UNIVERSITÉ LAVAL

LE MAINTIEN DE LA PAIX

INSTITUT QUÉBÉCOIS DES HAUTES ÉTUDES INTERNATIONALES

BULLETIN N° 50
janvier 2001


Vols d'Ibis rouges (fragments), *La Terre vue du Ciel*, Éditions de La Martinière, 1999.

# LE SYSTÈME ÉCHELON: UNE NOUVELLE DONNE DANS L'ESPIONNAGE ÉLECTRONIQUE

Dans une missive envoyée à *The Wall Street Journal*, le 22 mars 2000, l'avocat et ancien directeur de la Central Intelligence Agency (CIA), R. James WOOLSEY , déclarait sans ambiguïté: «Oui chers amis du continent européen, nous vous avons espionnés». Cette affirmation venait confirmer ce que d'autres sources avaient déjà mis en lumière, à savoir l'existence du réseau d'écoute électronique Échelon. Cette révélation-choc d'un ancien acteur important de la sécurité et du renseignement aux États-Unis a mis à l'avant-scène deux séries de problèmes de plus en plus aigus dans le nouvel ordre international de l'après-guerre froide: l'empiétement sur la vie privée des citoyens, en raison des impératifs de la sécurité nationale des États par l'écoute électronique (voir le Bulletin numéro 49) ainsi que l'importance de plus en plus grandissante pour les agences du renseignement de l'espionnage économique. Si l'un et l'autre de ces problèmes ne sont pas nouveaux, le développement des nouvelles technologies et le statut quasi hégémonique des États-Unis aux plans économique et militaire, en modifient radicalement leur signification. Pourtant, il n'est pas surprenant que la question de l'espionnage économique et des «pratiques commerciales jugées déloyales» prenne aujourd'hui tant d'ampleur. Du temps où R. James WOOLSEY était directeur de la CIA, il avait souligné que l'espionnage économique représentait «la question la plus brûlante en matière de renseignement». La confirmation de l'existence d'Échelon, grâce à différents rapports du parlement européen en 1998 et 1999, semble renforcer l'idée que les pratiques en matière du renseignement sont de plus en plus liées à des questions de nature économique. Le partenaire militaire et diplomatique risque d'être aussi le concurrent économique. La dichotomie de la guerre froide entre amis et ennemis s'estompe donc graduellement. Mais qu'est-ce que l'espionnage économique? Pour en comprendre les enjeux, il est nécessaire de bien distinguer les notions d'intelligence économique, d'espionnage économique et de pratiques déloyales.

## LE RENSEIGNEMENT SUR LES TRANSMISSIONS

À partir des travaux d'Abram SHULSKY, il est possible de définir le renseignement sur les transmissions de la manière suivante:

Le renseignement sur les transmissions (ou SIGINT) est le terme générique utilisé pour désigner le procédé par lequel on obtient des renseignements en interceptant des ondes électromagnétiques (radio), appelées généralement signaux. L'ensemble peut être subdivisé en trois catégories, selon le type d'ondes électromagnétiques interceptées:

### COMINT

L'interception de signaux de communications étrangers (messages radio) et l'extraction de renseignements de ces signaux par des personnes autres que celles auxquelles ils étaient destinés, sont connues sous le nom de renseignement sur les communications ou COMINT.

### TELINT

L'interception, le traitement et l'analyse de télémétrie étrangère sont connus sous le nom de renseignement télémétrique ou TELINT.

### ELINT

L'interception, le traitement et l'analyse de radiations électromagnétiques ne concernant pas les communications émises par un équipement militaire (comme un radar) pendant son fonctionnement sont connus sous le nom de renseignement électronique ou ELINT.

## INTELLIGENCE ÉCONOMIQUE VERSUS ESPIONNAGE ÉCONOMIQUE ET PRATIQUES DÉLOYALES

Dans un rapport intitulé *Intelligence économique et stratégie des entreprises*, soumis au Commissariat général du Plan en France, on définissait l'intelligence économique comme: «l'ensemble des actions coordonnées de recherche, de traitement, de distribution et de protection de l'information utile aux acteurs économiques, obtenue légalement» (source: http://www.plan.gouv.fr/publications/4PAGintelligence.htm). L'intelligence économique recouvre ce qui est habituellement désigné sous les vocables de veille technologique, de surveillance concurrentielle, de veille globale, d'information critique, etc. La notion d'intelligence économique est née aux États-Unis à la fin de la décennie 1960, principalement avec l'ouvrage de Harold WILENSKY *Organizational Intelligence: Knowledge and Policy in Government and Industry*. L'auteur identifiait déjà les deux grands axes de la problématique de l'intelligence économique:

- les stratégies collectives et la coopération entre les gouvernements et les entreprises dans la production d'une connaissance commune pour la défense de l'avantage concurrentiel;

- l'importance de la connaissance dans l'économie et l'industrie comme moteur stratégique du développement et du changement.

