays et concernant leurs sécurité nationale. Dans ce cas, Echelon est un réseau multinational « Comint »,
- *les nations du « deuxième cercle » :* celles-ci mettent à disposition des Etats-Unis des emplacements pour y installer des centres d'écoute et autorisent l'accès à leur réseau national de communication. En contrepartie, le réseau Echelon leur fournit du renseignement démarqué[10] intéressant leur sécurité nationale. Dans ce cas, il s'agit plus de l'application du principe de subsidiarité.

I. 4.2 Le système Carnivore : la partie immergée

Pour intercepter les communications nationales américains et les courriers électroniques, les Etats-Unis ont développé un système particulièrement redoutable : CARNIVORE. Ce système se raccorde directement sur les serveurs Internet des fournisseurs d'accès et les routeurs et fonctionne comme une boite noire : il filtre toutes les informations qui y circulent sans que l'opérateur puisse connaitre le fonctionnement du dispositif. Programmé directement en ligne par les services de sécurité américains, il permet de réagir très rapidement.

[10] Terme utilisé pour signifier que le renseignement transmis ne dévoile pas la source

L'existence de Carnivore a été révélée par le *Wall Street Journal* en juillet 2000 à la suite de révélations de l'avocat du fournisseur d'accès Internet « Earthlink ». En 1999, le FBI aurait installé sur les serveurs de cette société un système de surveillance des courriers électroniques.

Un tel outil est particulièrement redoutable à l'échelle mondiale, même s'il n'est implanté qu'aux Etats-Unis, car la grande majorité des serveurs Internet sont installés dans ce pays. En mettant en place un système de surveillance à usage national, les Etats-Unis disposent de fait d'un système qui permet de surveiller l'ensemble des courriers électroniques qui transitent par ce pays. D'un point de vue législatif, la loi américaine est très protectrice des libertés des citoyens américains. En revanche, elle autorise l'interception systématique des communications des non-américains.

I. 4.3 Les principales publications

La principale publication de référence sur le réseau Echelon est le rapport du parlement européen publié le 11 juillet 2001. Ce rapport est particulièrement exhaustif et repose sur une analyse scientifique pertinente. Toutefois, publié avant septembre 2001, il ne prend pas en compte le revirement stratégique des Etats-Unis qui a certainement eu un impact majeur sur Echelon. Comme l'ont souligné plusieurs parlementaires, ce rapport élude la question de la participation de la Grande-Bretagne, membre de l'Union européenne, à ce réseau.

Précédemment, le rapport d'information du parlement français du 11 octobre 2000 était une des premières publications officielles d'un état sur la menace que constitue le réseau Echelon pour les libertés individuelles. Toutefois, ce rapport, publié lui aussi avant septembre 2001, souffre de deux lacunes : l'absence de base scientifique pour étayer son analyse des capacités et la faible coopération des services français de renseignement, souligné par son rapporteur Monsieur Arthur Puecht. En revanche, il souligne l'importance de développer des moyens de cryptologie pour se prémunir des écoutes.

En outre, de nombreuses publications anglo-saxonnes existent sur le sujet. Les plus complètes sont celles du journaliste britannique Duncan Campbell dont le premier article sur Echelon date de 1988.

I. 4.4 L'analyse objective des capacités

Un certains nombre d'éléments permettent de mener une analyse objective des capacités du réseau Echelon. Typiquement, une étude détaillée des clichés des grands centres d'écoute permet de déterminer le nombre de satellites interceptés et éventuellement de déterminer le satellite visé. En effet, les antennes d'interception sont de grandes paraboles pointées dans la direction du satellite écouté. La mesure de l'angle de pointage permet d'en déduire la position orbitale du satellite visé. De plus, une antenne intercepte une seule liaison satellitaire descendante. Toutefois, dans un souci de discrétion et de protection contre les intempéries, ces antennes sont parfois installées sous des radomes. L'analyse des zones de couverture des satellites, fournit par les sociétés de télécommunications, permet aussi d'estimer sans trop de risque d'erreurs la famille de satellites concernée.

Figure : Antennes d'interception des liaisons descendantes des satellites de communications en orbite géostationnaire. Site www.arpege-defense.com (société française de vente de matériels de guerre électronique)

En revanche, il est impossible de mener une analyse objective des capacités réelles du réseau Echelon en matière d'interception coopérative sur les routeurs, serveurs internet, câbles sous-marin, liaisons filaires, etc. Toutefois, il est important de souligner que depuis les attentats de septembre 2001 les Américains et les Britanniques ont mis en place des

législations très dures en matière de lutte contre le terrorisme, autorisant le contrôle des serveurs Internet ainsi que de tous les moyens de communications. Enfin, il n'est inutile de rappeler que les câbles sous-marins transatlantiques aboutissent tous en Grande-Bretagne, membre du réseau Echelon.

I. 4.5 Conclusion : synthèse sur la réalité du réseau Echelon

Même si certaines capacités du système sont suspectées mais pas avérées, il est raisonnable d'estimer que les Etats-Unis, ainsi que plusieurs autres nations, ont mis en place à l'échelle mondiale un réseau global d'interception des communications. Ainsi, les capacités visibles d'écoute, représentées par les centres d'interception des communications par satellite ou en gamme HF, ne doivent pas masquer la volonté américaine, affirmée ouvertement depuis 2001, d'avoir une maitrise totale de l'information. Dans cet esprit, le développement de capacités légales de contrôle de tous les réseaux est logique. L'existence de Carnivore est parfaitement crédible.

