10. Nouvelles technologies et relations internationales

ECHELON : ORIGINES ET PERSPECTIVES D'UN DEBAT TRANSNATIONAL

PAR

FRANCK LEPREVOST et BERTRAND WARUSFEL (*)

L'année 2000 a été marquée, parmi d'autres questions, par les remous provoqués en Europe et au sein des institutions communautaires par de nouvelles révélations concernant l'existence d'un dispositif transnational d'interception électronique qui serait, pour l'essentiel, dirigé par les Etats-Unis et leur principale agence fédérale en la matière, la *National Security Agency* (NSA). Si beaucoup a déjà été écrit sur un tel sujet, on a encore peu pris en compte la dimension politique d'un tel débat et sa signification au regard du contexte des relations internationales dans l'après-guerre froide. Cet article n'a pas d'autre but que de synthétiser l'essentiel de ce que l'on peut raisonnablement admettre comme acquis concernant cette forme d'espionnage électronique et de décrire, le plus fidèlement possible, le processus par lequel ce sujet opaque et longtemps resté l'apanage de quelques experts a pu devenir un thème politique, juridique et – par certains côtés – éthique, dont le traitement et les conséquences ne seront pas sans effet sur les relations euro-américaines dans la prochaine décennie.

LA RÉALITÉ DE L'ESPIONNAGE ÉLECTRONIQUE TRANSNATIONAL

On connaît depuis plusieurs dizaines d'années les origines historiques de ce que nous appelons aujourd'hui « Echelon ». Il s'agit de la prolongation et de l'institutionnalisation – pour cause de guerre froide – de la coopération technique et opérationnelle scellée entre la Grande-Bretagne et les Etats-Unis durant la Seconde Guerre mondiale en matière de renseignement et de cryptanalyse.

(*) Franck Leprévost est Professeur au département de mathématiques de l'Université Joseph Fourier (Grenoble). Bertrand Warusfel est Maître de conférences à la faculté de droit de l'Université René Descartes (Paris V) et Conseil en propriété industrielle.

Les origines d'Echelon

Durant le second conflit mondial, on sait l'importance stratégique que prit rapidement l'exploitation du renseignement issu des interceptions radios et du décryptement des machines à chiffrer allemandes et japonaises (1). A une première collaboration engagée dans les premiers mois de la guerre entre les services français, polonais et britanniques (et qui permit notamment d'obtenir les premiers décryptages de la machine Enigma allemande) (2) succéda, en effet, dès l'entrée en guerre des Etats-Unis, une relation privilégiée entre les services britanniques et particulièrement la « *Government Code and Cypher School* » (créée en 1919 et rattachée au Foreign Office) de Bletchley Park et les services de renseignement électromagnétique de l'armée américaine (3). Et cette coopération – démarrée officieusement dès la fin de 1940 – fut concrétisée par l'accord BRUSA (Britain-USA) signé en mai 1943 (4).

Et dès cette époque, les services britanniques et américains utilisaient leurs moyens d'écoute et de déchiffrement non seulement pour contrer les menaces militaires de l'Axe, mais également pour surveiller les menées soviétiques dans le monde. On connaît aujourd'hui, par exemple, l'existence des déchiffrements « *Mask* » effectués par la GCCS à la fin des années trente sur les interceptions des communications radio entre les communistes britanniques et le Komintern (5). Mais on sait surtout qu'à partir de 1939, l'US Army's Signal Intelligence Service (devenue ensuite « *Signal Security Service* », puis « *Signal Security Agency* ») enregistra les communications diplomatiques soviétiques (en particulier, celles entre Moscou et les Etats-Unis) et entreprit à partir de février 1943 de les déchiffrer dans le cadre d'un programme secret d'abord dénommé « *Bride* », puis « *Venona* » et auquel fut ensuite associé en 1948 le service d'interception britannique GCHQ (qui succédait à la GCCS) (6).

(1) Cf. notamment F.W. WINTERBOTHAM, *The Ultra Secret*, Weidenfeld & Nicolson, Londres, 1974, traduction française : *Ultra*, Robert Laffont, 1976 et pour les décryptements des chiffres japonais, James RUSBRIDGER et Eric NAVE, *Betrayal of Pearl Harbor – How Churchill Lured Roosevelt into World War II*, Simon & Schuster, New York, 1991, traduction française : *Trahison à Pearl Harbour – Comment Churchill a entraîné Roosevelt dans la Seconde Guerre Mondiale*, Pygmalion/Gérard Watelet, 1992; Ronald W. CLARK, *The Man Who Broke Purple*, Weidenfeld & Nicolson, Londres, 1977.

(2) Cf. notamment – en ce qui concerne les témoignages du côté français – Gustave BERTRAND, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Plon, 1973 et Paul PAILLOLE, *Notre agent chez Hitler*, Robert Laffont, 1985.

(3) Cf. notamment Ralph ERSKINE, « Anglo-US Cryptological Co-operation », conférence au 5e colloque annuel de l'International Intelligence History Study Group, 18-20 June 1999 (résumé in *International Intelligence History Study Group Newsletter*, Vol. 7, n° 1, Summer 1999, http://intelligence-history.wiso.uni-erlangen.de/).

(4) Cf. R. ERSKINE, *op. cit.*; James BAMFORD, Puzzle Palace, p. 397.

(5) Cf. IIHSG Newsletter, vol. 5, n° 2 (hiver 1997); également *The Times*, 10 octobre 1997.

(6) Cf. notamment Nigel WEST, *Venona – The greatest secret of the Cold War*, Harper/Collins, Londres, 1999. Pour une présentation officielle de l'historique du programme Venona et la reproduction de transcriptions de messages soviétiques (déclassifiées en application du Freedom of Information Act), cf. le site officiel de la National Security Agency (http://www.nsa.gov/docs/venona/index.html). Ces décryptements Venona furent à l'origine de la découverte de plusieurs des affaires d'espionnage soviétique (Fuchs, Rosenberg, Bur-

Une fois la paix revenue en Europe et suite à l'apparition des premières tensions de la guerre froide (soviétisation des pays d'Europe centrale, crise de Berlin), les Américains et les Britanniques reconduisirent en 1947 leur accord BRUSA sous la nouvelle dénomination d'UKUSA (UK-USA). Selon l'ancien analyste de la NSA Perry Fellwock qui, le premier, révéla l'existence de cet accord en 1972 (7), cet accord fut signé à l'origine entre les agences de renseignement électronique des Etats-Unis (SSA, future NSA), du Royaume-Uni (GCHQ), du Canada (CBNRC) et d'Australie (DSD). Mais les informations divergent sur le nombre exact des signataires directs de cet accord : selon certaines sources, par exemple, l'accord de 1947 n'aurait été réellement signé que par les Américains et les Britanniques et ce n'est qu'en 1948 (date parfois mentionnée purement et simplement comme celle de l'accord lui-même) (8) que les trois autres agences anglo-saxonnes auraient à leur tour contresigné l'accord initial (9). Et, pour leur part, les Canadiens affirment que leur pays n'a jamais signé formellement l'accord (10) tout en reconnaissant collaborer aux échanges UKUSA et avoir conclu, en parallèle, en 1949 un accord direct de coopération bilatéral avec les Etats-Unis, dénommé « CANUSA » (11). Au-delà des agences anglo-saxonnes ainsi associées depuis les origines (et dénommées « *Second Party* » dans le jargon UKUSA), d'autres agences de pays alliés des Etats-Unis (identifiées comme « *Third Party Nations* ») paraissent participer à un moindre niveau à la coordination du recueil et de l'échange de certaines informations électroniques : il s'agirait de l'Allemagne, du Danemark, de la Grèce, de l'Italie, du Japon, de la Norvège, de la Corée du Sud, de la Thaïlande et de la Turquie (12), voire de la Chine (qui bien qu'étrangère au camp occidental, aurait accepté d'implanter deux sites d'interception à sa frontière avec l'URSS) (13).

Dans ce cadre, les interceptions des communications des pays socialistes et du Pacte de Varsovie se sont développées durant toute la guerre froide par toute sorte de moyens : d'une part, le branchement sur certains câbles

gess-Maclean, ...) et restèrent – de ce fait – longtemps l'un des secrets les mieux gardés de l'après-guerre. Le programme Venona ne fut officiellement arrêté que le 1er octobre 1980.

(7) Dans une interview (sous le pseudonyme de Winslow Peck) publié par le magazine contestataire *Ramparts*, Vol. 11, n° 2, août 1972, pp. 35-50 (« US Electronic Espionnage : A Memoir » reproduit in http://jya.com/nsa-elint.htm). Cf. *infra*.

(8) Cf. par exemple, Peter WRIGHT, *Spycatcher : The Candid Autobiography of a Senior Intelligence Officer*, Viking Penguin, 1987, p. 99 (pour la traduction française : Spycatcher, Robert Laffont, 1987, p. 117).

(9) Cf. Nicky HAGER, *Secret Power*, Craig Potton Publishing, 1996, p. 61.