De son côté, l'espionnage économique, pour reprendre la définition de Samuel PORTEOUS du Service canadien du renseignement de sécurité (SCRS), est «le fait, pour un gouvernement étranger ou ses affidés, d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour acquérir des renseignements économiques» (source: http://www.csis-scrs.gc.ca/fra/comment/com46.html). Ces deux définitions permettent de bien voir que loin d'être synonymes, les deux notions sont à l'opposé dans l'obtention de l'information et dans la création de la connaissance liée à la prise de décision. Les conséquences de l'espionnage économique sont difficiles à mesurer. Outre les cas médiatisés, dont ceux concernant Échelon, les différentes entreprises, surtout les entreprises américaines, aux prises avec cette problématique préfèrent l'éluder. Leurs réticences s'expliquent par:

- la culture organisationnelle générale des entreprises qui n'aiment pas beaucoup exposer leurs problèmes à l'extérieur;
- la peur de représailles possibles des gouvernements en cause;
- la crainte que de telles révélations n'entraînent l'obligation d'avoir à dévoiler davantage que ce que les sociétés sont prêtes à dire;
- la crainte de perdre la confiance des actionnaires.

On estime que les pertes provoquées par cette situation représentent plusieurs milliards de dollars. La société IBM, l'une des rares entreprises à rendre publique et à comptabiliser ses pertes financières reliées à l'espionnage économique, en arrive à la même conclusion. Depuis le début de la décennie 1990, on constate que la position adoptée par la CIA est de considérer l'espionnage économique comme un sous-ensemble d'une catégorie plus large: celle des pratiques déloyales. On considère que les pratiques déloyales sont «le fait, pour un gouvernement ou une personne morale étrangère, d'utiliser des moyens illégaux, clandestins, coercitifs ou trompeurs au profit de ses intérêts économiques propres» (source: http://www.csis-scrs.gc.ca/fra/comment/com46.html). Comme le démontrent les cas reliés à la découverte d'Échelon, les pratiques déloyales concernent une panoplie de situations qui ne nécessitent pas nécessairement l'intervention d'un gouvernement ni l'obtention par des moyens illégaux d'informations ou de technologies appartenant à un État, à une personne morale ou à un ressortissant. Dans la plupart des situations, les autorités américaines craignent qu'un individu étranger en corrompe un autre, ce qui pourrait mettre en péril les avantages concurrentiels dont disposent les grandes entreprises américaines sur le marché international. C'est avec la Loi FCPA (Foreign Corrupt Practices Act) que le mandat de l'agence américaine a été élargi à la corruption dans les pratiques commerciales. Les négociations sur l'adoption de lois similaires se poursuivent au sein de l'Organisation de coopération et de développement économique (OCDE). L'objectif vise à criminaliser tout versement de pots de vin à des étrangers. La FCPA fait écho aux scandales qui ont secoué les États-Unis dans la décennie 1970. Comme la loi américaine a une portée extraterritoriale, elle vise à forcer les pays alliés à faire en sorte d'agir de la même manière, ce qui uniformiserait les pratiques commerciales entre pays alliés. Si tous les États adoptaient les mêmes comportements, la loi américaine perdrait ainsi sa raison d'être. Elle est cependant dénoncée aux États-Unis même, puisque selon l'ancien secrétaire d'État américain, Warren CHRISTOPHER, cette loi a fait perdre des milliards de dollars aux entreprises américaines. Jusqu'à présent, l'administration CLINTON a peu progressé dans sa tentative de convaincre ses autres partenaires de l'OCDE d'adopter une loi semblable. Certains pays, en plus de fermer les yeux sur ces pratiques commerciales douteuses, acceptent même que leurs ressortissants déduisent de leurs impôts, comme frais professionnels, les pots de vin versés à des étrangers. Les autorités fédérales américaines se sont donc tournées vers la CIA pour lutter contre les pratiques commerciales jugées déloyales. Au milieu de la décennie 1990, James WOOLSEY affirmait que la CIA avait permis de sauver des contrats de plusieurs milliards de dollars aux firmes américaines et que très souvent, les responsables de ces compagnies n'étaient même pas au courant de l'intervention de la CIA. Jusqu'à tout récemment, une question demeurait sans réponse: quelles étaient les méthodes utilisées par l'agence américaine pour lutter efficacement contre ces pratiques déloyales? La découverte du réseau d'écoute électronique Échelon répond en grande partie à cette interrogation.

