LE MONDE diplomatique

Révolution dans la communication
« Manière de voir » #46 • juillet-août 1999

RÉVOLUTION DANS LA COMMUNICATION

Le système Echelon

Avec un budget annuel de 26,7 milliards de dollars — autant que pendant la guerre froide —, les services de renseignement américains sont les mieux dotés de la planète. Des alliances stratégiques et une technologie puissante leur permettent d'espionner de manière routinière téléphone, fax et courrier électronique dans le monde entier.

PAR PHILIPPE RIVIÈRE

LES Etats-Unis sont-ils désormais si puissants qu'ils ne craignent plus les réactions de leurs alliés européens ? Il avait fallu l'obstination d'un chercheur néo-zélandais, Nicky Hager, pour dévoiler l'existence d'un formidable réseau de surveillance planétaire, le système Echelon, en place depuis les années 80... Son enquête (1) exposait en détail, pour la première fois, comment l'Agence de sécurité américaine (National Security Agency, NSA), un des organismes américains les plus secrets, surveille, depuis presque vingt ans, l'ensemble des communications internationales (2).

M. Zbigniew Brzezinski, conseiller à la sécurité nationale sous la présidence de M. James Carter, avoue, non sans cynisme : *« Quand vous avez la capacité d'avoir des informations, il est très dur d'imposer des barrières arbitraires à leur acquisition.* (...) *Devons-nous refuser de lire* (3) *? »* L'embryon du réseau d'espionnage américain date du début de la guerre froide lorsqu'un premier pacte de collecte et d'échange de renseignements, dénommé Ukusa, fut établi entre le Royaume-Uni et les Etats-Unis. A ces deux Etats se sont joints le Canada, l'Australie et la Nouvelle-Zélande. Depuis les années 70, des stations d'écoute implantées dans ces pays captent les signaux retransmis vers la Terre par les satellites de type Intelsat et Inmarsat. Et une centaine de satellites d'observation « écoutent » les ondes : radio, téléphones cellulaires, etc.

Par ailleurs, affirme Duncan Campbell (4), tous les réseaux de communication sont écoutés, des câbles sous-marins (des capteurs sont déposés par des plongeurs spécialisés) au réseau Internet (la surveillance du réseau mondial est particulièrement aisée : la quasi-totalité des données transitent par des « noeuds » situés sur le territoire américain, même lorsqu'il s'agit de connexions européennes ! Ainsi, chaque jour, des millions de télécopies, de télex, de messages électroniques et d'appels téléphoniques du monde entier sont passés au crible, triés, sélectionnés, analysés.

« Le système Echelon, explique Nicky Hager, *a été conçu de manière à interconnecter* [tous les systèmes d'écoute] *pour leur permettre de fonctionner comme les composants d'un tout intégré. »* Les stations de réception satellitaire captent l'ensemble des faisceaux des satellites Intelsat, la plus importante d'entre elles, localisée à Menwith Hill, en Angleterre, étant placée sous le contrôle direct de la NSA. La masse d'informations recueillies est toutefois trop importante pour pouvoir être exploitée sans traitement préalable par les effectifs — pléthoriques, mais pas infinis — des services de renseignement.

« La clé de l'interception, continue Nicky Hager, *repose sur de puissants ordinateurs qui scrutent et analysent ces masses de messages pour en extraire ceux qui présentent un intérêt. Les stations d'interception reçoivent les millions de messages destinés aux stations terrestres légitimes et utilisent des ordinateurs pour dénicher ceux qui contiennent des adresses ou des mots-clés préprogrammés. »*

Adresses et mots-clés que les services de renseignement s'échangent sous forme de *« dictionnaires »* reflétant leurs préoccupations du moment. Il suffit que des mots comme terrorisme, drogue, guérilla, ou des noms comme Castro, Kadhafi, Saddam Hussein, etc. soient émis pour que la communication entière soit identifiée, retenue, analysée. Un peu à la manière des moteurs de recherche sur Internet, ces « grandes oreilles », munies des meilleurs systèmes automatiques de reconnaissance

vocale, de lecture optique et d'évaluation des contenus, sélectionnent les communications à surveiller. Duncan Campbell précise toutefois que, si les ordinateurs de la NSA sont en mesure de reconnaître automatiquement les locuteurs lors d'une conversation téléphonique, ils ne sont pas encore capables d'en retranscrire le contenu.