(10) Le Premier Ministre Pierre Trudeau aurait notamment soutenu cette position dans une déclaration officielle devant le Parlement fédéral en 1974 (cf. *House of Commons Debates*, 10 janvier 1974, p. 9227.). Cf. également, James LITTLETON, *Target Nation : Canada and the Western Intelligence Network*, Lester and Orpen Dennys, 1986, p. 95.

(11) Cf. David J. BERCUSON et J.L. GRANATSTEIN, *The Dictionary of Canadian Military History*, Oxford University Press, 1992, p. 43. Selon d'autres sources, l'échange de lettres concrétisant l'accord CANUSA daterait du 15 septembre 1950 (cf. *Canada-US Arrangements in Regard to Defence, Defence Production, Defence Sharing,* Washington, DC Institute for Policy Studies, 1985, p. 31, cité par Jeffrey T. RICHELSON, *The US Intelligence Community*, New York, Ballinger, 1989 (Second Edition), p. 278).

(12) Cf. J. RICHELSON, *op. cit.*, p. 283.

(13) Cf. J. RICHELSON, *op. cit.*, pp. 280-281 ; également la carte mondiale des stations NSA publiée *in* Jacques BAUD, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 1997, p. 357.

de communication (14), ensuite, le recueil des émissions radio clandestines, enfin – à partir du milieu des années soixante – l'interception des faisceaux des satellites de télécommunication (15). Mais, à partir du début des années soixante-dix un certain doute commença à s'établir (au moins parmi les spécialistes) sur la nature des cibles de ces interceptions. C'est ainsi qu'en 1972 dans un entretien, qui fit alors scandale, un ancien analyste militaire de la NSA camouflé sous le pseudonyme de Winslow Peck (et aujourd'hui identifié sous son véritable nom de Perry Fellwock) indiqua notamment que ces capacités d'écoute et de décryptage américaines n'étaient pas uniquement tournées vers les pays socialistes mais qu'elles étaient aussi utilisées pour suivre les communications des autres pays occidentaux (comme la France) (16) ou comme celles de certaines « *third parties* » (17), voire celles de certains membres du second groupe, comme le Royaume-Uni ou le Canada (18). Mais ce n'est pourtant qu'au cours des années quatre-vingt-dix que l'attention des media et du débat public se fixa progressivement sur ce sujet. C'est aussi à cette période que fut révélé le terme « Echelon » comme étant le nom de code d'un des principaux programmes de coordination et d'échange des interceptions de communication conduit dans le cadre de l'accord UKUSA.

Description succincte des techniques mises en œuvre

D'après les informations officiellement rendues publiques – et celles plus nombreuses révélées par les différents enquêteurs et journalistes indépen-

(14) L'interception la plus célèbre (et l'une des moins efficaces, puisqu'elle fut dénoncée immediatement par un agent britannique travaillant pour le KGB) fut celle réalisée à Berlin grâce à un tunnel aboutissant aux câbles de télécommunication utilisés par l'état-major soviétique à Berlin-Est (cf. notamment Cf. David MARTIN, *The Wilderness of mirrors*, Harper & Row, New York, 1980, traduction française : *KGB contre CIA*, Presses de la Renaissance, 1981, pp. 102 à 124; également, à propos de la trahison par la « taupe » Blake : E.H. COOKRIDGE, *Shadows of a Spy – The Complete Dossier on George Blake*, Leslie Frewin Publishers, Londres, 1967, pp. 157-158).

(15) Les premières stations destinées à intercepter les communications passant par les satellites Interlsat auraient été construites par la NSA à partir de 1967 (James BAMFORD, *op. cit.*, p. 421). Mais leur nombre et leur répartition géographique auraient été accrus une dizaine d'années plus tard pour permettre une meilleure interception les nouvelles générations 4 et 5 des satellites Intelsat (cf. le second chapitre de l'ouvrage de Nicky HAGER, *Secret Power – New Zealand's Role in the International Spy Network*, Craig Potton Publishing, Nelson, NZ, 1996).

(16) L'ancien responsable du MI5, Peter Wright a reconnu plus récemment (dans son ouvrage publié en 1987) que le Royaume-Uni avait également cassé le code diplomatique français (dans le cadre d'une opération dénommée « *Stockade* ») et en avait partagé les premiers fruits avec les Américains en 1960 (cf. P. WRIGHT, *op. cit.*, p. 146, et p. 170 dans la traduction française).

(17) D'après David Kahn, les révélations faites en 1960 par les transfuges Martin et Mitchell (analystes de la NSA passés à l'Est) permirent de savoir que la NSA avait cassé, dans les années 50, les chiffres de plusieurs nations, y compris alliés, comme la France, l'Italie ou la Turquie (cela fut également confirmé à propos de la crise de Suez).

(18) Fellwock/Peck indiquait notamment que depuis la base militaire américaine de Chicksands au Royaume-Uni et depuis les locaux de l'ambassade américaine à Londres, la NSA interceptait les communications diplomatiques britanniques (*Ramparts, op. cit.*). De son côté, Mike Frost, ancien membre du service canadien de renseignement électronique (le CSE, Communications Security Establishment, ex-CBNRC), affirme que l'ambassade américaine à Ottawa possède des équipements d'interception orientés vers les bureaux du Premier Ministre fédéral (cité par Bruce LIVESEY, « Trolling for Secrets – Economic Espionage is the New Niche for Government Spies », *Financial Post*, 28 février 1998).

dants travaillant sur cette question – le processus de collection, de traitement et de gestion de l'information au sein du programme Echelon apparaît comme particulièrement structuré. Il s'en dégage schématiquement quatre étapes selon le rapport Campbell rédigé pour le Parlement européen en 1999 (19) : tout d'abord, il convient de planifier les besoins (identifier les données ciblées, donner des priorités, etc.), et les moyens à mettre en œuvre pour les satisfaire. Il s'agit ensuite d'accéder aux media de communication, afin de pouvoir effectuer des interceptions. La sophistication des moyens de communication (par exemple, satellites ou câbles sous-marins de fibres optiques sont utilisés pour la télévision, le téléphone, le fax, etc.). A l'interception suit la récolte des informations, qui est ensuite convertie sous un format exploitable pour l'analyse, soit humaine, soit automatisée. A ce stade, il peut être nécessaire d'effectuer des traductions, ou des explications de texte (remplacer par exemple « msg » par « message »). Il convient enfin d'évaluer ces informations dans des rapports destinés au demandeur. Le jargon professionnel désigne par COMINT et SIGINT certaines des étapes ainsi décrites. Plus précisément, la NSA désigne par COMINT (Communications intelligence) les informations et renseignements techniques dérivés de l'interception de transmission par des tiers (20). Ces activités de COMINT de la NSA ne doivent pas juridiquement couvrir l'écoute des media publics ni les écoutes téléphoniques ou de messages oraux effectués au cours d'opérations de contre-renseignement sur le territoire américain (21). Dans le concept américain (et désormais international) du renseignement technique, COMINT est une composante importante du SIGINT, qui concerne la récolte de tous signaux (y compris par exemple ceux émis par les radars).

L'interception proprement dite des communications internationales peut se faire à l'aide de tout un arsenal de moyens, qui est fonction des caractéristiques techniques des moyens de communication ciblés.

Ainsi, l'interception d'ondes radio haute fréquence est assez simple, de par la structure même de ces ondes, qui « rebondissent » sur l'ionosphère et sur la surface de la terre. Selon Campbell, la NSA et le GCHQ ont procédé de telles interceptions de manière routinière entre 1945 et le début des années quatre-vingt, en particulier à partir de Chicksands (Angleterre), à l'aide de l'antenne AN/FLR9 (ces antennes ont environ 400 mètres de diamètre). D'autres systèmes de communication ont été introduits, en particulier les micro-ondes radio dans les années cinquante pour favoriser les communications à haute capacité de ville à ville pour le téléphone, le télégraphe et ulté-

(19) Duncan CAMPBELL, « The State of Art in Communications Intelligence (Comint) of Automated Processing for Inteligence Purposes of Intercepting Broadband multi-language Leased or Common Carrier System, and its Applicability to Comint Targeting and Selection, Including Speech Recognition » (Stoa PE 168.184/part. 4/4 avril 1999).

(20) Cf. J. BAUD, *op. cit.*, p. 121.

(21) Cf. notamment la directive 5200.24 du Department of Defense ; également, le témoignage du général Michael Hayden, directeur de la NSA devant le comité du renseignement de la Chambre des représentants, le 12 avril 2000.

rieurement la télévision. Les stations de relais des transmissions sont, en raison de la courbure de la surface de la terre, en général éloignées les unes des autres de 30 km à 50 km. Les communications longues distances ainsi réalisées peuvent transiter par plusieurs douzaines de stations relais. En fait, chacun des relais ne récupère qu'une partie du signal original, le reste allant vers l'espace, où des satellites peuvent le récupérer (il est d'ailleurs souhaitable de placer un tel satellite, non pas à la verticale d'une station relais, mais à 80 degrés de longitude). Selon Campbell, le premier satellite américain espion destiné à ces fins, CANYON, a été lancé en août 1968, suivi bientôt d'un second, contrôlés depuis la station terrestre de Bad Aibling en Allemagne. Du succès de CANYON est né son successeur CHALET (renommé ensuite VORTEX, puis MERCURY), géré par la station terrestre de Menwith Hill (Angleterre). Cette base gère d'ailleurs depuis 1994 un nouveau réseau de satellites SIGINT.