Globalement, en termes de maitrise du risque, la synthèse pourrait être la suivante :

- le risque est maximal pour toutes les communications internationales,
- le risque est maximal pour tous les courriers électroniques et la téléphonie par Internet dans tous les cas, même si l'expéditeur et le destinataire ont le même fournisseur d'accès ou s'ils résident sur le même territoire,
- le risque n'est pas maitrisé pour les communications nationales (voix ou fax) transitant par un opérateur étranger de téléphonie,
- le risque est très faible pour les communications nationales (voix ou fax) transitant par un opérateur national fiable.

DEUXIEME PARTIE : MENACE OU MODELE ?

II. 1 Echelon : une menace ou seulement un risque pour l'Europe ?

II. 1.1 Un risque dont nous sommes libres de nous protéger !

Pour démontrer que le réseau Echelon constitue une menace pour l'Europe, il est nécessaire de montrer que celui-ci dispose de capacités de nuisance et que son intention est agressive. A défaut, si l'intention n'est pas démontrée, il ne constituerait qu'un risque.

Le principal dilemne soulevé par les rapports des parlements européens et français sur Echelon est son utilisation à des fins de renseignement économique pour soutenir les entreprises américaines en concurrence avec des sociétés européennes. Sur cette problématique, il est indéniable d'affirmer que le réseau Echelon dispose des capacités pour intercepter, par exemple, les communications ou les courriers électroniques émis par un dirigeant français d'un grand groupe industriel de Défense à destination d'un haut fonctionnaire d'un pays du Moyen-Orient. L'interception sera d'autant plus facile que la liaison ne sera pas cryptée et que l'origine du message sera aisée à reconnaitre (préfixe téléphonique du central du siège de la société, identification du serveur de la société, etc.).

Quant à l'intention agressive, elle est inutile à démontrer. Ce serait faire preuve de beaucoup d'angélisme que de penser que la compétition économique obéit à des règles strictes d'honnêteté et d'équité. A contrario, l'argumentation américaine pour défendre l'existence de ce réseau est claire :

- lutter contre les pratiques commerciales déloyales,
- certains pays, comme la France ou l'Allemagne, disposent de capacités similaires d'interception.

Face à cette situation, les Européens ne sont pas désarmés. Dès octobre 2000, le rapport du parlement français soulignait l'importance de se protéger contre les interceptions et proposait des pistes.

Globalement, il faut retenir que le réseau Echelon n'est qu'une forme moderne d'espionnage, comme il y en a toujours eu dans l'histoire. De même que nos ennemis ou

nos adversaires se protègent de nos actions de renseignement, c'est à nous de nous protéger du réseau Echelon en réduisant nos vulnérabilités.

II. 1.2 Réduire nos vulnérabilités

Pour l'usager, le seul et unique moyen de protéger efficacement ses communications (voix, fax, courrier électronique, etc.) est de les crypter avec un moyen fiable national. La France fait partie des rares pays à disposer d'une forte expertise en cryptologie et d'une maitrise complète de la chaine de production de moyens de chiffrement : de la fonderie étatique pour créer les composants électronique aux sciences mathématiques. Toutefois, un important effort de sensibilisation à la sécurité des communications reste encore à mener en France et en Europe.

Les communications font partie du parti du patrimoine stratégique d'un Etat qu'il a le devoir de préserver, même dans une dynamique générale d'externalisation et d'ouverture à la concurrence. Typiquement, le marché des opérateurs privés de téléphonie ne doit pas être totalement débridé : la recherche permanente du moindre coût ne doit pas devenir une finalité lorsque l'on traite d'un secteur stratégique. L'Etat doit introduire des clauses de sécurité de l'information, conformes à l'intérêt national, et mettre en œuvre des moyens de contrôle et une politique coercitive pour ceux qui y dérogent. Par exemple, les opérateurs devraient s'engager à héberger l'ensemble des moyens (routeurs, serveurs, etc.) sur le territoire national et ne pas faire transiter les communications nationales par l'étranger même si ces solutions sont économiquement plus rentables.

Enfin, dans le domaine des logiciels, il est nécessaire de favoriser l'éclosion des logiciels libres d'origine européenne. Il ne s'agit pas de tomber dans la psychose du « big brother » américain ni de voir systématiquement des collusions entre la NSA et les sociétés américaines de télécommunications mais simplement de pouvoir conserver sa liberté d'action dans un domaine éminemment stratégique.

II.2 Un modèle de coopération réussie

II.2.1 Un domaine peu disposé aux coopérations

Le renseignement d'origine électromagnétique (ROEM) est certainement le domaine le plus sensible du renseignement par les mesures permanentes prises pour protéger les sources de recueil. Ce principe fondateur de protection des sources est un frein à toute forme de collaboration entre les services d'un même pays et, a fortiori, entre services étrangers. Dans cette logique, commune à toutes les nations, la création d'un réseau de renseignement d'origine électromagnétique commun à plus de cinq nations est une réussite assez unique. Elle mérite d'être analysée finement pour en tirer éventuellement des leçons dans le cadre de la montée en puissance d'une « Europe du renseignement ».