D'autres chercheurs ont établi le scénario suivant, correspondant certainement plus à la réalité de la fin des années 80 qu'aux capacités actuelles du système (5). Chaque jour, les analystes des diverses agences examinent la moisson de la veille, qui arrive marquée de dates, d'indications de provenance et de destination, et de chiffres-clés : 5 535 représente, par exemple, les communications diplomatiques japonaises ; 8 182, les échanges concernant les technologies de chiffrement, etc. Les données sont transcrites, déchiffrées et traduites sous forme de rapports détaillés, de gists donnant l'essence d'une conversation ou de résumés reprenant les informations dans leur contexte.

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

Ce système diffère des écoutes téléphoniques « classiques » par deux caractéristiques particulièrement préoccupantes. La première constitue un problème majeur de souveraineté nationale pour les petits pays de l'alliance Ukusa : dans les années 80, à la suite du refus du premier ministre travailliste de l'époque, M. David Lange, de laisser entrer dans les eaux territoriales néo-zélandaises un navire, l'USS Buchanan, doté de capacités nucléaires, les Néo-Zélandais croyaient leur pays coupé des renseignements de la NSA. Mais, en réalité, sans en référer à leur gouvernement, les services néo-zélandais avaient, au contraire, accru leur collaboration avec la NSA et accéléré le déploiement d'Echelon. Parallèlement, la presse néo-zélandaise déclenchait une campagne de désinformation sur le thème : « Que ferons-nous sans les renseignements américains ? »

Surveiller des mots-clés

De plus, le fait même qu'Echelon permette des échanges de « dictionnaires » aboutit à faire de chaque service de renseignement un agent de collecte, sur son territoire, d'informations destinées à des partenaires étrangers. Mais la transmission se fait... de manière automatisée et, en raison du mode de programmation du système, il ne permet pas à la partie néo-zélandaise de connaître les mots-clés utilisés par ses partenaires. La réciproque, on s'en doute, n'est pas vraie... Cela aurait, par exemple, pu permettre aux Etats-Unis d'utiliser les infrastructures néo-zélandaises pour espionner les communications de l'association Greenpeace, lors de sa campagne de protestation contre les essais nucléaires français autour de l'atoll de Mururoa en 1995, sans en informer Wellington !

Autre originalité par rapport aux écoutes « classiques », les interceptions menées par Echelon sont pilotées à partir de mots-clés, et non pas en plaçant sous surveillance systématique des numéros de téléphone, de fax, ou des adresses Internet de personnes précises. Cet aspect technique, certes très prometteur en termes de renseignement, efface toute possibilité de définition — par décision judiciaire, militaire ou politique — de la source surveillée : toute personne est susceptible d'être écoutée pour peu que sa conversation soit jugée « intéressante » par le logiciel ! Les dérives sont inévitables. Un ancien espion canadien, M. Mike Frost, accuse ainsi M me Margaret Thatcher d'avoir fait venir à Londres, en février 1983, des opérateurs canadiens pour surveiller deux des ministres de son propre gouvernement qui — naïfs — ourdissaient quelque trahison politique... en communiquant avec leurs téléphones cellulaires.

Il est tentant d'utiliser un système si secret et si puissant pour les renseignements généraux et les opérations de basse police : en 1992, des opérateurs de haut rang des services secrets britanniques, fâchés de certaines dérives, dévoilèrent qu'Amnesty International, entre autres organisations non gouvernementales, avait été écoutée... à partir de mots-clés relatifs au trafic d'armes. Et, pour l'exemple, ils montrèrent au journaliste de l'Observer comment ils procédaient pour intercepter les conversations relatives au mot-clé « aide au tiers-monde » (6). Le choix de ce journal était tout indiqué : les propriétaires de l'Observer, après la publication d'une enquête, en 1989, sur les agissements du fils de M me Thatcher, avaient également été mis sur écoutes par cette dernière (7).

Dérives isolées ? Comme l'explique M. Steve Wright, chercheur à la Fondation Omega, une organisation britannique de défense des droits humains, dans le prérapport qu'il remit au Parlement européen en janvier 1998, *« Echelon est principalement dirigé contre des cibles non militaires : gouvernements, organisations et entreprises dans virtuellement tous les pays.* (...) *Bien que beaucoup d'informations* [recueillies par le système] *concernent de potentiels terroristes, il s'y produit beaucoup d'intelligence économique, notamment une surveillance intensive de tous les pays participant aux négociations du GATT* (8) *».* Les systèmes d'écoutes ne se cantonnent donc pas à la surveillance des activités terroristes ou mafieuses. Le renseignement économique et, partant, les renseignements généraux d'ordre politique en sont aussi un enjeu central. Chacun des pays impliqués est censé empêcher que ses propres citoyens soient écoutés, mais, en l'absence de tout contrôle extérieur, cette disposition reste

largement théorique. Cela inquiète notamment le Congrès des Etats-Unis, où un projet d'amendement à la loi de finances 2000 vise à contraindre la NSA à dévoiler le mode de fonctionnement d'Echelon et à confirmer sa compatibilité avec la Constitution... ce qui, au vu du sinistre bilan des écoutes illégales pratiquées de tous temps par l'agence américaine, est hautement improbable !

