DU RÉSEAU ECHELON A LA « RÉVOLUTION DES AFFAIRES DE RENSEIGNEMENT » AUX ETATS-UNIS

PAR

CLAUDE DELESSE (*)

LA DÉCOUVERTE INGÉNUE PAR L'EUROPE DU RÉSEAU ECHELON

L'existence du réseau technologique d'espionnage et de contre-espionnage américain du nom de code Echelon a été révélée à l'opinion en 1988 lors de l'affaire du Watergate par deux reporters du *Cleveland Plain Dealer* (Ohio), C. Epstein et John S. Long (1). C'est l'enquête du journaliste britannique Duncan Campbell (2), commencée la même année, qui alerta l'Europe. En 1996, un journaliste néo-zélandais, Nicky Hager, réussit à s'infiltrer dans une base secrète du réseau.

De l'intérieur du système, une poignée d'agents, choqués par les pratiques de leur service, n'hésitèrent pas à sacrifier leur carrière en dénonçant les orientations illégales de ce réseau d'écoutes (ce fut le cas notamment de Fred Stock, qui alerta des parlementaires et engagea des plaintes contre l'agence canadienne, lesquelles furent étouffées pendant cinq ans et laissées sans suite). Divers mouvements de protestation s'organisèrent en Grande-Bretagne, où des militantes féministes, bravant arrestations, évacuations musclées, procès et prison, harcelèrent épisodiquement la plus grosse station d'écoute anglaise dans le Yorkshire, Menwith Hill (3). Elles campèrent aux alentours, fouillèrent les poubelles, découpèrent les grilles de sécurité et pénétrèrent dans les lieux. D'autres activistes, en octobre 1999, tentèrent d'engorger les ordinateurs du réseau en envoyant des *e-mails* bourrés de mots-clefs provocateurs.

L'Europe découvrit ainsi progressivement un réseau d'espionnage qui semblait fonctionner en partie à son détriment. L'ouvrage dans lequel Nicky

(*) Professeur à Bordeaux Ecole de Management et chercheuse associée au Centre d'analyse politique comparée, de géostratégie et de relations internationales (CAPCGRI) de l'Université Montesquieu (Bordeaux, France).

(1) Les communications du sénateur républicain Strom Thurmond auraient été interceptées.

(2) Duncan CAMPBELL, « Somebody's listening », *New Statesman*, 12 août 1988, pp. 10-12, disponible sur le site Internet duncan.gn.apc.org/echelon-dc.htm (dernière consultation le 9 juillet 2002).

(3) Base dirigée jusqu'en 1966 par l'armée américaine, puis placée sous le contrôle de la NSA : réceptrice des satellites de reconnaissance électronique, elle est aujourd'hui la plus importante base d'interception du réseau ; elle utilise 1 500 agents américains et coordonne vingt-deux terminaux pour satellites.

Hager avait révélé les résultats de sa grande enquête, *Secret power* (4), inspira en 1997, à la demande de la Commission des libertés publiques et des affaires intérieures du Parlement européen (5), une étude réalisée par le Bureau d'évaluation des options techniques (6). Puis quatre rapports (dont un commandé à Duncan Campbell) soulignèrent les dangers que faisait peser ce réseau sur les pays de l'Union et sur leurs entreprises (7). À la proposition des Verts de créer une Commission d'enquête, fut préférée la constitution, le 5 juillet 2000, d'une commission temporaire de trente-six membres. Dépourvue de réels moyens, enfermée dans un « *silence embarrassé* », celle-ci rédigea en 2001 un document de travail (8) qui devait précéder une visite d'eurodéputés mandatés à Washington. Dans ce document, les rapporteurs s'inquiétèrent plus de la légitimité que de la menace que représentait Echelon; le cryptage des *e-mails* communautaires y était toutefois recommandé. Les Américains ayant considéré que la rencontre envisagée entre les responsables concernés de leurs services et la délégation européenne était inappropriée, les entrevues furent annulées à la dernière minute. La parution du rapport européen sur Echelon allait susciter peu de réactions. Il faudra attendre octobre 2003 pour que le Parlement de Strasbourg décide la création d'une agence de lutte contre les menaces électroniques : l'European network and information security agency (ENISA), dotée d'un budget de 24,3 millions d'euros, vit le jour en janvier 2004 (9). Désormais, à Bruxelles, les débats semblent clos. Une résolution de septembre 2001 a simplement demandé au Royaume-Uni et à l'Allemagne de respecter la convention relative aux droits de l'homme...

Ces réactions d'institutions européennes, toujours en gestation et affaiblies par les divisions de leurs Etats-membres, apparaissent particulièrement paradoxales, au moins pour trois raisons. D'abord, l'origine historique du réseau en question se situe au cœur de l'Europe, au cours de la Seconde Guerre mondiale. L'*Intelligence service* du général Menzies réussit à percer le secret du chiffre nazi en s'emparant de plusieurs exemplaires de la machine

(4) Nicky HAGER, *Secret power : New Realand's role in the international Spy Network*, Craig Potton Publishing, Nelson, 1996, 300 p.

(5) Aujourd'hui Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures.

(6) Steve WRIGHT, *An Apraisal of Technologies of political Control. Interim Study, Rapport pour le Bureau d'évaluation des options techniques et scientifiques (Stoa) du Parlement européen*, Fondation Omega, Manchester, 19 janvier 1998.

(7) En particulier celui de Duncan CAMPBELL, *Interception Capabilities 2000 : The State of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, ant its applicability to COMINT targeting and selection, including speech recognition*, IPTV Ltd, Edinbourg, avril 1999. Pour plus de précisions sur les révélations et les débats suscités, *cf.* Frank LEPRÉVOST / Bertrand WARUSFEL, « Echelon : origines et perspectives d'un débat transnational », *Annuaire français de relations internationales*, vol. 2, 2001, pp. 865-888.