II.2.2 L'analyse de cette coopération

Globalement, l'analyse de la montée en puissance du réseau Echelon montre qu'elle a obéit à trois règles fondamentales :

- une construction progressive à partir d'un « couple fondateur » solide : les Etats-Unis et la Grande-Bretagne. L'ouverture aux autres pays a eu lieu progressivement,
- un objectif commun initial : le Pacte de Varsovie. Depuis le 11 septembre 2001, un nouvel objectif stratégique est aussi clairement identifié : la guerre contre le terrorisme,
- Un pays « leader » : les Etats-Unis. Ce dernier point est très important car ce choix donne une visibilité politique et stratégique claire : les grandes priorités sont celles des Etats-Unis.

Il est intéressant, par analogie, d'analyser les facteurs de réussite du système multinational d'observation par satellite Hélios :

- le système Hélios 1 est une coopération trilatérale entre la France, l'Italie et l'Espagne. Son successeur Hélios 2 regroupe au moins six pays : la France, l'Allemagne, l'Italie, l'Espagne, la Grèce et la Belgique,

- l'objectif commun stratégique était de se doter d'une capacité autonome d'appréciation de la situation, distincte des Etats-Unis,
- un pays « leader » : la France. Sur Hélios 1, la France détenait 74% du programme. Sur Hélios 2, la France continue de conserver la maitrise stratégique du système.

Bien que ces systèmes soient radicalement différents, il est intéressant de souligner certaines constances communes à la mise en place de réseau multinationaux de renseignement : la présence systématique d'un pays « leader », la définition d'un objectif stratégique commun et une construction progressive à partir de deux ou trois pays.

II.2.3 Quelles leçons pour la construction de l'Europe du renseignement ?

En appliquant ces grands principes observés sur Echelon et Hélios, il est possible de faire le constat suivant:

- la création d'une Europe du renseignement ne pourra se faire que sur la base d'une coopération bilatérale ou trilatérale existante. Elle ne pourra pas se créer *ex nihilo* à partir de 27 pays,
- l'absence d'objectif stratégique commun est flagrante. Les dissensions entre les visions française et britannique sur la nature même de l'Europe est un problème de fond,
- l'absence de « pays leader ». Aucun pays ne semble vouloir mettre en avant son expertise nationale au profit d'un dessein européen.

Toutefois, à partir de ce constat pessimiste, certaines pistes se dessinent. L'Europe s'est toujours construite pierre par pierre, poussée par la volonté de certains pays pionniers. Le déficit de vision stratégique commune peut être contourné par la définition d'un objectif commun ciblé sur lequel un consensus fort se dégage. Typiquement, la « stratégie européenne de sécurité » constitue une base solide.

II.3 Du « Frenchelon » à l' « Eurechelon »

II.3.1 La France, pilier central d'un « Eurechelon » ?

Partant de l'idée que l'Europe du ROEM se construira par la mise en réseau de capacités nationales existantes, il est intéressant de faire un état des lieux des aptitudes des différents pays. Il est indispensable de posséder une base solide à la mise en place d'un réseau européen d'interception des communications à l'échelle mondiale, appelée « Eurechelon » par analogie au surnom donné par les média au système français de ROEM : « Frenchelon ».

Le rapport du Parlement européen estime[11] que seule la France, en Europe, dispose des conditions géographiques et techniques pour constituer la base d'un tel système :
« Pour pouvoir intercepter, à l'échelle mondiale, des communications internationales acheminées par les satellites de la première génération, des stations de réception sont indispensables dans la zone atlantique, dans la zone de l'océan Indien et dans la zone de l'océan Pacifique. Pour la génération plus récente de satellites, permettant une émission par sous-région, il faut encore respecter d'autres conditions quant à la position géographique des stations d'interception si l'objectif consiste à capter l'ensemble des communications transmises par satellite. Un autre système d'interception fonctionnant à l'échelle mondiale doit installer ses stations ailleurs que dans les territoires relevant des pays UKUSA.

La mise en place d'un tel système d'interception fonctionnant à l'échelle mondiale doit cependant également présenter un intérêt économique et politique pour le ou les exploitants. Le ou les bénéficiaires d'un tel système doivent avoir des intérêts économiques et militaires ou d'autres intérêts en termes de sécurité, ou à tout le moins croire qu'ils font partie des puissances mondiales. Dès lors, le cercle des pays concernés se limite, pour l'essentiel, à la Chine et aux pays du G8, sans les États-Unis et le Royaume-Uni.

[11] Par devoir de réserve, l'auteur de ce mémoire se refuse de s'exprimer sur les capacités françaises de ROEM.

Dans les trois zones précitées, la France possède des territoires, départements et collectivités locales qui lui sont propres. Dans l'Atlantique, il y a, à l'est du Canada, Saint-Pierre-et-Miquelon (65° O / 47° N), au nord-est de l'Amérique du Sud, la Guadeloupe (61° O / 16° N) et la Martinique (60° O / 14° N) ainsi qu'au large de la côte nord-est de l'Amérique du Sud, la Guyane française (52° O / 5° N). Dans la zone de l'océan Indien, il y a, à l'est de l'Afrique australe, Mayotte (45° E / 12° S) et La Réunion (55° E / 20° S), ainsi que tout au sud, les terres Australes et Antarctiques françaises. Dans la zone du Pacifique, on trouve la Nouvelle-Calédonie (165° E / 20° S), Wallis et Futuna (176° O / 12° S), ainsi que la Polynésie française (150° O / 16° S).