De nouveau, selon le rapport Campbell, plusieurs générations de tels satellites se sont succédé. Bien que les détails précis manquent concernant les satellites lancés après 1990, il semble que les systèmes de collection d'information aient crû. Les stations terrestres principales sont : Buckley Fielf, Denver (Colorado), Pine Gap (Australia), Menwith Hill (Angleterre), Bad Aibling (Allemagne). Le coût des satellites et de l'infrastructure *ad hoc* est de l'ordre de 1 Mrd de dollars US chacun. Il semblerait que les Etats-Unis soient en mesure d'intercepter les signaux de communications mobiles et les micro-ondes radio ville-à-ville en tout point de la planète. Cela étant, compte tenu des difficultés d'exploitation, il est vraisemblable que les cibles visées soient celles présentant les plus grandes priorités nationales, en particulier militaires. Il semblerait qu'aucune autre nation n'ait développé des satellites comparables : les projets ZIRCON de la Grande-Bretagne et ZENON de la France n'ont pas abouti. Depuis le début des années soixante-dix, des stations ont été construites pour intercepter les informations transitant par Intelsat (par exemple, Morwenstow en Cornouailles, Yakima, dans l'Etat de Washington, ou encore Sugar Grove, en Virginie occidentale). En se basant sur le nombre d'antennes installées sur les stations d'interception COMSAT ou SIGINT, il semblerait que les nations de l'accord UKUSA interceptent à l'heure actuelle environ 120 satellites. Les opérateurs téléphoniques ont également mis en place des nouveaux réseaux de satellites à basse altitude, comme le réseau Iridium par exemple, permettant ainsi une couverture globale de la planète. Cette stratégie semble avoir posé de nouveaux problèmes aux centrales d'écoute, car les satellites ainsi mis en place bougent très vite, et relaient les signaux directement entre eux ou vers une destination quelconque, mais très restreinte de la planète. Les informations peuvent également transiter par des câbles, y compris sous-marins (qui sont en particulier utilisés pour faire passer des fibres optiques). Là encore, il

semblerait que les communications transitant par ce media ne soient pas à l'abri d'interceptions.

Depuis quelques années, on constate aussi une augmentation très importante des communications liées à Internet. Les informations transitant sur Internet sont typiquement coupées en « paquets » (datagrams). Ces paquets contiennent en particulier tant leur adresse de départ que celle d'arrivée (adresses IP, ou Internet Protocole). Ces adresses identifient de manière unique tout ordinateur relié à Internet. Depuis le début des années quatre-vingt-dix, des systèmes ont été développés pour la récolte, le filtrage et le traitement des informations transitant sur Internet. Les chemins pris par les paquets Internet dépendent de l'origine et de la destination des données, ce qui est indiqué dans les adresses IP. Bien entendu, la plupart des échanges sur Internet ne sont que de peu de valeur du point de vue COMINT. D'après le rapport Campbell (22), la NSA aurait installé des « sniffers », chargés de récolter les informations intéressantes sur neuf points d'interconnection Internet (IXP).

Selon le rapport Campbell, le programme Echelon se caractérise par une grande automatisation des tâches de collecte et de traitement des données recueillies par les différentes stations d'interception appartenant aux services de l'alliance UKUSA. Il utilise les réseaux de communication de type Internet de la NSA et du GCHQ, afin de permettre aux opérateurs partenaires décentralisés d'utiliser leurs ordinateurs de manière locale, et recevoir automatiquement les résultats des recherches opérées. L'outil clef de ce système est présenté sous la forme de « dictionnaires » locaux, qui sont en fait des mémoires stockant une liste exhaustive des cibles (noms, mots clefs, adresses, numéros de téléphone, etc.). Les contenus des messages interceptés sont comparés à cette liste, et ceux identifiés comme présentant un intérêt selon ces critères sont alors traités. Un certain nombre de brevets ont d'ailleurs été déposés par la NSA pour protéger des technologies spécifiques de tri et d'extraction des données interceptées (23).

Un autre aspect important concernant Echelon est que, avant cette automatisation, les pays et les stations impliquées dans le recueil savaient ce qui était intercepté et à qui cela était destiné (puisqu'une partie du tri était effectué localement avant d'être transmis au service demandeur). Mais maintenant, l'essentiel des messages sélectionnés par les ordinateurs formant le système des « dictionnaires » répartis de par le monde sont renvoyés vers la NSA ou les autres clients, sans être lus ou traités localement.

Si Echelon n'est donc pas un nouveau réseau d'interception (comme on le croit souvent), il s'agit cependant d'un progrès radical dans la manière de

(22) Voir aussi Wayne MADSEN, « Puzzle Palace Conducting Internet Surveillance », *Computer Fraud and Security Bulletin*, juin 1995.

(23) Par exemple, le brevet US5418951 déposé par la NSA en mai 1995 (« Method of Retrieving Documents that Concern the Same Topic »), et poursuivant le brevet US 07/932522 déposé en août 1992.

gérer à l'échelle mondiale les interceptions électroniques. Cela explique sans doute pourquoi la découverte de son existence et de certains des détails de son fonctionnement ont engendré un véritable débat transatlantique.

Echelon, ou la naissance d'un débat euro-américain

Comme nous l'avons indiqué dans la première partie de cet article, les activités d'interception des télécommunications internationales sous l'égide de la NSA existent depuis l'après-guerre et sont connues – au moins dans leur principe – depuis plusieurs décennies. Mais il est clair que les révélations du journaliste britannique Duncan Campbell à la fin des années quatre-vingt et la popularisation progressive du nom « Echelon » au cours des années quatre-vingt-dix ont donné au débat autour de cette question une nature publique et, du même coup, de plus en plus politique, qui a culminé en 1999 avec la publication par le service des études du Parlement européen (STOA) de quatre rapports indépendants (24). Il est donc utile de revenir sur cette chronologie d'un débat qui s'est progressivement déplacé du cercle étroit des spécialistes du renseignement vers des enceintes plus politiques et mediatiques.

Echelon avant Echelon : les informations sur les interceptions de la NSA avant 1988

Si la première mention explicite des accords UKUSA remonte à l'interview, précédemment citée, publiée par *Ramparts* en 1972, chacun s'accorde à considérer que le premier ouvrage significatif ayant décrit le contexte global des activités de renseignement électronique américaines fut le livre très remarqué de James Bamford « *The Puzzle Palace* » paru en 1982 et entièrement consacré à la NSA. Cet ouvrage ne se contentait pas d'indiquer l'existence de la coopération entre agences UKUSA, il indiquait également et, apparemment pour la première fois, que la NSA s'était dotée en particulier de moyens informatiques spécifiques pour traiter les volumes d'interception en permettant la détection de mots-clés dans les communications interceptées (25).

S'engouffrant ensuite dans la brèche ouverte par l'interview du soi-disant Winslow Peck puis par Bamford, plusieurs autres ouvrages journalistiques furent publiés qui décrivaient les méthodes et certains moyens employés par la NSA et ses alliés. On citera notamment, le livre de Jeffrey Richelson (aujourd'hui, chercheur au centre indépendant *National Security Archive* et, à ce titre, l'un des principaux responsables de la déclassification et de la

(24) Cf. *infra*.
(25) Cf. James Bamford, *op. cit.*, p. 418.

publication de documents administratifs sur la NSA et Echelon (26) et Desmond Ball's, *The Ties that Bind*, paru en 1985 (27) ainsi qu'en 1986 le livre du producteur de la télévision canadienne James Littleton, *Target Nation – Canada and the Western Intelligence Network* (28).

Mais à la même période, le journaliste alternatif britannique Duncan Campbell avait également commencé à suivre cette question des écoutes électroniques et du rôle qu'y jouait le Royaume-Uni. Il explique que son premier article en 1976 (29) fut écrit après qu'il eut rencontré Fellwock *alias* Winslow Peck à Londres lors de la visite que celui fit en Grande-Bretagne cette année-là. Son but était de réaliser, s'agissant de la Grande-Bretagne et du GCHQ, « *l'équivalent de ce qu'avait fait Winslow pour les USA et la NSA* » (30). Cet article eu tellement d'effets dans les milieux gouvernementaux qu'il donna lieu à une action en justice pour révélation d'informations classifiées et donna lieu en 1978 à un procès retentissant et relativement rocambolesque, qui demeure connu dans les annales judiciaires britanniques sous le nom de l'affaire *ABC* (en raison des initiales des trois inculpés, dont Campbell (31).