(8) Gerhard SCHMID, Working document in preparation for a report on the existence of a global system for intercepting private and commercial communications (Échelon interception system), European Parliament, Temporary Committee on the Echelon Interception system, 4 mai 2001.

(9) « L'Union européenne se dote d'une agence de cybersécurité », *Le Monde* informatique, 10 octobre 2003, disponible sur le site Internet www.weblmi.com (dernière consultation le 17 octobre 2003).

de codage Enigma que les Allemands croyaient inviolable (10). La maîtrise d'Enigma, qui raccourcit de plusieurs mois la guerre sur terre, dans les airs et sur mer, entraîna, en 1943, la signature, entre les Etats-Unis et la Grande-Bretagne, d'un accord de coopération entre leurs services réciproques d'interception des télécommunications. En 1946, cet accord, renommé UKUSA, fut élargi au monde anglophone (Canada, Australie, Nouvelle-Zélande). Ensuite, il faut rappeler que de nombreux Etats européens, depuis l'après-guerre, grâce à l'Alliance atlantique, sont devenus des partenaires et des clients du renseignement américain dans la lutte anticommuniste puis dans celle contre le terrorisme et les activités de réseaux criminels. Une dizaine de pays participent plus ou moins au système dans la logique de leur alliance stratégique globale avec les Etats-Unis. L'Autriche, la Norvège, le Danemark, l'Allemagne, l'Italie, la Grèce, la Turquie, la Thaïlande, le Danemark, la Norvège, la Corée du Sud (alliés historiques des Etats-Unis), soit accueillent des stations d'interception, soit possèdent des paraboles de type Echelon, soit collaborent étroitement avec les services américains. Il en est de même pour un pays comme la France qui, malgré des fluctuations dans ses rapports avec l'OTAN et avec les Etats-Unis, a parfois fait appel aux données interceptées par le réseau (notamment dans la lutte antiterroriste) et a normalisé ses relations avec certains services américains. Il faut rappeler enfin que la plupart des Etats désireux de maintenir leur puissance dans le monde (la Chine, la Russie, la France, l'Allemagne, Israël, l'Inde, le Pakistan, divers pays d'Asie du Sud ou d'Amérique du Sud...) possèdent eux-mêmes un réseau d'écoute spécifique, intégré à leur système de défense et de renseignement, même si celui-ci ne revêt pas l'importance quantitative de celui des Etats-Unis. On estime au nombre d'une cinquantaine les Etats concernés, dont beaucoup ont pu acheter sur le marché des technologies d'interception électromagnétique. Tout grand Etat, en définitive, n'a pas d'ami ou d'allié éternel et doit se défendre d'actions concurrentes contraires à ses intérêts. Notons que pour la plupart des gouvernements, la publication de renseignements confidentiels sur un réseau comme Echelon implique des informations relevant du « secret Défense », de la sécurité interne et externe.

Nous nous proposons ici, sans souci d'exhaustivité, d'esquisser une réflexion sur le réseau Echelon aujourd'hui, dans le contexte de l'après-11 septembre. Après avoir dans un premier temps rappelé brièvement ses fonctions politiques et économiques antérieures, nous nous interrogerons ensuite sur les transformations du système de renseignement américain dont Echelon constitue le fleuron technologique.

(10) Cela fut possible grâce à une collaboration étroite de l'IS, depuis 1939, avec les services du 2e Bureau français (Colonel Paillole), qui obtinrent les codes de chiffrage grâce à un espion, le capitaine Schmidt, introduit à l'état-major de Hitler, ainsi qu'un exemplaire d'Enigma, dont les codes furent percés par un mathématicien des services polonais de décryptage... *Cf.* Paul Paillole, *Notre espion chez Hitler*, Robert Laffont, Paris, 1985; Anthony Cave Brown, *La Guerre secrète*, Pygmalion, Paris, 1981.

Les fonctions du système Echelon

Le 4 novembre 1952, après avoir aboli l'Armed forces security agency (AFSA) (11), Truman créa la National security agency (12). En 1972, celle-ci devint la NSA/CSS. Elle emploie aujourd'hui près de 40 000 agents et son budget dépasse celui du FBI et de la CIA réunis. La mission du CSS (Central security service) consiste à « *coordonner les activités de cryptologie et à harmoniser les procédures d'écoutes et de sécurité électroniques au sein du département de la Défense* » (13). Une directive de Reagan la rendit responsable en 1984 de la sécurité informatique pour l'ensemble des organes fédéraux. Dénommée communément « *Sigint City* » (14), la NSA fut chargée de coordonner Echelon (à l'origine appelé « Project 415 » (15)). Simple logiciel de traitement des écoutes téléphoniques au départ, Echelon désigna ensuite le réseau de surveillance mondiale des télécommunications dans le cadre de l'UKUSA. La NSA intercepte les informations en relation avec quatre autres services de renseignement dans les différentes zones planétaires (16). A partir de 1983, Platform, un réseau informatique basé à Fort Meade, quartier général de la NSA, relia entre eux cinquante-deux systèmes informatiques (17). Dans quel but ? George H.W. Bush, en déplacement à Fort Meade, précisa que les écoutes constituaient « *un facteur essentiel* » du processus américain de décision en matière internationale (18). De même, le vice-amiral de l'US Navy, John Mac Connell, directeur de la NSA de mars 1992 à février 1996, déclara en 1994 qu'il n'y avait pas un seul événement de politique étrangère intéressant le gouvernement auquel la NSA ne fût directement mêlée.