## LA COMMUNAUTÉ DE RENSEIGNEMENT UKUSA

La Seconde Guerre mondiale a mis à l'avant-scène l'importance du renseignement sur les transmissions ou SIGINT (Signals Intelligence), c'est-à-dire celle de capter et d'analyser (décrypter) les ondes électromagnétiques (ondes radio) ennemies. La collaboration entre le Royaume-Uni et les États-Unis débute, plus précisément en mai 1943 avec l'accord Brusa. En effet, les Britanniques avaient réussi «à casser» le code du chiffre allemand et ils avaient décidé, après quelques hésitations, de partager leurs secrets avec les Américains. Ce premier accord allait être le prélude à l'accord secret de sécurité Royaume-Uni/États-Unis (UKUSA) de 1947 sur le partage des interceptions électromagnétiques. C'est à la fin de ce conflit, plus précisément en septembre 1945, que le président américain Harry TRUMAN décida qu'il était nécessaire de poursuivre les opérations SIGINT en temps de paix en collaboration avec d'autres États. En décembre de la même année le gouvernement canadien arrivait à la même conclusion. En 1946-1947, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande créaient une communauté SIGINT sous la supervision du United Kingdom's Government Communication Headquarter (GCHQ) britannique. Ce premier accord était complété par le traité connu sous le nom UKUSA. Ce traité, encore secret aujourd'hui, est divisé entre les «premières parties» que sont le Royaume-Uni et les États-Unis et les «secondes parties» que sont le Canada, l'Australie et la Nouvelle-Zélande. Ce traité divise les sphères d'influences et les responsabilités en matière de cryptographie. Il semble que les «secondes parties» fournissent principalement les données brutes, tandis que les «premières parties» font à la fois la collection des données brutes dans leur secteur d'attribution et le traitement et l'analyse des données. C'est au sein de cette communauté du renseignement qu'est utilisé le système d'écoute électronique Échelon.

| PAYS | AGENCES | PRINCIPAUX TERRITOIRES COUVERTS |
|---|---|---|
| ROYAUME-UNI | *The United Kingdom's Government Communication Headquarter (GCHQ)* | L'Afrique, l'Europe contientale et la Russie européenne |
| AUSTRALIE | *Australia's Defense Signals Directorate (DSD)* | L'Asie du Sud-Est et la Chine méridionale |
| NOUVELLE-ZÉLANDE | *New Zealand's Government Communication Security Bureau (GCSB)* | La zone du Pacifique |
| CANADA | *Centre de la sécurité des télécommunications (CST)* | Le nord de la Russie et probablement l'Amérique latine |
| ÉTATS-UNIS | *National Security Agency (NSA)* | L'Amérique du Sud, l'Asie, la Russie asiatique et la Chine |

## DE L'AVION-ESPION U-2 à ÉCHELON

Une semaine après l'humiliation faite aux États-Unis par la défense antiaérienne de l'URSS qui abattit l'avion espion U-2 de Gary POWERS le 1er mai 1960, le président EISENHOWER ordonna la mise sur orbite du premier satellite d'espionnage électromagnétique, ce qui fut fait le 22 mai 1960. Une nouvelle ère de l'espionnage électronique venait de naître. Ce premier lancement du GRAB (Galactic Radiation And Background), allait être suivi par des dizaines d'autres dont les satellites de type SSF (Sub Satellites Ferrets), entre 1963 et 1986, de type Ryolithe de 1970 à 1978, de type Canyon de 1968 à 1977, de type Jumpseat de 1971 à 1983, et finalement de type Vortex de 1978 à 1989. Il convient aussi d'ajouter à cette liste trois autres systèmes qui complètent la capacité des «oreilles indiscrètes» des États-Unis dans le domaine des SIGINT et des COMINT.

- Les satellites-espions Orion; plus précisément trois Orion ont été lancés (1985,1989 et 1990) lors de missions militaires de la navette spatiale. La spécialité des Orion est l'écoute des COMINT qui se retrouve dans les bandes supérieures à 100 MHz. Ils permettent d'intercepter tout particulièrement les communications des téléphones cellulaires.

- Le Mercury ou Advanced Vortex vise à capter les signaux de la bande des 20KHz. Il semblerait que sa vocation soit surtout d'ordre militaire. En outre, il serait en mesure d'intercepter les communications des sous-marins en plongée.

- Enfin, le Trumpet a comme créneau spécifique l'interception de l'ensemble des communications militaires russes.