S'agissant de l'existence éventuelle de stations du service de renseignement français . la DGSE (Direction générale de la sécurité extérieure) . dans ces régions d'outre-mer, les renseignements sont peu nombreux. Selon certains journalistes français, il existe des stations à Kourou (Guyane française), ainsi qu'à Mayotte. Aucune donnée précise n'est disponible en ce qui concerne la grandeur de ces stations ainsi que le nombre ou les dimensions des antennes satellites. En France, d'autres stations existeraient à Domme (près de Bordeaux) et aux Alluetts-le-Roi (près de Paris). Jauvert estime à 30 au total le nombre des antennes satellitaires. L'écrivain Erich Schmidt-Eenboom affirme qu'une station serait également en service en Nouvelle-Calédonie et que le service de renseignement allemand utiliserait dans une certaine mesure cette installation.
En théorie, la France, qui réunit non seulement les conditions géographiques mais aussi les conditions techniques et financières, pourrait également exploiter un système d'interception fonctionnant à l'échelle mondiale. Votre rapporteur ne dispose toutefois pas de suffisamment d'informations de sources publiques pour pouvoir l'affirmer sérieusement ».

En dépit de cette domination française dans le domaine du ROEM européen, la France a de nombreux intérêts à soutenir activement la constitution d'un « Eurechelon » :

- partager l'effort financier et humain entre les différentes nations,
- bénéficier de l'appui technique de certaines nations dans des domaines critiques (traduction de langues rares, décryptage, etc.),
- développer en coopération des satellites d'écoute,
- bénéficier des facilités juridiques de certains états. Typiquement, la loi française ne permet pas l'interception systématique sur des supports

filaires transitant par le territoire national, alors que certains pays voisins disposent d'un dispositif législatif plus souple.

II.3.2 Quelques pistes de coopération

La création d'un système européen de ROEM doit se bâtir avec beaucoup de pragmatisme sur une base franco-allemande, qui est la seule crédible:

- le couple franco-allemand a toujours été le principal moteur de la construction de l'Europe de la Défense,
- par ses capacités, la France est le seul pays à pouvoir fournir une colonne vertébrale fiable à un tel système,
- l'Allemagne a décidé de l'acquisition d'une composante ROEM aéroporté à base d'un drone haute altitude longue endurance : « Eurohawk »[12],
- la France se dote d'une première capacité ROEM spatial grâce aux constellations de satellites Essaim,

De plus, depuis septembre 2001, la lutte contre le terrorisme constitue un enjeu majeur particulièrement fédérateur. Cette thématique pourrait constituer l'objectif stratégique commun pour l'ensemble des nations qui souhaiterait rejoindre « Eurechelon ».

II.3.3 Quelles relations entre Echelon et un futur « Eurechelon » ?

La mise en en place d'un système européen de ROEM pose le problème de la place des pays qui appartiennent déjà à Echelon : la Grande-Bretagne et certainement d'autres pays.[13] Deux cas sont possibles :

- le cas britannique : l'ensemble de ses capacités ROEM est engagé dans Echelon. Ce pays ne peut pas se permettre de dupliquer ses moyens de renseignement au profit de deux réseaux différents,
- le cas des pays de « deuxième cercle »[14] : leur participation à Echelon est symbolique (mise a disposition d'emprises géographiques pour installer

[12] Le nom de « Eurohawk » a été donné par les Américains à cette version du « Globalhawk » destiné au marché européen.
[13] Le cas de la Pologne est cité.

des centres d'écoute, surveillance des réseaux de communication locaux, etc.). La participation de ces pays à un système européen n'est pas incompatible de leur engagement auprès des Etats-Unis.

Dans ce jeu d'alliances européennes et transatlantiques, il est légitime de d'interroger sur la position du « Eurechelon ». Un tel système n'a-t-il pas vocation à intégrer un système Echelon OTAN rassemblant le réseau Echelon actuel et les capacités européennes ? Certainement pas, et pour plusieurs raisons :

- dans un domaine aussi stratégique, les Etats-Unis ne partageront jamais leur position dominante. Ceci constituerait un point de blocage pour la France qui milite pour un partenariat transatlantique équilibré, a contrario des Britanniques qui peuvent accepter ce rôle de « petit frère »[15],
- la France et l'Allemagne seraient reléguées à des rôles subalternes en raison de l'absence de vision politique commune avec les Etats-Unis,
- la France perdrait un outil précieux d'autonomie stratégique.

En revanche, des coopérations ciblées seraient souhaitables sur des objectifs bien particuliers exigeant un effort commun, comme par exemple la prolifération nucléaire iranienne.