(11) L'AFSA avait été créée le 20 mai 1949 au sein du Département de la Défense et était subordonnée directement au « Joint chiefs of staff ».

(12) A la suite d'un mémorandum du 24 octobre 1952, classifié « Top secret », intitulé « Communications intelligence activities ».

(13) Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Pamazol, 2002, 743 p.

(14) La NSA est un organe de renseignements de signaux Sigint, qui agit au profit de l'ensemble de l'Intelligence community. Elle est autorisée à produire Sigint en accord avec les objectifs, les demandes et les priorités établies par le Director of central intelligence, avec l'avis du National foreign intelligence board. *Cf.* le site Internet www.nsa.gov/about_nsa/mission.html.

(15) Le principe est d'aider à l'interception, au tri et à l'interprétation des signaux grâce à de puissants ordinateurs reliés entre eux.

(16) En collaboration avec le Government communications headquarters britannique (GCHQ), le Government communications security bureau néo-zélandais (GCSB), le Defense signals directorate australien (DSD) et le Communications security etablishment canadien (CSE). Le GCHQ s'occupe de l'Europe continentale, de la Russie à l'ouest de l'Oural et de l'Afrique, tandis que le CSE surveille la Russie septentrionale, le GCSB le Pacifique occidental et le DSD, l'Asie du Sud-Est et la Chine méridionale.

(17) Jacques Baud, *op. cit.*, p. 254.

(18) Déclaration citée par Vincent Jauvert, « Comment l'Amérique nous espionne ? », *Le Nouvel Observateur*, n° 1 779, 10-16 décembre 1998, pp. 10-22.

Techniquement parlant, Echelon est constitué de bases qui interceptent des communications multiples transmises automatiquement à la NSA (19). A partir de satellites et de relais spatiaux et terrestres, il sélectionne jour et nuit les communications par téléphone, télex, télécopies et courriers électroniques. Des radômes (sortes d'énormes balles de golf) dissimulent dans les stations l'orientation des paraboles qui couvrent le monde entier grâce à la situation géostratégique des cinq principales agences d'interception. Des satellites de télécommunications Inmarsat et Intelsat, d'autres d'observation à l'écoute des ondes radio et des téléphones cellulaires, des capteurs sur les câbles sous-marins, des équipements secrets, installés dans les ambassades, composent le dispositif appelé COMINT (20). Les ordinateurs, qui analysent des millions de signes par heures, dénichent les messages à partir de numéros de téléphone, d'adresses, de mots-clefs inscrits dans des « dictionnaires » ou par reconnaissance vocale. Les données sont livrées à des systèmes de lecture optique, d'évaluation des contenus ou de décryptage, puis à des analystes multilingues.

Comme le montrent les fonctions assumées par Echelon, les cibles ont évolué à travers les différentes phases du système des relations internationales.

Les fonctions militaires et politiques d'Echelon

Lors de la Guerre froide, conflit de haute intensité entre l'Alliance atlantique et le bloc communiste, Echelon fit preuve d'une grande efficacité dans la lutte informationnelle et la lutte d'espionnage qui s'ensuivirent (21). Il permit d'intercepter les communications du bloc soviétique et constitua un des maillons essentiels de la stratégie de *containment* des Etats-Unis à l'égard du Pacte de Varsovie. Son utilisation fut particulièrement importante lors des conflits de Corée, lors de l'affaire de l'U2, lors de la crise de Cuba ou de la guerre du Vietnam. Le réseau servit encore à des fins de manipulation de l'opinion occidentale. Ce fut le cas au Vietnam, entre 1967-1968, lorsque les responsables des opérations se retranchèrent derrière ses capacités techniques pour justifier les quotas quotidiens des missions de bombardement des B-52 (22). Il permit aussi d'ignorer certaines crises pour éviter de fâcher diplomatiquement un allié.

À partir des années quatre-vingts, Echelon se focalisa sur les nouvelles menaces liées au terrorisme international. Ainsi, par exemple, les intercep-

(19) National security agency : on aurait tout ignoré de cette agence jusqu'à la publication, en 1982, de l'ouvrage du journaliste américain James BAMFORD, *The Puzzle of Palace : a report on America's Most Secret Agency*, Houghton Mifflin, Boston, 1982, suivi de *Body of Secrets : Anatomy of the ultra-secret National Security Agency from the Cold War through the dawn of a new century*, Doubleday, New York, 2001.

(20) COMINT (Communication intelligence) constitue l'activité principale de SIGINT (Signals intelligence), qui traite des émissions électroniques telle que la télémétrie des radars ou des missiles.

(21) François GÉRÉ, *Pourquoi les guerres : un siècle de géopolitique*, Larousse, Paris, p. 52.

(22) Manœuvre visant à modifier la perception d'un événement ou d'une observation. Des services d'interception britanniques, australiens et néo-zélandais auraient aidé les services secrets américains à localiser des cibles. Ces opérations, à l'intensité pas forcément justifiée, furent largement médiatisées.

tions et le décryptage des communications des ambassades libyennes à Berlin-Est et à Rome en 1986 décidèrent Reagan à faire bombarder Tripoli pour répondre à l'explosion d'une discothèque de Berlin-Ouest qui avait tué deux soldats américains. Les trafics de produits illicites et d'armes de destruction massive firent également l'objet d'une surveillance particulière. En relation avec les services de renseignement, la NSA traqua les fabricants et les fournisseurs en combinant les écoutes de numéros à surveiller, les images radars et infrarouge des satellites espions, savamment analysées par des photos-interprètes. Echelon permit aussi d'observer les activités et les déplacements des terroristes. Rapidement cependant, il s'est mis à contrôler les alliés et les pays amis des Etats-Unis, y compris les membres intégrés au système de surveillance.