Il récidiva ensuite en 1980 avec un article spécialement consacré à la base de Menwith Hill, qu'il décrivit comme étant la principale base d'écoutes américaine en Europe occidentale (32). Mais c'est dans son article d'août 1988 du *New Statesman* relatant la découverte aux Etats-Unis de l'existence d'écoutes à l'encontre d'un politicien du Sud par le témoignage d'une employée américaine à Menwith Hill, qu'il mentionna que parmi les différents programmes secrets menés par la NSA, un programme d'informatisation du contenu des interceptions (à partir de mini-ordinateurs VAX) était dénommé « Echelon » et que différentes stations étaient situées au-dehors des Etats-Unis (dont Menwith en Grande-Bretagne ou encore les deux sites chinois déjà mentionnés) (33). Le terme ne fut pas immediatement repris par les media, mais lorsque d'autres publications vinrent progressivement fournir de nouvelles informations sur la manière dont pouvait fonctionner ce système intégré de traitement des interceptions, Echelon commença à être identifié – de manière quelque peu abusive – comme synonyme de toutes les pratiques d'espionnage électronique organisées au niveau mondial par les Etats-Unis, alors qu'il ne s'agit, en réalité, que de l'un des aspects

(26) Cf. le site de la National Security Archive : http://www.gwu.edu/_nsarchiv/.

(27) Desmond BALL and Jeffrey RICHELSON, *The Ties That Bind : Intelligence Cooperation Between the UKUSA Countries*, Allen & Unwin, Boston, 1985.

(28) *Op. cit., supra.*

(29) Duncan CAMPBELL & Mark HOSENBALL, « The Eavesdroppers », *Time Out*, juin 1976.

(30) Duncan CAMPBELL, « The Discovery of Global Sigint Networks : The early years – Part 2 ».

(31) Sur certains aspects de ce procès, cf. Bertrand WARUSFEL, *Contre-espionnage et protection du secret – Histoire, droit et organisation de la sécurité nationale en France*, Lavauzelle, 2000, p. 342.

(32) Duncan CAMPBELL and Linda MELVERN, « America's Big Ear on Europe », *New Statesman*, 18 juillet 1980, pp. 10-14.

(33) « They've got it taped », *New Statesman*, 12 août 1988, pp. 10-12 (reproduit in http://jya.com/echelon_dc.htm).

de ces pratiques. Mais avec cette généralisation sémantique, l'attention du public et des autorités politiques put se fixer plus facilement sur un symbole. Et c'est avec les rapports commandés par le Parlement européen à plusieurs experts indépendants, dont Duncan Campbell, que s'ouvrit sur le sujet un débat politique de grande ampleur.

La cristallisation du débat autour des rapports du Parlement européen

L'amplification progressive des révélations autour d'Echelon et des activités de la NSA aux débuts de la dernière décennie fut largement accélérée par les effets de la chute du Mur de Berlin puis la disparition du Pacte de Varsovie et de l'Union soviétique. En effet, la fin de la guerre froide qui s'ensuivit fit perdre aux systèmes de renseignement électronique occidentaux une partie de ce qui était leur légitimité essentielle, à savoir la surveillance étroite des activités soviétiques et la détection anticipée d'éventuels préparatifs militaires à l'Est. On vit d'ailleurs certains pays démanteler certaines de leurs stations d'écoute anciennement dirigées vers la frontière orientale (comme ce fut le cas de certaines stations militaires françaises en Allemagne et à Berlin) (34). Mais au bout de quelques années, il apparut que – pour l'essentiel – les moyens de recueil électronique des Etats-Unis et de leurs principaux associés d'UKUSA demeuraient stables, voire se renforçaient dans certaines régions (comme à proximité du Moyen-Orient). Et si la guerre du Golfe et certaines menaces de prolifération (notamment du côté de la Corée du Nord) furent présentées comme justifiant un renforcement des mesures d'interception (en vue de détecter les « *bad guys* » de la politique mondiale), le soupçon grandit parmi les experts et une partie de l'opinion quant à un possible repositionnement du renseignement électronique en direction des intérêts économiques et commerciaux des Etats-Unis.

Et une nouvelle fois, cette suspicion fut particulièrement forte dans les pays anglo-saxons partenaires (les « *Second Parties* ») de l'UKUSA. Après les révélations de Campbell en Grande-Bretagne et de Littleton au Canada, deux nouveaux ouvrages parurent, l'un au Canada, l'autre en Nouvelle-Zélande. Le premier fut rédigé en 1995 par Mike Frost, ancien officier du CSE canadien, qui décrivait notamment les méthodes d'interception radio et micro-ondes mises en œuvre à partir des différentes ambassades américaines ou de pays participant à UKUSA (35). Le second fut publié en Nouvelle-Zélande en 1996 sous le titre accrocheur « *Secret Power* » (36). Il étudiait de façon détaillée des activités de renseignement électronique du service néo-zélandais, le GCSB (le Government Communications Security

(34) Cf. notamment, *Le Monde*, 30/31 mai 1993 et 16 juin 1993.

(35) Mike FROST et Michel GRATON, *Spyworld : How CSE Spies on Canadians and the World*, Seal/McClelland-Bantam, Toronto, 1995.

(36) N. HAGER, *op. cit.* (cf. pour des extraits : http://www.fas.org/irp/eprint/sp/index.html).

Bureau, dont il révélait notamment que l'un des principaux directeurs avait été entre 1984 et 1987 un officier américain de la NSA) et décrivait l'intégration dans le réseau d'interception piloté par la NSA des deux stations d'écoute néo-zélandaises de Tangimoana (spécialisée dans les interceptions radio) et de Waihopai (spécialisée dans les interceptions des satellites Intelsat au-dessus du Pacifique). Il précisait notamment le rôle que jouent dans le système informatisé Echelon les ordinateurs dénommés DICTIONARY chargés de la détection par mots-clés des messages et installés de manière décentralisée dans chaque station d'interception du réseau UKUSA (comme les deux stations néo-zélandaises). Et dans son introduction, l'ancien Premier Ministre néo-zélandais David Lange reconnaissait que, quand il avait pris la décision de créer la station de renseignement satellitaire de Waihopai (qui fut ouverte en 1989), il n'avait pas été informé par ses propres services de sécurité du fait qu'elle serait reliée au réseau mondial de la NSA, ainsi que le démontrait cet ouvrage (37).

Enfin, en 1997, les responsables de British Telecom durent reconnaître en justice que leur entreprise avait interconnecté leur réseau de télécommunications avec la station d'écoutes américaine de Menwith Hill, permettant ainsi à la NSA d'intercepter une part importante des communications transitant par le réseau de télécommunications à grande vitesse de l'opérateur historique britannique. Même si le juge de la cour de York accepta finalement de reconnaître le caractère confidentiel des détails d'une telle interconnexion et se contenta d'infliger à BT le paiement de dommages et intérêts, cette affaire fit grand bruit et renforça considérablement la crédibilité des révélations faites autour de l'UKUSA et du programme Echelon.

Tout cet ensemble d'informations fut repris et exploité en 1997-1998 par les consultants de la fondation Omega de Manchester qui avait été chargée par le service d'études du Parlement européen (STOA, Scientific and Technological Options Assessment) de réaliser une étude sur la question beaucoup plus large de l'« évaluation des techniques de contrôle politique » (38). Dans leur rapport intérimaire de 1998, les auteurs de cette étude, affirmèrent notamment, à propos des techniques d'interception électronique, que « *toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la National Security Agency des Etats-Unis, qui transfèrent toutes les informations provenant du continent européen via le centre stratégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York*

(37) « *We even went the length of building a satellite station at Waihopai. But it was not until I read this book that I had any idea that we had been committed to an international integrated electronic network* » (David LANGE *in* N. HAGER, *op. cit.*, p. 9).

(38) European Parliament, Scientific and Technological Options Assessment stoa, An appraisal of technologies of political control, working document (consultation version) Luxembourg, 6 janvier 1998, doc PE 166 499 (cf. *http://cryptome.org/stoa_atpc.htm,* et pour un résumé officiel : http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm).

Moors au Royaume-Uni. Le système a été mis au jour pour la première fois dans les années soixante-dix par un groupe de chercheurs au Royaume-Uni (Campbell, 1981). Des travaux menés récemment par Nicky Hager (Secret Power, Hager, 1996) fournissent des détails extrêmement précis sur un projet nommé ECHELON. (...) Le système ECHELON fait partie du système anglo-américain mais, à l'inverse de nombreux systèmes d'espionnage électronique développés au cours de la guerre froide, ECHELON vise essentiellement des cibles non militaires : des gouvernements, des organisations et des entreprises dans pratiquement tous les pays. Le système ECHELON fonctionne en interceptant sans distinction de très grandes quantités d'informations puis en en triant les éléments intéressants à l'aide de systèmes d'intelligence artificielle comme Memex, à la recherche de mots-clés. Cinq nations se partagent les résultats, les Etats-Unis faisant figure de partenaire principal en vertu de l'accord UK-USA de 1948 et la Grande-Bretagne, le Canada, la Nouvelle-Zélande et l'Australie ayant un rôle subalterne de fournisseurs d'informations ».