[14] Cf. § I.4.1 l'analyse proposée des relations entre pays partenaires du réseau Echelon
[15] que le général de Gaulle a résumé avec beaucoup de sarcasme : « Les Britanniques ont bradé leur droit d'ainesse pour un plat de Polaris »

Conclusion

Cette étude a mis en exergue l'importance du réseau Echelon dans la stratégie américaine de maîtrise globale de l'information. Elle a mis en lumière les capacités avérées d'interception des communications internationales qui peuvent être indifféremment orientées vers la lutte contre le terrorisme ou le renseignement économique. Face à ce risque bien identifié depuis plusieurs années, notamment à travers le rapport d'information du parlement français d'octobre 2000, les Européens sont libres de se protéger des interceptions en se dotant de moyens adaptés de cryptage pour sécuriser leurs communications.

Sur le fond, ces travaux ont montré que les réseaux nationaux de communication appartenaient au patrimoine stratégique d'une nation et que celle-ci avait le devoir de les protéger pour garantir son indépendance. Typiquement, le marché des opérateurs privés de téléphonie ne doit pas être totalement débridé : la recherche permanente du moindre coût ne doit pas devenir une finalité lorsque l'on traite d'un secteur stratégique.

Etudié en temps que modèle de construction d'un système multinational de renseignement, le réseau Echelon constitue un exemple rare de réussite, au même titre que le système Hélios ; ces deux systèmes ayant été construits sur des logiques similaires. Ainsi, seul le couple franco-allemand dispose des capacités pour former la colonne vertébrale d'un futur réseau européen de renseignement. La construction d'une Europe du renseignement constitue un des défis majeurs auquel les 27 pays de l'Union devront faire face.

La réflexion sur la mise en place d'une coopération bilatérale franco-allemande dans le domaine du renseignement d'origine électromagnétique doit inciter les autorités nationales à développer une nouvelle approche interministérielle du renseignement afin de satisfaire, au mieux, les besoins de l'Etat et d'améliorer notre efficience. Un système multinational sera d'autant plus performant si ses pions nationaux ont déjà développés une véritable culture de l'efficacité puis de l'efficience.

Enfin, une étude sur la définition d'une Europe du renseignement ne peut pas faire l'économie d'une réflexion sur la position britannique, tiraillée entre son engagement

européen et sa relation privilégiée avec les Etats-Unis. Le pragmatisme britannique va nécessairement atteindre tôt ou tard ses limites. Quelles sont les éléments qui inciteront la Grande-Bretagne a entré pleinement dans l'Europe ?

« En Dieu nous croyons, le reste nous l'écoutons »
(Devise officieuse de la NSA)

ANNEXE

A. 1 Les liaisons radio hertziennes de proximité

Ce sont des émissions hertziennes de portée limitée, de quelques dizaines de mètres à plusieurs dizaines de kilomètres selon la gamme de fréquence et la puissance de l'émetteur. Elles sont destinées à relier un émetteur-récepteur mobile à un autre, fixe ou mobile. Pour faciliter la mobilité de l'appareil, les émissions radioélectriques sont généralement omnidirectionnelles. Une multitude d'applications civiles ou militaires existe car cette solution a l'énorme avantage d'offrir une solution techniquement fiable et à faible coût en s'affranchissant de l'installation d'un système filaire fixe. Les principales applications connues sont :

- les communications tactiques militaires sol-sol, air-sol ou air-air en gamme V/UHF[16] : dans les usages air-sol ou air-air et en l'absence d'obstacle à la propagation des ondes, ces émissions peuvent permettre de communiquer jusqu'à plusieurs dizaines de kilomètres,
- les liaisons entre les téléphones mobiles et leur borne de raccordement, appelée BTS[17] : en téléphonie mobile, l'espace est divisé en « cellules », c'est-à-dire une zone au sein de laquelle l'ensemble des communications est assuré par la même BTS. Le rayon d'une cellule varie de quelques centaines de mètres dans les grands centres urbains à plusieurs kilomètres dans les campagnes,
- les liaisons entre un téléphone sans fil et son socle de raccordement : destiné à un usage domestique, ce type de liaison est généralement de faible portée, de l'ordre de quelques dizaines de mètres,
- les liaisons « sans fil » de tout type: blue-tooth, Wi-fi, etc. Afin de simplifier l'usage de ces nouvelles technologies et d'éviter les interférences entre des fréquences trop proches, ces dernières sont maintenant normalisées.

Dans un souci de clarté et pour éviter des confusions avec le paragraphe § I.2.4 sur les liaisons HF, il est important de souligner que le terme de liaison HF est aussi utilisé pour

[16] V/UHF : ensemble des fréquences couvrant les gammes VHF (30 à 300 MHz) et UHF (300 à 3000 Mhz)
[17] BTS : Base transceiver station

décrire des liaisons de très courte portée, tel le blue-tooth. En effet, la propagation des ondes HF s'effectue de deux manières bien différentes :

- par « onde de sol » : la propagation s'effectue en épousant la rotondité de la surface de la Terre. Les liaisons de ce type sont généralement de très courte portée : c'est ce procédé qui est utilisé pour les nouvelles technologies de communication évoquées supra mais aussi pour les usages militaires tactiques, appelés « HF tactique ». Toutes ces liaisons sont décrites dans le paragraphe « liaison hertzienne de proximité »,
- par rebond des ondes sur les couches de troposphères : ce type de propagation permet d'atteindre plusieurs milliers de kms. Il est décrit dans le paragraphe §I.2.4 « liaison HF ».