Divers problèmes de fonctionnement interne surgirent à ce niveau. Après 1946, l'accord UKUSA, qui détermina les procédures, les cibles, les équipements et les méthodes communes à toutes les agences SIGINT, se révéla asymétrique entre les partenaires du réseau. Chacun n'était alimenté par les autres qu'au *prorata* des informations qu'il leur apportait. La NSA décida que les informations interceptées par les moyens spatiaux américains relevaient de la stricte propriété nationale : seuls les Britanniques y eurent accès par dérogation. Les mêmes mots-clefs ne furent pas forcément portés à la connaissance de tous les membres. Grâce à cette astuce, les Etats-Unis utilisèrent par exemple les infrastructures néo-zélandaises d'écoute à l'insu de leurs responsables : leur objectif était d'espionner les communications de Greenpeace, qui protestait contre les essais nucléaires français à Mururoa en 1995. Quelque temps plus tard, l'interdiction par le Premier ministre travailliste David Lange de laisser entrer dans les eaux territoriales le navire nucléaire *USS Buchanam* n'empêcha pas les services secrets néo-zélandais de participer au développement d'Echelon et de répondre aux demandes de renseignement de la NSA (23). Or, le contenu de ces informations portait plus ou moins atteinte à la ligne diplomatique retenue par leur gouvernement.

Les efforts d'Echelon se portèrent également sur les Etats des pays amis ou alliés et leurs administrations, sur les partis d'opposition, sur les conférences commerciales, sur les agences des Nations Unies... Relevons la place privilégiée des Britanniques (24), alliés depuis toujours des services secrets américains. Forts de cinq stations d'écoute (dont l'énorme Menwith Hill), ceux-ci imposent à la British Telecom de les consulter lorsqu'elle souhaite

(23) Philippe Rivière, « Le système Echelon », *Manière de voir*, n° 46, 2001, pp. 40-42, sur le site Internet www.monde-diplomatique.fr/mav/46/RIVIERE/m1.html.

(24) « *Le gouvernement de Tony Blair se refuse à prendre le moindre engagement public touchant cette question sensible, mais semble avoir pris des dispositions en ce qui concerne les échanges de renseignement, avec les services de renseignement européens. Lors des rencontres dans le cadre du club Totem, qui réunit les services de renseignement de l'OTAN, les Britanniques seraient assez généreux sur les informations qu'ils transmettent à leurs homologues* ». *Cf.* le site Internet reseauechelon.free.fr/chapitre4.html.

infléchir sa stratégie (25). Tout en surveillant l'Angleterre elle-même, Echelon a facilité depuis le territoire de cette dernière la surveillance d'amis compétiteurs comme la France qui irritait les Etats-Unis) par sa politique nucléaire et d'indépendance, cela dans le cadre du programme « Corona ». Des clichés de l'époque, remis aux archives nationales par Bill Clinton, révélèrent le contrôle par Echelon des installations du centre d'expérimentation du Pacifique en 1964 à Mururoa, de la première campagne d'essais en 1966, de la première explosion d'une bombe thermonucléaire en août 1968 (26).

Echelon a aussi exercé un contrôle interne sur le territoire des Etats-Unis. Il s'agissait de connaître les projets et les plans des éléments jugés subversifs ou déstabilisateurs. Cependant, dans un pays où les contre-pouvoirs démocratiques sont effectifs, ces fonctions sécuritaires ont inquiété le Congrès, attentif à la protection des citoyens américains et au respect de la Constitution. Ainsi, la Commission Church (27) révéla, dans son rapport de 1976, que la NSA avait monté deux opérations parallèles secrètes : MINARET écoutait en toute illégalité des opposants contre la guerre du Vietnam; Shamrock interceptait la quasi-totalité des communications qui arrivaient aux Etats-Unis ou en partaient. Aujourd'hui, les services semblent s'accommoder des contrôles parlementaires, mais le pouvoir exécutif voudrait limiter l'accès des informations secrètes (28). Si l'Exécutif peut laisser fuir des informations par intérêt ou par volonté de manipuler l'opinion, certains parlementaires refusent que les capacités de renseignement soient dégradées par des « fuites » distillées à la presse. Un amendement a réclamé ainsi la criminalisation de la publication de toute information « classifiée », mais il fut bloqué par Bill Clinton (29).

Si, comme on a pu le voir, les opérations spéciales de renseignement et Echelon ont suscité régulièrement des réactions, dont certaines ont été orchestrées par des associations défendant les libertés civiles (30), parallèlement, à partir de 1993 (et à l'initiative du FBI), les responsables policiers de divers pays de l'Union européenne et de l'UKUSA ont décidé de se réunir une fois par an pour un « International law enforcement telecommunications

(25) « Une véritable mainmise sur British Telecom », *Courrier international*, n° 387, 2-8 avril 1998, sur le site Internet www.courrierinternational.com/dossiers/soc/Echelon/Echelon02.htm (dernière consultation le 23 janvier 2003).

(26) Vincent JAUVERT, *op. cit.*, p. 14.

(27) Frank CHURCH, sénateur démocrate.

(28) Présidents des deux assemblées du Congrès et des deux commissions du renseignement, ainsi que leurs quatre homologues de l'opposition.

(29) *Cf.* « La mauvaise réputation », *in* Jean GUISNEL, *op. cit.*, 2002, pp. 39-86.