L'une des recommandations de l'étude Omega de 1998 ayant été de consacrer des recherches spécialement focalisées sur la question de l'espionnage électronique au niveau international et de la situation juridique des Européens face à cette menace, le STOA lança alors une étude globalement intitulée « *Development of surveillance technology and risk of abuse of economic information* » et destinée à la commission des Libertés Publiques et des Affaires Intérieures du Parlement européen. Cette étude fut constituée à partir de quatre rapports distincts confiés à quatre experts indépendants. Le premier de ces rapports, directement confié au journaliste et producteur de télévision écossais Duncan Campbell, visait à faire une synthèse des connaissances acquises concernant les activités de COMINT menées en particulier au travers du programme Echelon au niveau mondial (39). Un second rapport, rédigé par le mathématicien français Franck Leprévost (à l'époque chercheur au CNRS), présentait l'état de l'art en matière de technologie de sécurité susceptible de servir de parade aux interceptions électroniques (40). Un rapport juridique avait été confié au juriste britannique Chris Elliott (41). Enfin, le cabinet d'études Zeus situé à Patras a mené, sous la direction de Nikos Bogonikilos, un travail d'évaluation des conséquences économiques potentielles des pratiques d'interception électronique (42).

L'ensemble de ces quatre rapports – qui concluaient à l'existence d'une menace réelle sur la confidentialité des communications civiles et commer-

(39) D. Campbell, *op. cit.*, Stoa PE 168.184/part. 4/4, avril 1999.

(40) Franck Leprévost, « Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie » (Stoa PE168.184/part 3/4, avril 1999).

(41) Dr Chris Elliot, « The legality of the interception of electronic communications : a concise survey of principal legal issues and instruments under international, european and national law » (Stoa PE 168.184/part. 2/4 : avril 1999).

(42) « The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception » (Stoa PE 168.184/int.st/part1/4 : mai 1999).

ciales, notamment en Europe et de pratiques systématiques d'interception sous l'égide des Etats-Unis – déclencha une vive émotion dans l'opinion publique et les différentes classes politiques européennes alors même qu'elle suscitait une réaction embarrassée et très prudente de la Commission européenne. Et, au moins en ce qui concerne la France, le débat lancé à cette occasion, fut officiellement présenté comme étant l'une des causes de l'inflexion substantielle qu'a engagée le gouvernement de M. Jospin en ce qui concerne le contrôle des produits de cryptologie. Il est donc intéressant de rappeler les différentes facettes de ces réactions politiques, technologiques et juridiques et de s'interroger sur le sens qu'il faut leur donner.

DES RÉACTIONS INSTITUTIONNELLES QUI N'EXCLUENT PAS UN CERTAIN SCEPTICISME

Si le débat largement ouvert par la publication des rapports du Parlement européen a contribué à accélérer une certaine reconnaissance de l'existence du système par certains de ses participants, il faut surtout remarquer que les réactions politiques et institutionnelles sont restées la plupart du temps embarrassées ou qu'elles ont servi de prétexte à justifier des décisions politiques ou technologiques déjà prises. Il faut donc tâcher de conserver vis-à-vis de ce dossier une certaine distance critique.

Une reconnaissance partielle de l'existence du système

L'une des premières conséquences de la publication des différents rapports du Parlement européen a été sans doute la fin du silence absolu que respectaient les autorités gouvernementales des pays de l'alliance UKUSA et l'amorce – timide – d'une certaine forme de reconnaissance officielle.

Jusqu'à une période récente, en effet, l'existence même des accords UKUSA et de leurs activités coordonnées d'interception était niée par les représentants officiels des Etats concernés. Aux Etats-Unis en 1982, une demande de communication (sur la base du *Freedom of Information Act* américain) de documents officiels relatifs à l'accord UKUSA avait été rejeté par la NSA dans ces termes : « *Nous avons considéré que la question de savoir si les documents que vous demandez existent ou non est en elle-même une information qui demeure encore classifiée* » (43). Et, plus récemment, en avril 1997, le Premier Ministre australien de l'époque, Malcolm Fraser, aurait encore refusé de répondre « *pour des raisons de sécurité nationale* » à une question du leader de l'opposition, M. Bill Hayden, concernant la participation de l'Australie à cette alliance.

(43) Lettre d'Eugene Y. Yeates, Director of Policy, National Security Agency, 7 décembre 1982, citée par J. RICHELSON, *op. cit.* p. 269. (http://jya.com/usic12.htm).

Ce n'est qu'en mars 1999 que le directeur du service de renseignement électronique australien (DSD) en personne reconnut finalement lors d'une émission télévisée que son service « *coopère avec des services de renseignement électronique homologues étrangers dans le cadre des relations UKUSA* » (44). Et quelques mois auparavant, un ancien directeur de la NSA, William Odom (qui dirigea l'agence dans les années quatre-vingt), avait déjà reconnu – à titre personnel – l'existence des opérations d'interception internationale menées par son ancien service et leur réalisation en coopération avec d'autres pays anglo-saxons en déclarant : « *Bien sûr que ce genre d'opération existe, et alors ? Où est le scandale ? Tout le monde essaie d'en faire autant, vous les Français en premier. Mais vous bricolez dans votre coin. Nous, nous avons des accords avec l'Angleterre et le Commonwealth, et donc des moyens considérables. Il vous faudrait des années et des milliards de dollars pour avoir un dispositif comme le nôtre* » (45).

Allant moins loin dans ses déclarations, un autre ancien haut responsable du renseignement américain, James Woolsey, ancien directeur de la CIA, accepta également d'évoquer les conclusions des rapports STOA devant les journalistes en mars 2000. A cette occasion, il ne dit rien sur la pratique des interceptions par la NSA, mais se concentra sur les griefs d'utilisation de ces interceptions à des fins d'espionnage économique imputé aux Etats-Unis. Il précisa qu'à sa connaissance, les services de renseignement américain ne pratiquaient pas d'actions d'espionnage économique au profit des entreprises américaines et qu'ils n'engageaient d'actions secrètes pour la collecte d'informations économiques que dans trois cas particuliers : la surveillance des pays soumis à des sanctions internationales, les risques de détournement de produits et technologies à double usage ou proliférants et – enfin – les cas de corruption menées par des sociétés étrangères (46). Citant plus particulièrement les deux exemples relevés par le rapport de D. Campbell (l'un concernant le marché des radars au Brésil qui opposa Thomson et Raytheon et l'autre s'agissant de la négociation entre Airbus et l'Arabie Saoudite), il confirma indirectement l'existence de telles opérations de renseignement mais s'en justifia en affirmant que, dans les deux cas, il ne s'agissait que de détecter les manœuvres corruptrices du concurrent européen et non de véritable espionnage économique (47). Cela n'empêcha pas la presse européenne

(44) Martin Brady, Directeur de DSD, 16 mars 1999, Broadcast on the Sunday Programme, Channel 9 TV (Australia), 11 avril 1999.

(45) Interviewé par Vincent JAUVERT, « Téléphone, fax, Internet : tout peut être écouté – comment l'Amérique nous espionne », *Nouvel Observateur*, n° 1779, 10 décembre 1998, p. 10.

(46) « Former Cia Director Woolsey delivers Remarks at Foreign Press Center », 7 mars 2000, (reproduit dans http://www.cryptome_org/echelon_cia.htm).

(47) « *In the Campbell report there are only two cases mentioned in which, allegedly, American intelligence some years – several years ago obtained information – secret information regarding foreign corporations. One deals with Thomson-CSF in Brazil, one deals with Airbus in Saudi Arabia. Mr. Campbell's summation of those issues in one case is five lines long, in the other case it's six lines long, and he is intellectually honest enough that in both cases he devotes one line in each to the fact that the subject of American intelligence collection was bribery. That's correct. Not technological capabilities, not how to design wing struts, but bribery.* » (J. WOOLSEY, *op. cit.*)

de considérer que, par ces propos, l'ancien directeur central du renseignement américain avait lui aussi contribué à renforcer la véracité des affirmations contenues dans les rapports du Parlement européen (48).

Mais au-delà de ces quelques déclarations partielles et souvent officieuses, les responsables gouvernementaux des différents pays UKUSA sont demeurés extrêmement prudents. Ainsi, en particulier, le Foreign Office britannique a indiqué en février 2000 que les services de renseignement britanniques travaillaient exclusivement dans le cadre de la loi et que celle-ci n'autorisait les interceptions que pour la protection de la sécurité nationale ou dans les intérêts de la « sécurité économique » [*economic well-being*] britannique et excluait toute collecte massive et non discriminée d'informations (49). Quant au gouvernement allemand – bien que son pays ne soit qu'un partenaire de second rang d'UKUSA – il est resté très évasif face aux questions du Bundestag sur ce sujet, se contentant d'indiquer « *qu'il avait pris connaissance des rapports du Parlement européen mais qu'il ne disposait pas d'informations sur l'état actuel de la coopération entre membres du pacte UKUSA ou sur les risques qu'Echelon pourrait représenter pour la vie privée des citoyens ou la compétitivité de l'économie allemande* » (50).

C'est dans ce contexte que les autorités communautaires (impliquées indirectement du fait des rapports commandés par le Parlement européen) et les gouvernements des pays européens non membres d'UKUSA (la France, en particulier) ont été amené à réagir à leur tour et à participer au débat public qui s'est instauré autour de ce sujet.

Des réactions politiques embarrassées

Au niveau des institutions communautaires, les réactions politiques furent embarrassées et limitées. Ce fut d'abord celle de Martin Bangemann, alors commissaire allemand dans la Commission Santer qui, intervenant devant le Parlement européen en 1998 affirmait qu'il n'avait aucun moyen de savoir si le système Echelon existait ou non (51). Mais l'intervention des rapports du STOA en 1999 relança les discussions et obligea la Commission à se prononcer à nouveau publiquement.