Ce large éventail de capacité d'écoute possède un important talon d'Achille: la nécessité d'avoir des stations au sol pour traiter les signaux transmis par les satellites en orbite et effectuer les mesures radio-goniométriques. En plus, les stations au sol sont incontournables pour «écouter» les communications des satellites civiles déployés tout autour du globe et particulièrement les dix-huit du consortium multinational Intelsat. C'est dans cette perspective que les partenaires UKUSA sont mis à contribution et c'est aussi dans ce même cadre qu'entre en jeu le système Échelon. En octobre 1999 au Parlement européen, le système d'écoute américain soulevait une grande indignation dans la plupart des chancelleries européennes, notamment en France avec la présentation du rapport officiel du journaliste écossais d'investigation, Duncan CAMPBELL. Mais qu'est-ce que Échelon? À tout considérer, le système Échelon est un dictionnaire mondial qui, à partir des capacités américaines d'interception et de ses acolytes d'UKUSA, trie de manière automatique par mots clés la majorité des communications de la planète (téléphone, télécopieur, courriel) à l'aide de puissants ordinateurs. Les États-Unis sont à peu près les seuls à disposer de telles capacités technologiques. Dans la décennie 1970, les Soviétiques ont tenté de suivre les Américains, mais l'éclatement de l'URSS et l'état de l'économie de la Russie ont pratiquement obligé cette dernière à déclarer forfait en la matière. Tout récemment cependant, Moscou aurait mis sur orbite de nouveaux satellites destinés à cette fin. Pour leur part, les Britanniques ont cherché à se libérer de la tutelle des États-Unis, surtout depuis leur conflit avec l'Argentine en 1982, où les renseignements américains n'auraient filtré qu'au compte-gouttes. Londres espérait construire un satellite-espion, le Zircon, mais les pressions de l'administration américaine l'ont forcé à mettre de côté cette option. En contrepartie, il semblerait que Londres ait plutôt acquis l'un des trois Orion lancés entre 1985 et 1990.

Même si Paris s'est indigné contre Échelon, la DGSE (Direction générale de la sécurité extérieure) connaissait depuis la fin de la décennie 1980 l'existence d'Échelon. Il en va de même du service allemand des renseignements, le BND (Bundes NachrichtenDienst). D'ailleurs, sans avoir les mêmes capacités que les «grandes oreilles» américaines, les deux services se sont entendus, avant la chute du mur de Berlin, pour espionner les satellites civils de communication et pour installer des stations d'écoute des transmissions radioélectriques. Le petit frère franco-allemand d'Échelon est construit autour de la base d'écoute secrète que constituent les installations spatiales françaises de Kourou en Guyane, et reliées à d'autres dispersées aux Antilles, à la Réunion, en Nouvelle-Calédonie, dans les Émirats Arabes Unis ainsi que les stations situées dans les représentations diplomatiques allemandes à travers le globe. Ce dispositif est complété par certains navires de guerre, dont le Bougainville, ainsi que par les satellites-espions Hélios 1A qui est en orbite depuis 1995 et Hélios 1B lancé au début de l'année 2000 et qui prendra le relais d'Hélios 1A, lorsque ce dernier aura épuisé ses réserves de carburant.

## ET DEMAIN ?

La National Security Agency (NSA) et les forces armées américaines espèrent joindre à tous ces systèmes spatiaux d'espionnage électronique d'autres éléments tels que des drônes stratégiques et des avions sans pilote. On sait que la jonction entre ces nouveaux engins et les satellites-espions est à la base du projet IOSA (Integrated Overhead Sigint Architecture) qui relève, semble-t-il, d'une nouvelle structure administrative mise sur pied par le gouvernement américain: le NSSAO (National Security Space Architect Office). Si le mariage souhaité entre les drônes et les satellites atteint les résultats escomptés, il permettra de réaliser un vieux rêve de la NSA: supprimer sa dépendance à l'égard des stations au sol dans les pays étrangers. En effet, la présence de ces stations attire trop facilement l'attention des groupes pacifistes, des investigations journalistiques et même politiques, comme le démontre le cas du rapport remis au parlement européen. En outre, la présence d'installations au sol augmente la probabilité de fuites en provenance de fonctionnaires locaux. Ainsi, l'IOSA viserait à remédier à cette vulnérabilité de la NSA. L'arrimage permettrait l'interception des SIGINT par les satellites et les drônes qui communiqueraient les données à des satellites relais qui, à leur tour, transmettraient l'information directement sur le territoire des États-Unis pour l'analyse. Cependant, ce rêve titanesque se bute à deux autres problèmes difficiles à surmonter: la capacité de traitement de l'information par les ordinateurs et les défis posés par la cryptographie. Bien que la NSA possède les ordinateurs les plus sophistiqués du monde, elle a été obligée d'admettre, le 24 janvier 2000, que l'ensemble de son réseau informatique de traitement et d'analyse avait connu une panne totale pendant trois jours. La raison en est simple: son système a été incapable de répondre au torrent d'informations recueillis à travers le monde.