(30) L'ACLU (American civil liberties union), qui gère le site Internet « Echelonwatch.org », la CAAB (Campaign for the accountability for the American bases), l'EFF (ELECTRONIC frontier foundation), l'EPIC (Electronic privacy information center) et Privacy international EPIC, centre de recherche d'intérêt public créé en 1994 à Washington, se focalisent sur le respect des libertés publiques, du premier amendement et de la constitution. Privacy International est une association soucieuse de préserver les droits de l'homme contre les interceptions et les politiques de sécurité; elle agit sur deux fronts violés par Echelon, à savoir la protection de la vie privée et la parité des conditions commerciales. Créée en 1990, elle est établie à Londres et à Washington. EPIC et Privacy animent un site Internet d'information commun www.privacy.org.

seminar » (ILETS) en vue de débattre de leurs besoins en matière d'interception des communications. Cette régulation relative ne doit pas faire oublier cependant le second aspect fondamental de l'utilisation d'Echelon : l'espionnage économique, qui fonctionne à plein dans un univers intégralement concurrentiel.

Les fonctions économiques d'Echelon

Dans les années quatre-vingt-dix, les rapports de force classiques entre Etats démocratiques se sont progressivement estompés derrière les rivalités économiques et financières, terrain de prédilection de la géo-économie (31). Le concept de « sécurité économique » privilégié par l'Administration Clinton a bien reflété ce déplacement des priorités pour les Etats-Unis. De nombreux cas d'interceptions de renseignements à des fins économiques confirment cette évolution, qui a entraîné un regain incontestable des activités de surveillance d'Echelon.

Des exemples ? Lors des négociations de l'Accord de libre-échange nord-américain (ALENA), les délégués mexicains ont été placés sur écoute. Il en aurait été de même, en 1993, des participants français aux négociations du GATT. En 1995, des cadres japonais de Toyota et Nissan furent espionnés lors des négociations sur les droits de douane et les quotas d'importation des voitures japonaises. Mickey Kantor, l'envoyé de Bill Clinton, aurait bénéficié de l'aide de la NSA pour obtenir l'information portant sur les normes d'émission des véhicules nippons, arme décisive dans ce type de négociations. Pour se défendre, les services de renseignement prétendirent qu'ils ne faisaient que veiller au respect des embargos et que dépister les pratiques commerciales déloyales aux dépens des firmes américaines (32). Ainsi, Echelon, en interceptant une vidéoconférence, aurait permis à General Motors de prouver la culpabilité d'Ignacio de Lopez, un de ses anciens cadres, parti avec des secrets industriels chez Volkswagen (33). En 1994-1995, Airbus, accusé d'avoir usé de manœuvres d'influence, perdit le marché de 6 milliards de dollars de vente d'avions à l'Arabie saoudite au bénéfice de Boeing et McDonell-Douglas. En 1994, Raytheon Corporation remporta le marché SIVAM, système de surveillance de la forêt amazonienne de 1,3 milliard de dollars, contre Thomson-CSF ; Raytheon assurait en fait la maintenance et l'ingénierie de la station de Sugar Grove et aurait eu le soutien du Département du commerce américain : de fait, Bill Clinton, informé par la NSA du

(31) Pascal Lorot, « De la géopolitique à la géoéconomie », *Revue française de géoéconomie*, n° 1, mars 1997, pp. 23-35.

(32) George J. Tenet, « Statement by Director of Central Intelligence on Allegations about SIGINT activities and the so-called Echelon programm : Before the House Permanent Select Committee on Intelligence », US Central Intelligence Agency, 1999, sur le site Internet www.cia.gov (dernière consultation le 16 novembre 2003).

(33) *Les affaires Echelon,* 16 octobre 2002, sur le site Internet www.confidentiel.firstream.net (dernière consultation le 23 janvier 2003).

montant des dessous-de-table versés par Thomson-CSF à des responsables brésiliens, serait personnellement intervenu auprès des autorités brésiliennes pour retourner la situation.

En réponse à l'espionnage économique des concurrents, le *National Industry Security Program* (NISP), activé en janvier 1993, a organisé avec le Département de la Défense et une vingtaine d'agences gouvernementales la protection des entreprises, des universités et des centres de recherche américains. Bill Clinton confirma explicitement en 1994 (34) le rôle du renseignement en la matière. Concrètement, c'est *l'Office of Executive Support* au sein du Département du Commerce qui assume le lien entre les négociateurs et les agences de renseignement. Parallèlement, l'*Economic Espionage Act* du 11 octobre 1996 sanctionne sévèrement le vol ou l'appropriation illicite de secrets commerciaux considérés comme criminels. Dans le même sens, sous l'Administration Bush, les missions de renseignement ont renforcé leur soutien à l'activité d'exportation des firmes américaines, au-delà de la simple « diplomatie économique ». L'amiral William O. Studeman, directeur de la NSA, déclara crûment à la Chambre du Maryland en avril 2002 : « *la NSA, confrontée à une restriction de budget* (35)*, propose de prendre de plus en plus pour cibles les affaires économiques des alliés des Etats-Unis et leurs groupes industriels* [...]*, les renseignements économiques généraux* [...]*, les renseignements compétitifs, dont les offres effectuées et les innovations techniques* » (36).

Les industries surveillées par Echelon relèvent, il est vrai, de secteurs stratégiques ou sensibles. Les rapports publiés par le Département du Commerce donnent la liste de centaines de contrats soutenus par le gouvernement et remportés au détriment de la concurrence étrangère. L'argument utilisé pour justifier l'utilisation de signaux interceptés est toujours le même : le principe de l'« *aplanissement du terrain* » (37), selon lequel les moyens utilisés sont légitimes dans la mesure où les gouvernements étrangers ne respectent pas les règles de la concurrence (38). Cependant, les Américains ne procèdent-ils pas de la même façon dans de très nombreux cas ? La « *maîtrise de la connaissance* » (39) en matière économique, qui complète les fonctions militaires et politiques d'Echelon, ne peut faire oublier cependant les limites d'un système de renseignement fondé principalement sur des dispositifs techniques d'écoute. Flagrantes lors des événements du 11 septembre, ces limites ont incité les décideurs à reconsidérer leur modèle.