A. 2 Les faisceaux hertziens

Les faisceaux hertziens sont des liaisons en vue directe entre deux antennes d'émission-réception, généralement installées en haut de mats ou de tours pour s'affranchir des reliefs. La portée des faisceaux hertziens (FH) est généralement limitée à plusieurs dizaines de kilomètres. Les ondes étant formées en faisceau, les FH permettent de transmettre des débits très élevés, de l'ordre de plusieurs dizaines de Mbits/s. Ce type d'installation est très répandu dans les réseaux d'infrastructure pour relier des zones où l'installation de câbles est difficile ou trop couteuse. Le réseau national de télécommunication est encore constitué de nombreux segments équipés avec des FH. Pour les Armées, ce moyen constitue une solution rapide pour installer une solution fiable et pérenne permettant de véhiculer des informations à haut débit.

Dans les pays en reconstruction, cette solution est généralement utilisée car elle permet d'installer rapidement un réseau de télécommunication moderne, compatible de la téléphonie mobile, en s'affranchissant des structures existantes, généralement détruites ou inadaptées aux nouveaux besoins.

A. 3 Les liaisons HF

Par cette propriété particulière de la propagation par rebond troposphérique, la liaison en gamme HF est un moyen assez ancien pour permettre d'assurer des

communications à très longue distance. Avant l'avènement des communications par satellite, la gamme HF était un outil privilégié des services diplomatiques pour joindre les différentes ambassades dans le monde. Elle était principalement utilisée en morse et, à moindre échelle, en phonie (voix).

Délaissées au profit des communications par satellite, les liaisons HF connaissent un nouveau gain d'intérêt en raison de leurs caractéristiques très propres :

- le coût : celui d'un équipement complet d'émission-réception est de l'ordre de quelques centaines d'euros et permet de communiquer gratuitement à travers le monde. La modicité du prix est certainement un des facteurs de son succès auprès des O.N.G.,
- la rusticité : une station HF est un moyen fiable et peu volumineux permettant d'établir des communications mondiales,
- la possibilité de transmettre des fichiers informatiques : longtemps cantonné au morse, la gamme HF permet maintenant de transmettre des courriers électroniques de taille informatique réduite (quelques dizaines de kilos octets).

Ainsi, les « primo-utilisateurs », à savoir les forces armées et les services diplomatiques, relancent depuis plusieurs années l'usage des liaisons HF pour s'affranchir des problèmes d'allocations de ressources satellitaires, de zone de réception et de coût.

A. 4 Les câbles sous-marins

L'usage du câble sous-marin, posé au fond des océans, pour transmettre des messages entre les continents date du télégraphe. Initialement, les premiers câbles étaient électriques et nécessitaient des relais à terre pour les liaisons de très longue distance. Typiquement, les câbles électriques entre l'Europe et l'Amérique du Nord ressortaient à Terre Neuve (Canada) pour ré-amplifier le signal et le réémettre. Les câbles actuels en fibre optique disposent de relais intégrés ne nécessitant plus de refaire sortir en surface les câbles lors d'une liaison transatlantique.

Ils sont aujourd'hui principalement utilisés pour les liaisons intercontinentales les plus exigeantes en termes d'échange de données : les deux principales artères sont Etats-Unis-

Europe et Etat-Unis-Asie du sud-est. La figure, en annexe xx, est une carte des câbles sous-marins actuels.

En terme de débit, les câbles en fibre optique offre des capacités incomparables, de la classe du Tbits/s par rapport aux capacités des télécommunications par satellite.

A. 5 Les liaisons filaires

Ce sont l'ensemble des liaisons utilisant un support physique : fibre optique, fil téléphonique en cuivre, etc. L'intérêt de la fibre optique est principalement sa capacité à transmettre de très haut débit de données et, à une moindre échelle, la difficulté de réaliser une interception sur un tel support. Depuis quelques années, l'installation de fibre optique est systématiquement effectuée lors de constructions d'ouvrages majeurs d'infrastructure : route, bâtiments, etc. Dans les pays en voie de développement, cet usage est favorisé par les nombreux financements d'organismes supranationaux, notamment de l'Union européenne, pour réduire la « fracture numérique ».

A. 6 Les liaisons transitant par satellite

La transmission des signaux via satellite s'effectue comme suit: le signal acheminé par une liaison est envoyé par une station terrestre équipée d'une antenne parabolique via un faisceau hertzien ascendant, appelé « liaison montante », vers un satellite. Le satellite reçoit le signal, l'amplifie et le renvoie via un faisceau hertzien descendant, appelé « liaison descendante », vers une autre station terrestre. Là, le signal est réintroduit dans un réseau câblé.

Globalement, les liaisons par satellite peuvent être classées selon différents critères : l'orbite, le service, la zone de couverture et la bande de fréquences.