Tout comme le fait le Pentagone pour l'industrie aéronautique militaire, la NSA saupoudre de milliards de dollars l'industrie de l'informatique. Trois sociétés sont directement impliquées dans ce créneau très spécifique: IBM, Cray et Compaq. L'objectif est de développer les machines pouvant répondre au défi teraFLOP, c'est-à-dire: des machines ayant la capacité de traiter plusieurs trillions d'opérations à virgules flottantes par seconde. Rappelons qu'un trillion égale mille milliards. L'objectif de la Maison-Blanche, dans un programme lancé en février 1998, est que l'industrie développe des ordinateurs ayant la possibilité de vitesse de traitement de 30 teraFLOPS en 2001 et de 100 teraFLOPS en 2004! Présentement, on estime que les machines les plus performantes ont une capacité de traitement de 5 teraFLOPS. Cette course contre la montre vise, bien sûr, à répondre au défi que pose la cryptographie. On l'a rappelé dans le Bulletin 49, cette technologie s'impose pour protéger les informations dans un marché de commerce électronique désormais en pleine expansion. Des civils, comme l'informaticien Phil ZIMMERMAN, ont même mis gratuitement sur le marché, des cryptosystèmes, tel le PGP pour *Pretty Good Privacy*. D'autres systèmes plus performants sont aussi sur le marché, ce qui donne évidemment beaucoup de fil à retordre à la NSA. Face à la concurrence, les États-Unis permettent désormais la libre circulation de ces logiciels sur le marché, mais des lois sont toujours à l'étude pour mieux en contrôler la portée en les assortissant à des conditions draconiennes: soit que la NSA en possède les clés soit qu'elle puisse les décrypter!

## QUELQUES EXEMPLES MÉDIATISÉS DE CAS D'ESPIONNAGE ÉLECTRONIQUE

La perte, en 1994, pour les firmes françaises Thomson et Alcatel, d'un contrat de matériel de surveillance de la forêt amazonienne qui a été attribué à la compagnie américaine Raytheons, un sous-contractant de la NSA dans le cadre d'Échelon.

La perte, en 1995, pour le consortium d'avionnerie Airbus d'un contrat avec l'Arabie saoudite au profit de l'entreprise américaine Boeing.

Retrait de la société Hughes Aircraft du Salon aéronautique du Bourget en avril 1993 à la suite d'une information communiquée par la CIA au directeur de la société; cette compagnie était sur une liste de 49 entreprises américaines ciblées par la DGSE française.

À Montréal, deux membres de l'ancienne police secrète est-allemande, la Stasi, ont utilisé de faux dossiers d'employés fournis par des sociétés «compréhensives» pour l'obtention d'emplois dans des entreprises canadiennes ciblées.

En 1992, les gens d'affaires ont été invités à ne pas voyager avec Air France en raison du fait que l'on avait découvert que la DGSE posait des micros dans les sièges des avions de la société française et que ses agents se mêlaient aux passagers et aux personnels de bord.

Dans la décennie 1980, des agents de renseignements du Japon ont été soupçonnés de mener, en concertation avec des firmes japonaises, des opérations contre les entreprises américaines de haute technologie de Silicon Valley en Californie.

Un employé de General Electric aurait reçu un million de dollars par année d'une entreprise sud-coréenne pour communiquer des procédés secrets entrant dans la fabrication du diamant synthétique.

Source: Rapport Campbell; voir aussi http://www.csis-scrs.gc.ca/fra/comment/com42.html

Dany DESCHÊNES, décembre 2000

Le bulletin *Le Maintien de la paix* est désormais accessible sur INTERNET à l'adresse suivante: http://www.ulaval.ca/iqhei

Prix de l'abonnement : $13.00 pour six numéros en l'an 2000-2001, ou 3,50 dollars le numéro. Veuillez libeller votre chèque au nom de l'IQHÉI et l'adresser au Pavillon Charles-De Koninck, bureau 5458, Université Laval, Québec, G1K 7P4.
Abonnement électronique via : hei@hei.ulaval.ca

Supervision éditoriale : Claude Basset

ISSN 1192-909X