Par la voie de son nouveau commissaire à la société de l'information au sein de la commission Prodi, M. Erkki Liikanen, la Commission déclara alors en substance, devant le Parlement européen le 30 mars 2000, que la question ne pouvait être abordée par les institutions communautaires que dans

(48) Cf. par exemple la chronique de la BCC : Martin Asser, « Echelon : Big Brother without a Cause ? », *BBC News Online*, 6 juillet 2000.

(49) Cf. Guardian Unlimited, 24 février 2000.

(50) Cité *in* Assemblée nationale, *Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale,* par M. Arthur Paecht, document n° 2623, 11 octobre 2000.

(51) « *Ich kann Ihnen also jetzt weder positiv noch negativ sagen, daß dieses System existiert* » (Intervention de M. M. Bangemann, Parlement européen, 14 septembre 1998.

la limite des compétences spécifiques que leur confiaient les traités européens, ce qui limitait leur intervention au domaine de la protection des données personnelles et – pour partie – aux aspects de sécurité publique relevant du troisième pilier de l'Union européenne (en excluant les questions de sécurité nationale, qui demeurent « *de la compétence exclusive des Etats membres* », ainsi que tout ce qui touche aux activités de renseignement) (52). Dans cette même déclaration, le commissaire européen indiquait, par ailleurs, que la Commission avait interrogé tout à la fois les gouvernements britannique et américain. S'agissant du Royaume-Uni, il signala que son représentant permanent avait répondu que les agences de renseignement britanniques réalisaient des interceptions, pour différents motifs d'intérêt national, de protection de la sécurité économique ou de lutte contre certaines activités criminelles majeures, dans le cadre de la loi britannique et que celle-ci avait été jugée compatible avec les exigences européennes en matière de droits de l'homme. Quant au gouvernement américain, il avait répondu à la demande de la Commission en réaffirmant que la communauté américaine du renseignement n'était pas impliquée dans des activités d'espionnage économique et n'acceptait pas de travailler pour le compte d'intérêts privés, que ce soit en matière commerciale, technologique ou financière.

La prudence de ces prises de position peut sans doute être imputée à plusieurs facteurs. Le premier exprimé dans l'intervention de M. Liikanen tient aux limites juridiques des institutions communautaires. Dans la mesure où ces pratiques de renseignement électronique sont exercées dans le cadre des prérogatives de chaque Etat en matière de sécurité et de défense, il paraît toujours difficile à l'Union européenne d'intervenir dans ces domaines que tous les Etats membres considèrent généralement comme leur « pré carré » et qui ne sont pas couverts explicitement par les mécanismes communautaires (mais ne peuvent ressortir que de mécanismes de coopération intergouvernementaux dans le cadre, en particulier, des second et troisième piliers du Traité de l'Union). Mais cet argument juridique n'est pas suffisant à lui seul, car on a déjà vu dans le passé les institutions communautaires s'intéresser de près à des sujets sensibles touchant la sécurité nationale (comme, par exemple, le contrôle des exportations de technologies à double usage (53). Plus important, sans doute, la position de la Grande-Bretagne, cofondateur d'UKUSA et supposé adjoint zélé des Etats-Unis dans le développement des interceptions Echelon tout en étant membre de l'Union européenne, explique la retenue des commissaires européens successifs. Mais à cela s'ajoute sans doute également le fait que les instances communautaires

(52) Commission Statement in the European Parliament, 30 mars 2000 under agenda point « Déclarations du Conseil et de la Commission. Système 'Echelon', sur l'existence du système d'intelligence artificielle permettant aux Etats-Unis d'Amérique d'intercepter et de surveiller toutes les communications téléphoniques et électroniques de l'Union européenne » (Discours d'Erkki Liikanen, Commissaire européen chargé d'Entreprise and Information Society, Parlement européen, Bruxelles, 30 mars 2000).

(53) Domaine aujourd'hui largement communautarisé par le nouveau règlement n° 1334/2000.

(et leurs agences spécialisées, comme Europol) sont également impliquées dans un dialogue technique avec les Etats-Unis (représenté plus particulièrement par sa police fédérale, le FBI – lequel a développé son propre système d'interception du courrier électronique, dénommé *Carnivore* et actuellement fort contesté aux Etats-Unis même) pour concevoir entre Européens et Nord-Américains un concept unifié de protection contre la cybercriminalité, laquelle passerait notamment par l'harmonisation des systèmes d'écoute téléphoniques et électroniques des différents services de police en vue de favoriser leur coopération transnationale.

Cette ambiguïté entre une certaine indignation politique des Européens et la volonté de la plupart des Etats membres ainsi que de la Commission elle-même, de prendre des mesures préventives en matière de lutte contre la criminalité informatisée, est également perceptible dans les réactions politiques françaises.

En France, la principale réaction officielle fut celle du garde des Sceaux, M^me^ Elisabeth Guigou, qui répondit au député Georges Sarre le 23 février 2000 qui l'interpellait sur ce dossier (54). Dans sa réponse, la ministre confirma l'existence du système d'interception : « *Le système Echelon a en effet été mis en place par les Etats-Unis en 1948, avec le concours de la Grande-Bretagne, du Canada, de la Nouvelle-Zélande et de l'Australie, ce afin de recueillir des informations militaires sur d'éventuels adversaires* », et releva les risques d'éventuel détournement : « *mais aujourd'hui, il semble que ce réseau soit utilisé à des fins d'espionnage économique et de veille concurrentielle. Nous devons donc nous montrer particulièrement vigilants!* » Mais sa réponse ne mit en avant aucune prise de position politique ou diplomatique et se contenta de relever les efforts engagés parallèlement par le gouvernement Jospin pour renforcer la sécurité des communications tant contre les risques d'interception (notamment en autorisant la pratique du chiffrement, cf. *infra*) que contre les autres formes de la « criminalité informatique » (à l'encontre de laquelle M^me^ Guigou citait la création récente d'un office central spécialisé au sein de la Direction générale de la police nationale). Le ministre de l'Intérieur de l'époque, M. Jean-Pierre Chevènement, réagit dans le même sens et se contenta essentiellement d'appeler à la « *vigilance* » et à « *la prudence et la discrétion des utilisateurs* ».

En voulant rapprocher la question du renseignement électronique transnational de celle des autres formes d'atteinte à la sécurité de l'information, les ministres français ont eux aussi biaisé leurs réponses. Non seulement il est difficile de confondre les interceptions d'Etat organisées dans le cadre de l'alliance UKUSA avec les autres formes de délinquance informatique, mais – comme nous l'avons déjà remarqué – il s'agit, en pratique, de deux thèmes qui peuvent devenir frontalement antagonistes. En effet, l'organisa-

(54) Assemblée nationale, Session ordinaire de 1999-2000 – 56^e^ jour de séance, 132^e^ séance, 1^re^ séance du mercredi 23 février 2000.

tion des forces de sécurité à l'encontre de la cybercriminalité conduit naturellement au renforcement des méthodes d'interception des communications et de surveillance des réseaux numériques et, d'ores et déjà, les principaux services spécialisés français de police et de gendarmerie, ainsi que nos deux centrales de renseignement extérieur (la DGSE – Direction générale de la sécurité extérieure – et la DRM – Direction du renseignement militaire) accroissent leurs moyens en ce sens. De ce fait, le développement – nécessaire – de la lutte contre la délinquance électronique passe plutôt par une coopération renforcée avec tous les services spécialisés à l'échelle internationale (y compris – et surtout – la NSA et le FBI) que par la dénonciation des pratiques de certains d'entre eux.

Mais, s'agissant du cas particulier de la France, on a pu constater que le gouvernement de M. Jospin avait profité de ce débat pour justifier – en partie *a posteriori* – une évolution récente de sa politique nationale en matière de contrôle de la cryptologie. On sait, en effet, que la France est le seul pays occidental (à l'exception partielle des Etats-Unis) à avoir maintenu une réglementation très stricte en matière de fourniture et d'utilisation des moyens de cryptologie, et particulièrement des moyens de chiffrement (55). Confronté depuis plusieurs années à la pression des industriels des technologies de l'information et à la demande des entreprises soucieuses de sécuriser les nouveaux services Internet et de commerce électronique, le gouvernement français a décidé en 1999 une libéralisation significative de ses procédures de contrôle. Il est clair que la publicité faite autour d'Echelon et des pratiques anglo-saxonnes d'interception est arrivée au bon moment pour donner l'occasion au gouvernement français de justifier son changement de position par la volonté de protéger notamment les entreprises françaises contre les risques d'espionnage électronique et économique. C'est – du point de vue français (mais aussi européen, puisque indirectement, le changement de la position française va débloquer les possibilités d'harmonisation européenne en la matière) – une dimension non négligeable de la gestion du dossier Echelon.

Une justification franco-française de la nouvelle politique en matière de cryptologie

Rappelons rapidement ce que sont les méthodes cryptographiques et en quoi elles peuvent apporter une réponse technique face au risque d'interceptions électroniques du type de celles apparemment pratiquées dans le cadre de l'UKUSA.