(34) Sorte de stratégie offensive de l'élargissement du modèle démocratique et libéral : *A National Security Strategy of Engagement and Enlargement*, The White House, Washington, février 1995, sur le site Internet www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf (dernière consultation le 20 novembre 2003).

(35) *Cf.* le site Internet www.nsa.gov/about–nsa/faqs–internet.html.

(36) Duncan CAMPBELL, *op. cit.*, p. 90.

(37) La politique de « *levelling the ground* », lancée par le Président Clinton, impliquait des arrangements pour le collectage, la réception et l'utilisation de renseignements secrets au bénéfice du commerce américain.

(38) Duncan CAMPBELL, *op. cit.*, 2001, p. 99.

(39) Didier LUCAS / Alain TIFFREAU, *La dissuasion par l'information*, 2002, sur le site Internet www.strategic-road.com/intellig/infostrategie/pub/dissuasion_information_txt.htm (dernière consultation le 14 novembre 2002).

UNE « RÉVOLUTION DES AFFAIRES DE RENSEIGNEMENT » ?

Qu'elle qu'ait été l'efficacité d'Echelon dans ses différentes fonctions, nombre de défis politiques et techniques ont remis en question la puissance des Etats-Unis au niveau planétaire. Pour faire face à des difficultés nouvelles après le grand traumatisme du 11 septembre, les responsables américains ont déployé une doctrine adaptée et ont élargi leur conception de l'organisation du renseignement.

La doctrine de la dominance informationnelle

Le Département à la Défense a investi progressivement une nouvelle doctrine de la « guerre de l'information ». Ce concept, apparu dans les années quatre-vingt-dix, implique que les vecteurs informationnels (contenant) et les messages que ceux-ci véhiculent (contenu) constituent des objets de convoitise, des enjeux de pouvoir et des cibles. La doctrine nouvelle vise l'« *ensemble des actions entreprises pour atteindre la supériorité dans l'information en agissant sur l'information, les processus informationnels, les systèmes d'information et les réseaux informatiques de l'adversaire, tout en défendant sa propre information, ses propres processus informationnels, ses systèmes d'information et réseaux informatiques* » (40). Commentant cette orientation, le consultant Winn Schwartau en est venu à conceptualiser la notion de « *conflit électronique* » dans lequel les équipements, les infrastructures informatiques et les systèmes deviennent des cibles cruciales susceptibles de conduire à un « *Electronic Pearl Harbor* » (41). L'importance des systèmes électroniques est apparue particulièrement évidente lors de la guerre du Golfe. Divers analystes ont aussitôt intégré cette nouvelle dimension stratégique et ont inspiré les vues officielles (42).

La doctrine des années quatre-vingt-dix doit beaucoup à la théorie d'un colonel de l'US Air Force, John Warden III, qui a redéfini l'ennemi comme formant un « *système* » de « *cinq cercles* » (43). Cette méthode veut prévoir les événements en hiérarchisant les faits et en se concentrant sur ce qui est important au bon moment. Martin Libicki, professeur à la National Defense University a distingué, dans le même sens, « *la guerre de commandement et*

(40) Cité par Frank DANINOS, « Guerre et dominance informationnelle : origines, histoire et significations stratégiques », *Diplomatie*, n° 2, mars-avril 2003, p. 9.

(41) Winn SCHWARTAU, « L'infoguerre vue des E-U : le Pearl Harbor informatique est possible », *L'information, c'est la guerre. Panoramiques,* n° 52, 2e trimestre 2001, pp. 100-105.

(42) Frank DANINOS, « Guerre et dominance informationnelle : origines, histoire et significations stratégiques », *Diplomatie*, n° 2, mars-avril 2003, pp. 9-13. Pour une définition précise du concept de RMA, *cf.* Thierry DE MONTBRIAL/Jean KLEIN, *Dictionnaire de Stratégie*, PUF, Paris, 2000, 607 p.

(43) A l'extérieur, le cinquième, constitue la puissance de feu ; le quatrième, la population civile ; le troisième, les structures de communication physique de l'ennemi ; le deuxième, les éléments organiques essentiels (l'énergie, le carburant, la nourriture, les finances) ; le premier, le commandement. *Cf.* « Les cinq cercles », *in* Jean GUISNEL, *op. cit.*, 2002, pp. 241-246 ; « The Enemy as a System », sur le site Internet www.aipower-.maxwell.af.mil/airchronicles/apj/warden.html.

de contrôle », « *la guerre du renseignement* », « *la guerre électronique* » (44), « *la guerre psychologique* » et « *la guerre des pirates informatiques* » (45).

