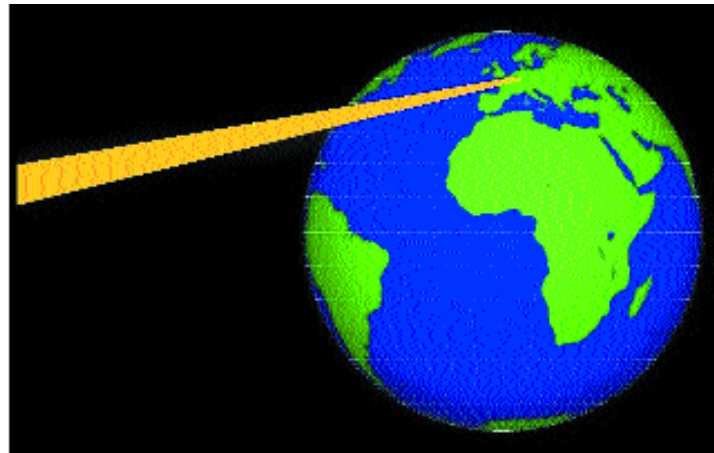


Satellite espion Vortex



La Troisième Guerre mondiale a déjà commencé

## A l'écoute des ondes

**Les troupes qui se lancent virilement à l'assaut d'un bunker en brandissant des grenades à main et en vociférant, cela c'est de la guerre à grand-papa. Les fantassins d'aujourd'hui sont plutôt issus du MIT ou d'autres instituts technologiques et sont assis derrière des écrans d'ordinateurs.**

La guerre est une option stratégique destinée à assurer l'emprise d'un Etat sur un ou plusieurs Etats tiers, considérés comme «ennemis». Pour parvenir à ce but, l'action militaire constituait une version tactique de mise jusqu'à tout récemment.

Désormais les gros souliers cloutés, les gamaches bien cirées et les chars blindés s'effacent devant les techniques évoluées de l'espionnage des télécommunications, qui parviennent aux mêmes objectifs sans qu'une seule goutte de sang ne soit versée. Une armée de l'ombre certes, mais dont les effectifs sont loin d'être minables. L'«ennemi» est devenu un «honorabile concurrent» et les assauts sont devenus beaucoup plus feutrés, mais ô combien plus efficaces.

### Compétition USA-Europe

L'ouverture officielle des hostilités s'est déroulée en 1993, lorsque *Bill Clinton* confia à *James Woolsey*, promu le 5 février

de cette année-là directeur de la *CIA* (Central Intelligence Agency), la mission de transformer la *CIA* et la *NSA* (National Security Agency) en une agence de renseignements économiques.

Clairvoyant, le président des USA avait compris qu'après la disparition du «rideau de fer» et l'effondrement de l'URSS, le temps des aventures militaires était définitivement révolu et qu'il s'agissait désormais de s'affirmer sur un champ de bataille à l'échelon mondial, dans lequel les bits remplacent les impacts d'obus. L'idée fondatrice de *Echelon* était née.

### Alliance USA-Grande Bretagne

En fait, le système *Echelon* ne bénéficie pas qu'aux seuls USA. Les renseignements recueillis profitent également au Royaume-Uni (la *GCHQ* britannique étant en liaison avec la *NSA*) et à d'autres pays anglophones, notamment l'Australie, la Nouvelle Zélande et le Canada.

Le nom officiel de *Echelon* est *Comint*

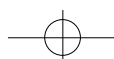
(Communications Intelligence). Il s'agit d'un vaste déploiement d'activités de récolte de renseignements touchant les secteurs diplomatique, économique, technologique et scientifique. Ces renseignements sont ensuite le cas échéant transmis de façon ciblée à des entreprises faisant partie du «club» anglo-saxon, via des officines privées.

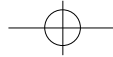
Il convient en l'occurrence de signaler la duplicité stupéfiante du Royaume-Uni (membre de l'UE) dans cette affaire : un véritable «Cheval de Troie» ! Autre constatation : le gouvernement américain ne fait pas un mystère de son potentiel de recherche de renseignement, voire même des techniques déployées, estimant qu'il est de «bonne guerre» de récolter toute information utile, pour assurer la prospérité économique de la nation.

Officiellement, et c'était *James Woolsey* (ancien directeur de la *CIA*) qui le déclara



Antenne parabolique pour l'interception de satellites Intelsat





rait encore récemment au début de cette année à *Jean-Jacques Mével* (envoyé spécial du «*Matin*» à Washington : «Ce n'est pas du chantage que de faire une démarche diplomatique auprès d'un gouvernement qui est l'objet d'une tentative de corruption». Et de préciser encore : «Le but est de faire reculer la corruption et non de faire attribuer le contrat au concurrent américain».