(55) Pour une rapide synthèse de ce sujet, on se reportera à notre chronique dans cette même revue, Bertrand Warusfel, « Dix ans de réglementation de cryptologie en France : du contrôle étatique à la liberté concédée », *Annuaire Français des Relations Internationales*, Bruylant, n° 1, mars 2000, pp. 657-661.

Les méthodes de protection des systèmes de communication sont de natures diverses, fonction de la menace ressentie. Les objectifs de la cryptographie sont précisément d'assurer l'intégrité, la confidentialité et l'authentification des données.

La cryptographie se sépare grossièrement en deux catégories : cryptographie à clef secrète et cryptographie à clef publique. La cryptographie à clef secrète de nouveau se subdivise en deux écoles : celle dite des « *stream ciphers* » et celle des « *blocks ciphers* ». Concernant les « *stream ciphers* », nous dirons seulement ici qu'ils codent un message bit à bit. Les « *blocks ciphers* » traitent l'information par blocs. Ils utilisent la même clef pour chiffrer un bloc que pour le déchiffrer. Le plus célèbre de ces algorithmes est le DES (Data Encryption Standard), estampillé FIPS (Federal Information Processing Standard) 46-2 du NIST (National Institute of Standard and Technology) en 1977. La longueur de la clef secrète est de 56 bits, et traite des blocs de 64 bits. Il est apparu ces dernières années que le DES n'offrait plus une sécurité suffisante, et le NIST a demandé à la communauté cryptographique mondiale de réfléchir et proposer de nouveaux algorithmes répondant à des critères publics, afin de définir l'AES (Advanced Encryption Standard). Le candidat le plus en vue est une proposition belge, appelée RIJNDAEL, seule retenue début octobre 2000 pour le troisième tour d'évaluation. Si aucune faiblesse irrémediable n'est mise au jour, il est vraisemblable que RIJNDAEL changera de nom en devenant l'AES au cours de 2001. Il traitera des blocs de taille 128 bits, avec des clefs de longueurs variables (128, 192, 256 bits). En fait, il sera suffisamment souple pour traiter des blocs de taille 64 bits, et sera efficace sur des plates-formes variées (processeurs à 8 bits, réseaux ATM, communications satellitaires, HDTV, B-ISDN, etc.).

L'un des problèmes de la cryptographie à clef secrète concerne la gestion des clefs. En effet, il est nécessaire d'avoir autant de clefs secrètes que de correspondants, ce qui devient très rapidement fort complexe. Une réponse à ce problème est fournie par la cryptographie à clef publique. Dans cette approche, chaque correspondant possède non pas une, mais deux clefs. L'une est secrète, l'autre est publique. Par exemple, si Alice et Bob (ces noms sont standards en cryptographie) souhaitent communiquer, Alice dispose d'une clef secrète x_A et d'une clef publique y_A, *mutatis mutandis* pour Bob. Si Alice souhaite envoyer un message à Bob, elle cherche la clef publique y_B de Bob, chiffre son message avec cette elle, et envoie le message ainsi crypté à Bob. Les clefs publiques et privées sont reliées par une certaine fonction, et seul Bob, avec sa clef secrète x–B est en mesure de déchiffrer le message d'Alice. La sécurité de ces protocoles repose sur des problèmes mathématiques. Le projet P1363, commencé en 1993 et achevé en août 2000, a, sous l'égide du comité de standardisation de l'IEEE (Institute of Electrical and Electronical Engineers), standardisé un certain nombre

d'algorithmes, de schémas et de protocoles de cryptographie à clef publique (56).

En pratique, on utilise rarement la cryptographie à clef publique toute seule, mais plutôt en la combinant avec la cryptographie à clef secrète. En effet, les protocoles à clef publique, s'ils permettent des échanges sécurisés sur des canaux qui ne le sont pas, sont en règle générale 1000 fois plus lents pour le chiffrement/déchiffrement que les protocoles à clef secrète. La solution consiste à initier une communication sécurisée à l'aide d'un protocole à clef publique, transférer une information disons de 128 bits, ce qui est parfaitement raisonnable sur le plan du temps de calcul, et d'utiliser ensuite cette information commune aux deux correspondants comme clef secrète d'un protocole à clef secrète. Le protocole à clef publique cède alors la place au protocole à clef secrète, et la communication se poursuit à l'aide de celui-ci. C'est par exemple ce que fait le produit PGP de Phil Zimmerman, qui combine un algorithme à clef publique, en l'occurrence RSA, avec un protocole à clef secrète nommé IDEA.

Il est particulièrement notable que ces standards AES ou IEEE-P1363 aient fait l'objet d'un débat scientifique ouvert et international. Il ne saurait donc y avoir au sein même de ces algorithmes de faiblesses cachées permettant d'en contourner l'efficacité (ce que les Anglo-Saxons appellent communément « *trap-doors* »). De plus, l'évaluation des propositions a été faite sur de longues années, dans le souci de pérennité des nouveaux standards.

A ces grands axes, il convient de rajouter des méthodes de protection à l'égard – entre autres – des effets TEMPEST (possibilité de reproduire à distance les émanations électromagnétiques d'un écran par exemple, et ainsi de le « recopier »), ou encore d'activer à distance via le canal D la fonction d'écoute d'un appareil téléphonique de type RNIS. Cependant, il nous semble peu probable que ces faiblesses puissent être exploitées par un réseau tel qu'Echelon, et nous n'en parlons pas davantage ici. Enfin, une méthode de transfert confidentiel de données sans utilisation (réelle) de la cryptographie repose sur les techniques de stéganographie. Il s'agit en l'occurrence de cacher des informations dans d'autres, typiquement des photos, des vidéos, ou du son (mais cela peut aussi être du texte, comme par exemple un programme écrit en langage C). L'une des applications commerciales de ces technologies est leur utilisation pour la protection des droits d'auteurs. En

(56) Sans rentrer dans le détail de chaque type d'algorithme, indiquons simplement que, tels que décrits dans ce standard, la sécurité des algorithmes à clef publique repose sur les problèmes et les familles d'algorithme suivants :

– Factorisation de grands entiers : RSA (Rivest-Shamir-Adleman) et Rabin-Williams ;

– Problème du logarithme discret : DSA (Digital Signature Algorithm), échange de clefs de Diffie-Hellman, chiffrement et signature électronique de El Gamal, de Schnorr et de Nyberg-Rueppel ;

– Problème du logarithme discret pour les courbes elliptiques : les analogues des algorithmes ci-dessus pour les courbes elliptiques, considérées sur des corps finis de cardinalité un grand nombre premier ou une puissance première de deux (voir Franck LEPRÉVOST, « Les standards cryptographiques du XXI^e siècle : AES et IEEE-P1363 », *La Gazette des Mathématiciens*, 85, juillet 2000).

effet, ce qui, dans ce contexte, s'appelle « *watermarking* », permet de labelliser ces documents, et ainsi de permettre leur traçabilité (57). Il est cependant parfaitement concevable d'utiliser aussi ces méthodes stéganographiques afin de transmettre des informations de manière confidentielle en les « cachant » dans des données plus anodines, comme des photos. L'un des intérêts réside dans le format des données transmises. En effet, lors de transfert de fichiers, leur format révèle s'ils sont cryptés ou pas, ce qui peut attirer l'attention. Ce n'est plus le cas avec la stéganographie (58).

Au total, les moyens de cryptographie ainsi que certaines techniques de stéganographie apparaissent techniquement comme les seuls instruments susceptibles d'assurer à une entreprise ou à un individu une protection suffisamment fiable à l'encontre d'éventuelles interceptions du type de celles pratiquées dans le cadre UKUSA. Et c'est cette argumentation que le gouvernement français a semble-t-il repris *a posteriori* à son compte pour justifier la poursuite de la libéralisation du régime de la cryptologie en France. Après, en effet, avoir assoupli les conditions d'autorisation et de déclaration des produits de chiffrement en mars 1999 (59), le gouvernement annonce toujours comme prochaine une libéralisation complète de l'usage des moyens de chiffrement (qui devrait prendre place au sein de la prochaine loi sur la société de l'information, attendue primitivement en 2001). Il est d'ailleurs soutenu désormais en ce sens par les parlementaires de la commission de la Défense de l'Assemblée nationale qui – par la voix de leur rapporteur, M. Arthur Paecht – ont mentionné dans les conclusions du récent rapport sur Echelon que « *la libéralisation des programmes de cryptographie ou de chiffrement devient impérative* » (60).

Si les autorités françaises semblent avoir trouvé ainsi une façon de mettre au service de leurs projets juridiques et technologiques à court terme le débat autour d'Echelon, il n'est pourtant pas certain que l'ensemble de la communauté française du renseignement et des questions de sécurité se soit réjoui du développement spectaculaire de ce débat autour d'Echelon. Comme l'indique, en effet, avec justesse le rapport Paecht, on peut consta-

(57) De nouveau, le STOA du Parlement européen suit particulièrement ces aspects, et a mandaté les auteurs du présent article pour une nouvelle étude technique et juridique portant sur l'utilisation des moyens de sécurité (cryptographie et stéganographie, principalement) pour la protection des droits intellectuels sur les contenus numériques, publiée fin mars 2001.