Tous les messages contrôlés

Déjà la Cour suprême avait imposé, en 1967, l'arrêt du projet « Minaret », fichage de milliers d'organisations et d'individus sur des « listes de surveillance » où figuraient des « dissidents » tels que Martin Luther King, Malcolm X, Jane Fonda ou Joan Baez ; en 1975, c'est le directeur de la NSA qui, face au tollé déclenché au Congrès, mettait un terme au projet « Shamrock » de surveillance, avec la complicité des principales compagnies de télégraphe, de tous les messages télégraphiques entrant ou sortant des Etats-Unis...

Dans un rapport remis, début novembre 1998, au Congrès, le chercheur Patrick Poole montre que les principales firmes bénéficiant du produit de l'espionnage mené par Echelon sont celles qui fabriquent l'équipement du réseau Echelon, notamment Lockheed, Boeing, Loral, TRW et Raytheon : *« Une relation incestueuse si forte, assure le rapport, que les renseignements recueillis sont parfois utilisés pour écarter des fabricants américains de marchés convoités par ces contractants majeurs des secteurs de la défense et du renseignement, qui sont par ailleurs souvent la source de grandes contributions financières aux deux partis qui dominent la vie politique américaine* (9). »

« Des entreprises européennes ont déjà fait les frais [d'Echelon], expliquait M. Alain Pompidou, président du comité d'évaluation des choix technologiques et scientifiques (STOA) du Parlement européen. *Mais, comme elles commercent avec les Etats-Unis, elles se taisent* (10). » A la décharge de ces entreprises, le fait qu'il n'existe aucun texte de droit international réglementant les écoutes mais également la difficulté d'obtenir des informations fiables. La participation britannique embarrasse les instances européennes qui, à l'instar de M. Martin Bangemann, alors commissaire européen en charge du commerce, attendent *« des preuves de l'existence du système »* avant que de risquer de nuire aux *« bonnes relations commerciales avec les Etats-Unis »*. Si le Foreign Office nous certifie qu'*« il n'existe aucune incompatibilité entre la position du Royaume-Uni dans l'Union européenne et son devoir de garantir la sécurité nationale »,* les députés européens demandent toutefois l'instauration d'un « code de bonne conduite » ainsi qu'un complément d'enquête, qui pourrait les amener à interroger... la NSA.

Des *« preuves »* ? Suite à un reportage diffusé à la télévision australienne, M. Martin Brady, le directeur du DSD, a mis un terme à plus de cinquante années de secret officiel et lâché les mots tabous : l'agence australienne *« coopère en effet avec ses homologues étrangères, les organisations d'interception des communications des pays réunis dans le pacte Ukusa »,* écrit-il au producteur du programme.

PHILIPPE RIVIÈRE

(1) Nicky Hager, *Secret Power. New Zealand's Role in The International Spy Network,* Craig Potton Publishing, Nelson, Nouvelle-Zélande, 1996. N'ayant pas trouvé d'éditeur aux Etats-Unis, le livre y est distribué par la revue Covert Action Quarterly [http://www.covertaction.org/], Washington DC.

(2) Steve Wright, *An Appraisal of Technologies of Political Control,* [http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm]Interim Study, STOA, Parlement européen, 19 janvier 1998. (Lire le texte intégral du rapport [http://cryptome.org/stoa-atpc.htm].)

(3) *Le Nouvel Observateur,* 10-16 décembre 1998.

(4) *Interception Capabilities 2000. Development of Surveillance Technology and Risk of abuse of Economic Information,* [http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm]STOA, Parlement européen, PE 168 184, avril 1999.

(5) Patrick S. Poole, « Echelon : America's Secret Global Surveillance Network », The Privacy Papers, no 4, novembre 1998, Free Congress Research and Education Foundation, Washington, DC.

(6) John Merritt, *The Observer,* Londres, 28 juin 1992, cité par Nicky Hager, op. cit.

(7) Hugh O'Shaughnessy, *The Observer,* 28 juin 1992.

(8) Steve Wright, *op. cit.*

(9) Patrick S. Poole, *op. cit.*

(10) *Le Figaro,* Paris, 19-20 septembre 1998.

Mot clés: Technologies de l'information