Le type d'orbite :

La très grande majorité des satellites de communications sont en orbite géostationnaire. Sur celle-ci, située dans le plan équatorial à 36000 km de la terre, les satellites ont une position fixe par rapport à la terre. De cette position, un satellite peut couvrir près d'un

tiers de la surface du globe. Trois satellites, décalés de 120°, suffisent pour couvrir la quasi-totalité du globe, à l'exception des zones polaires. La position du satellite étant fixe par rapport à la terre, le pointage des liaisons montante et descendante l'est aussi. Ce type de satellite a une durée de vie de 15 à 20 ans, ce qui est très largement supérieure à celle des satellites en orbite basse, limitée à 5 ans en général. Une autre famille d'orbite existe : les orbites basses elliptiques. Dans ce cas, les satellites sont dit « défilants » car leur position par rapport à la terre change en permanence. Ainsi, un même point au sol sera vu entre 15 et 20 minutes par un satellite à chaque ellipse. En général, il est nécessaire de disposer d'une constellation de satellites pour assurer une couverture permanente d'une région et de maitriser les liaisons entre satellites pour éviter une perte de liaison lorsqu'un satellite n'est plus en visibilité de l'émetteur au sol. Enfin, un dernier type d'orbite, très particulier mérite d'être cité : les orbites polaires : elles sont destinées à répondre à des besoins spécifiques. C'est le cas de la constellation russe Molnya conçue pour assurer une couverture permanente de l'ancien territoire soviétique et notamment des zones polaires,

Le service proposé (fixe ou mobile):

Les services fixes par satellite, appelé aussi Consortiums, sont des liaisons satellitaires entre deux stations terrestres fixes. C'est le cas d'Intelsat, Eutelsat ou Arabsat. Ce type de service, permettant de transmettre des communications à haut débit, est aussi utilisé pour la télévision et la radiodiffusion. Les services mobiles par satellite (SMS) relient une station terrestre fixe à une station mobile. Avec les dernières générations de satellite, il est maintenant possible de disposer de services mobiles reliant directement, par satellite, deux stations mobiles. Les principaux services mobiles sont Inmarsat et Thuraya.

La zone de couverture :

Celle d'un satellite géostationnaire de communication est l'emprise au sol dans laquelle il est possible d'émettre et de recevoir une communication. Elles sont classées en quatre catégories :

- couverture globale : la liaison descendante permet de couvrir près de 40% de la surface terrestre,
- couverture hémisphérique: 20 % de la surface terrestre,
- couverture zonale: 10 % de la surface terrestre,

- couverture par lobe étroit ou « spot beam » : la couverture est un cercle de quelques centaines de kilomètres de diamètre.

Les bandes de fréquences:

- la bande L (0.6 à 1.5 GHz): elle est utilisée pour les liaisons entre les mobiles (Inmarsat et Thuraya) et les satellites,
- la bande S (2.5 à 3.5 GHz) est citée pour mémoire: elle est peu utilisée,
- la bande C (3.5 à 6 GHz) est très utilisée pour les services fixes,
- la bande X (7-8 GHz) est utilisée par les services diplomatiques et militaires des pays occidentaux,
- la bande Ku (11-13 GHz) est, comme la C, employée pour la radiodiffusion, Eutelsat, etc.…
- la bande Ka (20-30 GHz) est très prometteuse: en raison de la saturation des bandes C et Ku, de nombreuses études portent sur la bande Ka.