La NSA s'est efforcée d'intégrer ces concepts. Elle a réorienté les systèmes d'interception en avançant la théorie des « C4ISR » (« *acronym for Command, Control, Communication, Computer intelligence collection, surveillance, and reconnaissance* »). Pour contrôler une bataille, il faut reconnaître les cibles et anticiper le schéma opérationnel de l'ennemi, de façon instantanée avec un objectif de « *zéro mort* » (46). Ainsi s'est généralisée la théorie de l'« infodominance » (ou domination informationnelle) (47), attachée à la prise en compte du différentiel entre adversaires (48). La réflexion a approfondi la question des modalités de combat dans les conflits « souterrains », les actes de guérilla, les guerres ethniques ou le terrorisme. Comment en effet s'informer, en dehors de la guerre conventionnelle, face à un ennemi dispersé, insaisissable, peu vulnérable à la guerre de l'information ? Les nouveaux ennemis invisibles, dissimulés dans les arcanes de sociétés secrètes ou d'organisations criminelles manipulent des systèmes communicationnels difficilement pénétrables. Ils déploient des dispositifs de brouillage, de camouflage, leurrent les moyens d'observation, investissent le cyberespace (49). La réplique implique que l'on contrôle les normes, les relais et les nœuds de répartition de l'information. C'est à ce prix que la puissance américaine peut imposer à la planète un ensemble de croyances et d'objectifs (50) (c'est le *soft power* informationnel dont parle Joseph Nye) (51). On ne contraint plus directement les partenaires, on les séduit et on les intègre dans des valeurs communes, savamment distillées, formant une « *noopolitique* » (52). Dans le

(44) La guerre électronique comprend SIGINT (*Signals intelligence*), ESM (*Electronic support measures*, mesures d'appui électroniques), ECM (*Electronic counter-measures*, contre-mesures électroniques), ECCM (*Electronic counter-counter-measures*, les contre-contre-mesures électroniques) *Cf.* Jacques BAUD, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, Pamazol, 2002, p. 355.

(45) Martin C. LIBICKI, *What is Information Warfare*, Center for Advanced Concepts and Technology, National Defense University, 1995.

(46) Saïda BEDAR, « La révolution dans les affaires militaires et la 'course aux capacités' », *Disarmament Forum de l'UNIDIR*, 4e trimestre 2001, sur le site Internet www.strategic-road.com/pays/pubs/revol_aff_milit_course_capacites_txt.htm (dernière consultation le 4 novembre 2003).

(47) Martin C. LIBICKI, Information dominance, Institute for National Strategic Studies and the National Defense University, Rapport n° 132, novembre 1997, sur le site Internet www.ndu.edu/inss/strforum/SF132/forum132.html (dernière consultation le 16 novembre 2003).

(48) « *Information superiority is the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same* », principe extrait de la *Joint Vision 2010* et clairement affiché sur le site Internet de la NSA www.nsa.gov/about_nsa/strategic/vision.html.

(49) Les techniques de pénétration par des agents bien intégrés dans les lieux et les organisations de l'adversaire sont revenues à l'ordre du jour, comme les bonnes vieilles méthodes « policières », moins coûteuses en budget que le déchaînement technologique. La dominance cybernétique en tant que tactique informationnelle a montré ses limites.

(50) François-Bernard HUYGHE, *Information, valeurs, menaces*, sur le site Internet Strategic – Road, avril 2002, www.strategicroad.com/intellig/infostrategie/pub/information_valeurs_menaces_1 (dernière consultation le 26 septembre 2002).

(51) Joseph S. NYE/William A. OWENS, « America's Information Edge », *Foreign Affairs*, vol. 75, n° 2, mars-avril 1996, p. 20.

(52) John ARQUILLA/David RONFELDT, *The Emergence of Noopolitik : toward an American Information Strategy*, The Rand Corporation, 1999.

même sens, le *perception management* constitue une doctrine complémentaire d'action, officiellement définie par le Département de la Défense. Adaptée aux nouveaux champs conflictuels, dont celui de la géo-économie, elle recouvre « *les actions consistant à fournir ou à camoufler une information sélectionnée et des indices à des audiences étrangères de façon à influencer leurs émotions, leurs motivations, leurs raisonnements* [...] *et à rendre leurs agissements favorables aux objectifs de l'émetteur. De plusieurs façons, le* perception management *combine l'apport d'informations authentiques avec des opérations de sécurité, de dissimulation et d'intoxication et des opérations psychologiques* » (53).

Ces orientations ont été complétées par une redéfinition de la stratégie internationale des Etats-Unis particulièrement cohérente sous l'Administration George W. Bush, même si certains éléments de continuité apparaissent par rapport à la période clintonnienne. Une nouvelle « *posture capacitaire stratégique* », largement soutenue par le budget de l'Etat fédéral (54), a été minutieusement définie par les néo-conservateurs américains (55), tenants du « *modelage du monde* » (*shaping the world*) qui se substitue au *containment* et à l'*enlargement* des années quatre-vingt-dix (56). Selon cette conception stratégique mondiale, qui intègre la politique internationale, la « guerre juste », l'affirmation des valeurs idéologiques de la démocratie américaine, la conception du conflit s'est élargie à une dimension « cognitive », « psychologique », « économique », mais aussi cybernétique et technologique. On souhaite toujours manipuler l'autre pour qu'il cause lui-même sa perte, comme le suggérait Sun Tzu, même si l'on distingue par gradation les pays amis et sûrs, les pays alliés (parfois douteux selon les dossiers traités et les circonstances, comme la Russie, la Chine, le Pakistan, l'Inde) et les pays ennemis (l'Iraq, l'Iran, la Corée du Nord...). Dans cette perspective globale, la « guerre de l'ombre » reste plus que jamais d'actualité (57).

Pour répondre tant aux défis nouveaux en matière de guerre de l'information qu'à la stratégie globale de leur nouvelle politique internationale (qui tente de répondre au défi du 11 septembre), les Etats-Unis ont déployé un élargissement des moyens et des tactiques de renseignement.

(53) Didier Lucas / Alain Tiffreau, *Guerre économique et information : les stratégies de subversion*, Ellipses, Paris, 2001, 240 p.