En clair, le gouvernement américain présente toute sa structure d'espionnage des télécommunications comme étant une vertueuse mesure de salubrité publique destinée à lutter contre la pratique (sous-entendue généralisée en Europe) des pots de vins, des dessous de table, des «graissages de pattes» et du blanchissage de l'argent sale. Un peu léger!

#### Méthodes évoluées

Les méthodes utilisées sont simultanément simples et évoluées. Simples parce qu'il est évident de s'intéresser prioritairement aux informations électroniques,

sans négliger pour autant les voies de l'espionnage «classique» (taupes, réseaux consulaires, associations, contacts personnels «privilegiés», antennes d'entreprises US en Europe...).

Actuellement presque tout passe par les télécommunications : Internet, e-mail, téléphonie fixe ou itinérante, etc.; via satellites et câbles terrestres ou sous-marins, sans oublier les tentaculaires réseaux mondiaux dévolus au traitement en temps réel des cartes de crédit et à l'enregistrement auprès des compagnies d'aviation. A titre d'exemple, rien de plus révélateur que de savoir, via le «sniffage» des réseaux des cartes de crédit et des réservations d'avions, que le PDG et une délégation de cadres d'une grande firme européenne sont en train d'organiser un déplacement en Corée (certainement pas pour y faire du tourisme collectif).

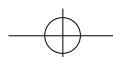
Simultanément, ces méthodes sont évoluées, parce que les moyens mis en œuvre ne relèvent pas de stratégies d'amateurs! Il est nécessaire en effet de disposer d'équipements techniques avancés (plus

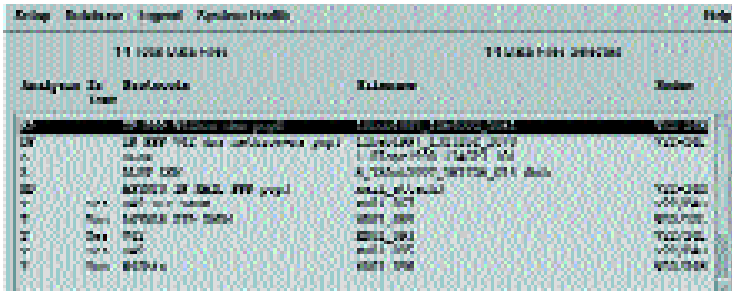
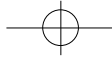
de 120 satellites espions, notamment de la classe *Vortex*), de bases d'antennes paraboliques, et même de sous-marins spécialement outillés pour «sniffer» les câbles de télécommunications transocéaniques.

A ce sujet, la NSA ne fait plus mystère aujourd'hui de son opération dans la mer d'Okhotsk dès octobre 1971, lorsque le sous-marin américain *Halibut*, camouflé en submersible de secours mais en fait doté d'une cloche de plongée spéciale, plaça un dispositif de captage composé d'un assemblage de selfs hypersensibles à un câble sous-marin de transmission soviétique, système qui fonctionna continuellement jusqu'en 1982.

Actuellement il est évidemment nécessaire de disposer d'ordinateurs dotés de logiciels performants pour extraire de l'immense smog hertzien les informations vitales dignes d'être recueillies, respectivement traitées (décryptées le cas échéant) et présentées sous une forme susceptible d'être exploitée. Finalement il est tout aussi nécessaire de disposer de personnel qualifié et d'un budget suffisant.

**MSM**  
Le Mensuel de l'industrie





«Comint»: logiciel permettant d'analyser plus de 10'000 messages enregistrés

Ces deux dernières conditions sont actuellement remplies. L'organisation *Echelon* dispose à cet effet d'un budget annuel estimé entre 15 et 20 milliards de dollars (3,5 milliards de dollars pour la seule NSA), cette dernière employant à elle seule 12'000 spécialistes en informatique, électronique et télécommunications.

### Pas seulement une affaire d'Etat

Les choses étant comme chacun le sait passablement «privatisées» outre Atlantique, la récolte de renseignements n'échappe pas à cette tendance.

La chute du Mur de Berlin a prélué à une restructuration de la CIA qui a vu ses effectifs fondre rapidement. La majeure partie des professionnels (souvent de haut niveau) concernés (1500 départs) se sont recyclés dans des officines privées, tel notamment le cabinet d'investigation *Kroll*, soupçonné en l'espèce d'avoir joué un rôle décisif dans nombre d'affaires mettant en concurrence des firmes américaines et européennes.