A.7 La carte synthétique du réseau Echelon

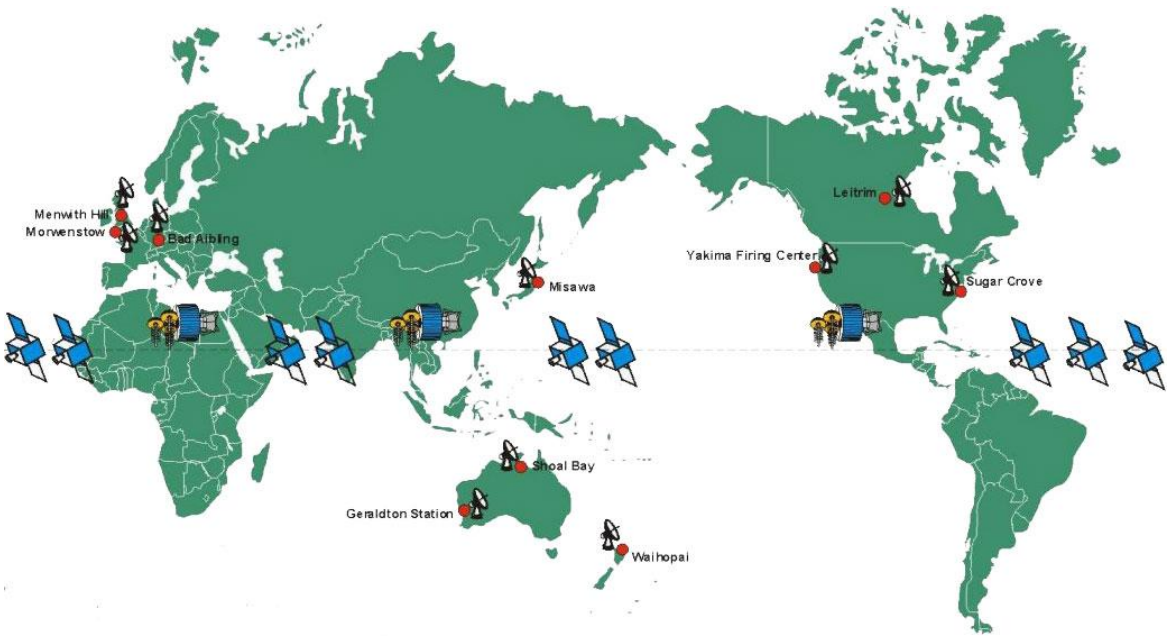

Figure : www.rr0.org/Echelon.html

A.8 La carte des câbles sous-marins

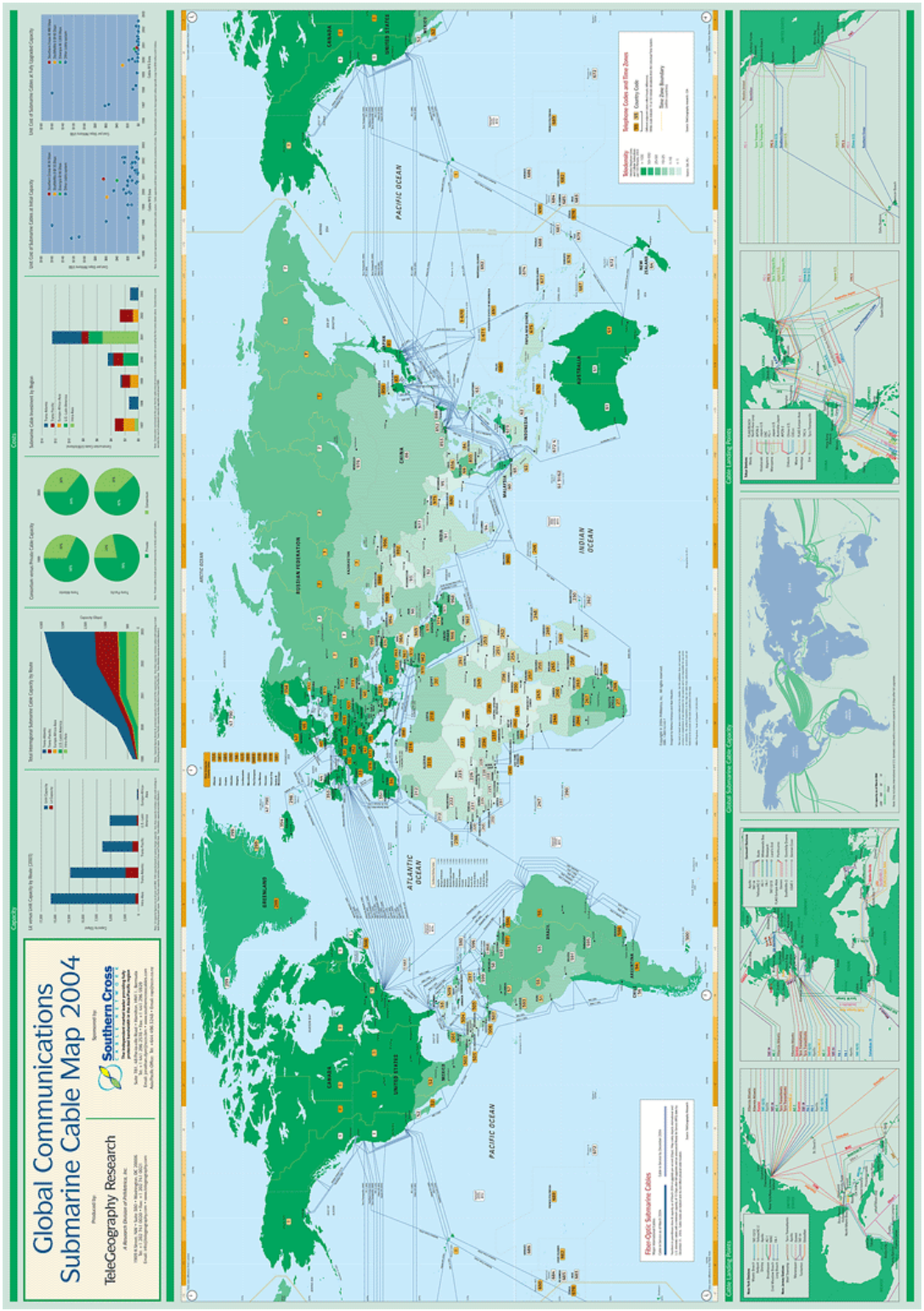

Figure : www.telegeography.com

BIBLIOGRAPHIE

DOCUMENTS INSITUTIONNELS :

- Rapport du parlement européen du 11 juillet 2001 : *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))*. *Rapporteur : Gerhard Schmid*
- Rapport d'information de l'assemblée nationale du 11 octobre 2000 : *Rapport d'information par la commission de la Défense nationale et des forces armées sur les systèmes de surveillance et d'interception électronique pouvant mettre en cause la sécurité nationale (n°2623), présenté par Monsieur Arthur Puecht, député.*

SITE INTERNET :

- www.telegeography.com: site en anglais sur les grandes artère de communications. De nombreuses cartes de référence: les cables sous-marins, la carte des communications mondiales, etc.
- www.echelononline.free.fr: site en français décrivant le fonctionnement du reseau Echelon, les technologies utilsées. Site très documenté.
- www.reseau.echelon.free.fr: site en français, très documenté sur les satellites d'écoute.
- www.nsa.gov: site de la National Security Agency

ARTICLES DE REVUES EN FRANÇAIS

- GUISNEL Jean, « Les Français aussi écoutent leurs alliés», *Le Point*, 06/06/1998, n°1342

TABLE DES MATIERES