(58) D'après certaines informations parues dans la presse spécialisée, il semblerait que les services gouvernementaux américains travailleraient actuellement à la mise au point de système d'interception des messages stéganographiés (cf. « Etats-Unis : les efforts de la NSA vis-à-vis du Web », *Le Monde du Renseignement*, n° 392 du 26 octobre 2000).

(59) Par les décrets et arrêtés du 17 mars 1999 (*JORF* du 19 mars 1999, pp. 4050-4053) qui ont établi de nouvelles règles de procédure : en particulier, le passage en régime déclaratif des produits de chiffrement asymétrique utilisant une clé de longueur inférieure ou égale à 128 bits (cf. notre synthèse dans cette revue, *op. cit.*, p. 660).

(60) Rapport Paecht, *op. cit.* (le rapport fait d'ailleurs, à cette occasion une confusion entre la limitation imposée par les textes actuels en matière de longueur de clés pour les algorithmes de chiffrement symétrique – 128 bits aujourd'hui – et la taille des clés utilisés pour les systèmes de génération et d'échange de clés, qui sont des systèmes asymétriques non soumis à la limitation à 128 bits).

ter les « réticences » des services de renseignement français à participer à la dénonciation des pratiques d'interception anglo-saxonnes et cela peut avoir différentes raisons qui nous incitent à conserver une approche critique de l'ensemble du dossier et de l'exploitation médiatique actuellement entretenue autour de lui.

Peut-on avoir une approche critique du débat autour d'Echelon ?

C'est sans doute l'un des premiers intérêts du rapport parlementaire rédigé par M. Paecht de s'être essayé à prendre du recul par rapport à l'ensemble de ce dossier Echelon. En suivant son approche, résumons, en effet, l'état de nos connaissances et de nos incertitudes.

S'agissant du système d'interception lui-même, nous pouvons certainement considérer comme avérée l'existence de mécanismes de renseignement électronique organisés et coordonnés par les Etats-Unis et certains de leurs alliés au niveau international. Les premiers documents déclassifiés indiquant l'existence de ces pratiques (et du programme Echelon lui-même) sont d'ailleurs désormais disponibles sur le Web (61).

L'incertitude plane, en revanche, sur les réelles capacités technologiques d'un tel système. Dans un article de synthèse paru dans le très respecté *Bulletin of Atomic Scientist*, J. Richelson mentionne par exemple le goulot d'étranglement que représenterait sans doute encore, aujourd'hui, l'absence de logiciels fiables pour assurer la reconnaissance de la parole, ce qui interdirait la détection automatisée du contenu des conversations téléphoniques interceptées et obligeant à continuer de traiter celles-ci par des méthodes humaines plus traditionnelles (62). Plus simplement, peut-on se poser quelques questions sur les capacités de traitement rapide de la masse d'informations que les différents centres d'interception affiliés à l'alliance UKUSA sont supposés récolter chaque jour. Enfin, on peut également s'interroger sur la capacité que ces systèmes peuvent avoir à déchiffrer la masse croissante des données interceptées qui sont désormais chiffrées avec les moyens commerciaux du marché (moyens sans doute insuffisamment performants pour résister à une cryptanalyse poussée de la part de services tels que la NSA ou le GCHQ, mais dont l'usage de plus en plus large – notamment sur l'Internet et les téléphones mobiles – va rallonger considérablement les délais pour parvenir à l'information claire et pour, le cas échéant, la sélectionner). Comme titrait récemment une publication spécialisée canadienne, « *Echelon : Big Brother, Little Brother, or both ?* » (63). Autrement dit, l'étalage des capacités technologiques supposées d'Echelon n'est-il pas éventuel-

(61) Cf. notamment les documents déclassifiés présentés par J. Richelson sur le site de la National Security Archive, déjà cité.

(62) Cf. Jeffrey RICHELSON, *The Bulletin of the Atomic Scientists*, March/April 2000, Vol. 56, n° 2, pp. 47-51 (http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html).

(63) *CASIS Intelligence*, n° 36, printemps 2000, pp. 14-15.

lement un moyen pour le renseignement électronique américain de cacher ses propres déficiences technologiques et de mener une campagne à usage interne en vue d'obtenir une croissance de ses crédits en matière de technologie et d'équipements.

De la même façon, il n'est pas réellement possible de déterminer jusqu'à quel point les objectifs économiques et commerciaux sont devenus prioritaires dans la collecte et le traitement des informations collectées par le système UKUSA. Comme l'indique avec sagesse Arthur Paecht, « *il n'est pas impossible que certaines informations recueillies puissent être utilisées à des fins politiques et économiques. Il n'existe pas de preuve formelle de détournement du système, mais l'ambiguïté des déclarations de certains responsables ne laisse aucun doute sur cette possibilité* ». Reconnaissons d'ailleurs, sur ce point, le caractère habile et difficile à contester de la position officieusement défendue par les responsables américains (et particulièrement bien illustrée par l'interview de J. Woolsey déjà cité) qui limite les actions de renseignement aux seuls objectifs de lutte contre la corruption, la prolifération et la violation des réglementations de contrôle des technologies ou des sanctions internationales.

Si l'on se tourne maintenant vers la situation des différents pays européens concernés, il faut là aussi constater que l'affaire n'est pas sans ambiguïté. Si l'on peut imaginer à première vue qu'une telle polémique est susceptible de renforcer la volonté d'autonomisation européenne face aux ambitions hégémoniques d'un partenaire américain accusé d'utiliser à son profit le jeu de la mondialisation, on s'aperçoit vite que la réalité est beaucoup plus complexe. Outre la position plus qu'ambiguë de la Grande-Bretagne, la plupart des autres pays européens (y compris la France) entretiennent des relations étroites d'échange et de coopération en matière de renseignement avec les Etats-Unis et ils aspirent – pour se préserver contre les risques d'une cyberdélinquance encore mal connue (et donc d'autant plus crainte) – à mettre en place des dispositifs de surveillance permanence des réseaux électroniques et à se doter des moyens juridiques pour pouvoir accéder, en cas de besoin, aux contenus clairs des flux électroniques (e-mail notamment) échangés sur les réseaux (64). La négociation actuellement en cours au sein du Conseil de l'Europe et en relation avec les autorités communautaires et le G8 concernant la lutte contre la cybercriminalité va notamment dans ce sens (65). On peut donc faire l'hypothèse que, d'une certaine façon, les services de sécurité européens éprouvent un certain malaise à voir enfler la contestation face aux interceptions Echelon car cette contestation ne se limite pas à une critique des ambitions impériales américaines mais risque

(64) Ces nouveaux pouvoirs d'investigation et d'injonction devraient être accordés à l'autorité judiciaire par la nouvelle loi française sur la société de l'information, en contrepartie de la libéralisation accrue de l'usage des moyens de chiffrement.

(65) Conseil de l'Europe, *Projet de convention sur la cybercriminalité,* 27 avril 2000, (http://conventions-.coe.int).

d'alimenter indirectement une réelle résistance « citoyenne » face à toute forme de « police des réseaux » (66).

Une fois encore, et quoi qu'il en soit, cette affaire des révélations autour d'Echelon nous permet de constater l'importance des ressorts psychologiques et sociologiques dans le développement d'un débat d'opinion transnational. Tout d'abord, il est frappant de remarquer que le débat mediatique n'a débuté que lorsque le sujet s'est cristallisé autour d'un nom simple et mystérieux, apte à devenir un symbole et à guider l'attention du public. Peu importe que ce nom « Echelon » ne soit finalement qu'un aspect technique secondaire de l'ensemble du système. Il fallait populariser l'affaire et pour cela il fallait un vecteur mediatique et mnémonique. Ensuite, on perçoit bien que chacun projette finalement tout à la fois ses ambitions et ses peurs dans cette vision fantasmagorique d'une grande oreille mondiale à laquelle rien n'échapperait. Le désir « pan-optique » (comme aurait dit Foucault) est d'autant plus dénoncé chez le partenaire-concurrent que chacun souhaiterait se doter de moyens pour réaliser à sa mesure un outil de surveillance et de collecte d'informations. Il est donc impossible de savoir déjà à qui profitera finalement la controverse. La gestion politique de ses conséquences ne fait que commencer, d'autant que des actions juridiques viennent d'être engagées en France et en Allemagne pour alimenter la campagne et obliger les acteurs officiels à prendre position. A court terme, seules les publications d'information à grand tirage et – plus sérieusement – les entreprises proposant des solutions de sécurité informatique peuvent espérer des retombées favorables rapides. Mais, au-delà, il n'est pas interdit d'espérer que de tels débats favoriseront, par contraste, une réflexion commune sur ce que devrait être à moyen terme une organisation européenne du renseignement et de la sécurité.

(66) Sur la perspective de ces « *polices de réseaux* » comme forme possible d'avenir pour les services de sécurité et de contre-espionnage, cf. B. WARUSFEL, *Contre-espionnage et protection du secret, op. cit.*, p. 409.