Dans certains cas, le président des USA lui-même, dûment informé, n'hésitera pas à intervenir directement, ce qui fut par exemple le cas lors d'une grande affaire portant sur la mise en place d'un système de surveillance de la forêt vierge amazonienne, mettant en concurrence (pour une affaire de 1,3 milliard de dollars) le Français *Thomson-CSF* et l'Américain *Raytheon*. C'est ainsi que *Bill Clinton* n'hésita pas à envoyer une lettre personnelle le 23 juin 1994 au président du Brésil, *Franco Itamar*, pour faire pencher la balance. Extrait : «Dear Mr. President, My Administration has closely studied Brazil's proposed Amazon Surveillance System (SIVAM) and has strong support for U.S. firms competing for this important project. I would like to add my personal support for US Industry».

Outre *Kroll*, de tels cabinets sont foison aux USA, quelques noms : *Futures Group*, *Kirk Tison International*, *Fuld & Co.*, *SIS*, etc. Au moins 2600 raisons sociales rassemblées autour d'une association de renseignement privé appelée *SCIP*.

*John Deutch*, ex sous-secrétaire à la Défense des USA et alors directeur de la CIA (poste auquel il avait été élu par un Sénat unanime le 10 mai 1995) ne cachait pas le changement d'orientation de son organisation. Il déclarait il y quelques années : «La sécurité économique est devenue une priorité nationale». A priori il s'agit d'une déclaration assimilable à une «vérité de la Palice», mais à mieux y regarder, elle est tout de même stupéfiante, venant du responsable d'un service interministériel. C'est révélateur.

Rappelons que *John Deutch* a été remplacé le 11 juillet 1997 par *George Tenet*, un scientifique issu de l'Université de Los Alamos. Pour la petite histoire, précisons que *John Deutch* hébergeait des informations sensibles sur son propre ordinateur personnel non sécurisé, lequel était simultanément utilisé pour le butinage et l'échange de documents par e-mail en direction et provenance de sites Internet à caractère plutôt coquin. En somme il a été pris à son propre piège!

### Les «oreilles» de l'espace

Il faut rechercher les premières manifestations d'intérêt des USA pour les affaires européennes au lendemain de la Seconde Guerre mondiale et à la veille de l'époque de Guerre froide entre l'Ouest et l'Est, donc au début des années cinquante.

A cette époque, c'était surtout (mais pas uniquement) la zone URSS et pays satellites qui étaient dans le collimateur, d'où la création de la base de *Bad Aibling* en Autriche, laquelle héberge actuellement un remarquable gisement de ra-

dômes recouvrant des antennes paraboliques branchées sur des satellites de télécommunications et d'espionnage.

Une autre station, la plus importante, se trouve à *Menwith Hill* en Grande-Bretagne. Etablie en 1956 par l'ASA (US Army Security Agency), elle a été remise à la NSA en juin 1966. Elle a d'ailleurs été élue «station de l'année» pour 1991, en raison du rôle décisif qu'elle avait joué dans le cadre de la Guerre du Golfe!

Au début des années 60, elle fut l'un des rares sites au monde à être équipé des premiers grands ordinateurs *IBM* pour traiter les messages télex interceptés. Actuellement, cela va sans dire, les innombrables radômes de la station sont raccordés à des ordinateurs puissants qui passent au peigne fin les appels téléphoniques, e-mails, télégrammes, trafic internet et autres messages provenant aussi bien de gouvernements que de sociétés privées et même de simples citoyens.

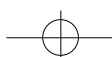
La station de *Menwith Hill* comporte 23 grands radômes et trois antennes paraboliques géantes, l'une d'entre elles ayant un diamètre de 60 mètres. Tous ces équipements sont pointés en direction de l'est, donc le continent européen. Deux câbles à fibres optiques, capables de transmettre chacun 100'000 communications simultanées, ont en outre été installés en 1996 entre le réseau de *British Telecom* et le site de *Menwith Hill*.

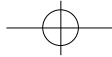
Une station terrienne, basée à Etam en Virginie, récolte les données en provenance des stations européennes via le satellite géostationnaire *Intelsat IV*.

Un site à vocation identique se trouve implanté à *Wahihopai*, dans l'île sud de la Nouvelle-Zélande. Il scrute depuis 1987 plus particulièrement la zone Pacifique, alors qu'un autre, basé à *Geraldton* (Australie) couvre l'Asie orientale, captant notamment les deux satellites de communication *Indian Ocean Intelsats*.

### Traitement des informations

Des informations arrivant en masse ne servent à rien sans un traitement adéquat. Un tri manuel est impossible. Raison pour laquelle dans de vastes salles d'ordinateurs, implantées sur les sites, s'opère l'analyse automatique de toutes les informations interceptées. L'enregistrement démarre uniquement lorsqu'un mot-clé apparaît. Ces mots-clés sont introduits dans un répertoire (thesaurus) constamment tenu à jour et introduits dans un program-





me d'analyse automatique évolué. L'utilité des informations retenues et enregistrées de la sorte dépend évidemment de la valeur du thesaurus et de la réactivité du système, ce qui exige des moyens informatiques impressionnants, autant du point de vue matériel que logiciel. Le traitement proprement dit des informations enregistrées (triage, classification et adressage) ne s'effectue pas sur le site, raison pour laquelle ces salles d'ordinateurs des bases ne comportent pas de personnel, à part les équipes de sécurité et de maintenance du site.

### Cryptage-décryptage

Reste la question des informations cryptées. Les algorithmes de cryptage/décryptage sont si complexes qu'il est humainement impossible de les reconstituer. Le seul moyen est de les obtenir à la source, c'est-à-dire au sein même de l'entreprise qui les a mis au point.

C'est ainsi que la société suisse *Crypto S.A.* sise à Zoug, aurait été suspectée (suite aux révélations d'un ancien employé de la société qui s'est ensuite rétracté après avoir été attaqué en justice) de manipuler ses systèmes de cryptographie pour les rendre accessibles à la NSA et que M. Boris Hägelin, fondateur et ancien PDG de l'entreprise zougnoise, aurait été en relation avec Nora L. MacKabee, cadre de la NSA.

M. Armin Huber, PDG de l'entreprise, dément ces bruits. Il déclarait notamment : «s'il y a eu manipulation ici, c'est le fait de journalistes plus attirés par la sensation que par la vérité». La Police fédérale suisse a mené une enquête débouchant sur un non-lieu. Néanmoins le slo-

gan «Total Information Security» de cette société s'est trouvé égratigné au cœur d'une controverse qui n'est pas encore éteinte actuellement, chacun ayant encore en mémoire les démêlés épiques de Hans Bühler, agent de *Crypto* à Téhéran, avec la justice de l'Iran (où il fut emprisonné dès mars 1992 durant 9 mois et interrogé longuement chaque jour), qui prétendait détenir la preuve que *Crypto* avait livré la clé de cryptage de son système à la NSA. Alors de deux choses l'une : ou les systèmes *Crypto* sont peu fiables et aisément décryptables, ou alors les sources sont communiquées à la NSA. Il n'y a pas d'autre alternative.

D'autre part, il est de notoriété publique actuellement que *Microsoft* a implanté des facilités d'accès dans les processeurs des systèmes d'exploitation *Windows*, à savoir un driver appelé *ADVAPI.DLL* comportant diverses fonctionnalités ayant trait à la sécurité de transmission des données, incluant notamment le *Microsoft Cryptographic API (MS-CAPI)*.

### Et la Suisse?

D'abord l'Europe. Evidemment c'est plutôt d'emblée «mal barré», étant donné le double jeu des Britanniques, et dans une moindre mesure celui des Allemands et des Autrichiens.

Toujours est-il qu'un rapport de 80 pages appelé «Systèmes de surveillance et d'interception électronique pouvant mettre en cause la sécurité nationale», présenté par le député français Arthur Paecht (Var), porte-parole de la Commission de la défense, a été présenté à l'Assemblée nationale française. Selon ce rapporteur, des renseignements indiquent



A gauche James Woolsey, à droite John Deutch, «patrons» successifs de la CIA

que le système «Echelon» actuel, qui commence à dater dans sa conception, est en voie d'être remplacé par un système beaucoup plus performant, grâce à de nouveaux moyens et de nouveaux partenariats.

La Commission propose ainsi une série de mesures basées sur le «principe de précaution», notamment en ce qui concerne une sécurisation absolue des communications par un cryptage approprié (logiciels de conception européenne) et l'élaboration d'un code de déontologie en matière de renseignements.

Un rapport de l'UE appelé «Interception Capabilities 2000» décrit en détail l'organisation et les méthodes utilisées par la NSA dans le cadre de *Comint*, les méthodes d'interception des télécommunications internationales, des informations détaillées sur les divers sites de l'organisation, les procédures de récolte de renseignements économiques et les perspectives de développement du système après l'an 2000. Ce rapport ne manque pas par ailleurs d'égratigner la probité de l'entreprise *Crypto S.A.*

Les Suisses commencent également à prendre la chose au sérieux et le Parlement a dégagé un budget de 100 millions de francs pour un projet dont la première phase devrait être opérationnelle déjà au milieu de cette année. Il s'agira d'utiliser les sites d'antennes paraboliques de Loèche (2 antennes paraboliques de 18 mètres de diamètre). De plus petites antennes (de 4 à 13 mètres de diamètre) seront implantées à Heimanschwand, alors qu'un centre de traitement des données sera mis en service à Zimmerwald, générant 40 places de travail. Ce projet a pour nom de code *Satos 3*.



Vue générale du site de Menwith Hill (GB)

EDOUARD HUGUELET  
Rédacteur en chef