(54) 400 milliards de dollars pour l'année fiscale 2004 annoncés dans le *National Defense Authorization Act for Fiscal Year 2004*, signé par George W. Bush le 24 novembre 2003. *Cf.* le site Internet www.whitehouse-.gov/news/releases/2003/11/20031124-2.html.

(55) *Cf.* Bernard Sionneau, « Réseaux Conservateurs et Nouvelle Doctrine Américaine de Sécurité », *Annuaire français de relations internationales*, vol. 4, 2003, pp. 498-531.

(56) President of the United States of America, *The National Security of the United States of* America, White House, Washington, septembre 2002, 35 p., sur le site Internet www.white-house.org (dernière consultation le 19 novembre 2003).

(57) Amiral (c.r.) Pierre Lacoste / François Thual, *Services secrets et géopolitique*, Lavauzelle, Pamazol, 2001, p. 115.

L'extension des moyens et des tactiques du renseignement

L'intégration organisationnelle des services et des dispositifs de contrôle

Comme de nombreuses réformes répondant à une situation de crise, les mesures de réorganisation ont commencé en premier lieu par un resserrement de la direction et du fonctionnement des services de renseignement.

L'asymétrie informationnelle constitue un avantage, mais à condition d'être soigneusement dissimulée à l'adversaire, comme le suggérait déjà Sun Tzu (58) (se renseigner, agir en secret et contre-informer, opacifier le système afin d'imposer sa volonté à l'adversaire, le surprendre et l'obliger à se disperser). Pour ce qui est d'Echelon, le partage et le traitement des informations en temps réel, montrèrent, de 1946 à 2001, maintes dysfonctions entre les partenaires du réseau. Au niveau du renseignement en général, les organisations prirent l'habitude de faire cavalier seul. Un agent du FBI tira ainsi les conclusions de ce blocage organisationnel devant la presse, après le 11 septembre 2001 : « *nous ne savions pas ce que nous savions* » (59). Le choc terroriste révéla aussi la négligence du renseignement humain (HUMINT), le désinvestissement du terrain et, inversement, la trop grande confiance accordée aux données électroniques. Le perfectionnisme technique a fini par endormir. Les agences de renseignement, « *belles machines à collecter de l'information, pas à l'analyser* », ont souffert d'un manque redondant de coopération (ce fait est connu depuis les analyses classiques d'Alison concernant le processus de décision lors de la crise de Cuba) (60). De nombreux ratés du temps de l'administration Bush révélèrent l'absence de coopération des services, devenus de véritables forteresses fermées sur elles-mêmes. Comment répondre aux menaces multiformes d'un ennemi insaisissable (61) ? Suivant les recommandations de la Commission Hart-Rudman (62), George W. Bush annonça la création de l'Office of homeland security, confié à l'un de ses fidèles, Tom Ridge, avec pour mission de « *diriger, superviser et coordonner une stratégie nationale d'ensemble pour sauver le pays du terrorisme* ». Il le dota du rang de ministre en officialisant le Departement of homeland security (DHS).

Autre changement après le 11 septembre : la recherche des réseaux de financement du terrorisme plaça le renseignement économique au rang de priorité défensive nationale. Le *National Economic Council* réintégra le *National Security Council*. Chaque entreprise ou institution américaine dis-

(58) Sun Tzu, *L'Art de la guerre*, Hachette, Paris, 2000.

(59) Propos d'un agent du FBI cité par le *New York Times*, 9-10 juin.

(60) Alain Frachon, « FBI-CIA, l'échec », *Le Monde*, 16-17 juin 2002, p. 13.

(61) Ces menaces, caractérisées par le renseignement américain sont : le terrorisme par des moyens conventionnels, cybernétiques et NBCR (nucléaire biologique, chimique, radiologique) ; les opérations informationnelles ; la prolifération d'armes de destruction massive ; la menace du renseignement étranger ; le C3D2 (*Cover, Concealment*, Camouflage, *Denial and deception*) ; le crime organisé.

(62) *Les Guerres secrètes de la mondialisation*, Lavauzelle, Pamazol, 2002, p. 223.

pose désormais d'un correspondant « *Homeland security* ». La création de la « *homeland security policy* » entraîna quant à elle une réorganisation importante des agences fédérales, qui positionne les agents en réseau. Révolution spectaculaire : la CIA a accès maintenant au renseignement intérieur (63). Outre la collaboration avec les divisions SIGINT des agences militaires de renseignement, la NSA s'est vue intimer l'ordre de collaborer avec la CIA, sous le couvert du *SCS Special Collection* (Service des opérationnels clandestins). Ce service, autorisé à utiliser des méthodes illicites d'intrusion dans les systèmes, lui permet d'intercepter des communications bien protégées en utilisant notamment des relais d'écoute situés dans les ambassades et bâtiments diplomatiques.

Le *Department of homeland security* (DHS) mobilise des ressources considérables (64) et génère de nouveaux programmes, comme la surveillance du *net*. Le *Cyber Security Enhancement Act* permet à la police de procéder à des écoutes sans mandat d'un tribunal. Il autorise les fournisseurs Internet à communiquer plus facilement à la police des données concernant leurs abonnés et se montre plus sévère en cas d'attaques informatiques. Le *Patriot Act* (USAPA), signé le 26 octobre 2001, autorise les services de police et de renseignement à pratiquer, sous un contrôle judiciaire réduit, des écoutes et des perquisitions secrètes, la surveillance des communications téléphoniques et des communications par Internet, ainsi que le partage des informations entre tous les services.

Ces décisions heurtent les convictions de nombreux défenseurs de la protection des libertés individuelles car, désormais, les agents fédéraux agissent plus librement pour traquer des suspects. Ils ont la possibilité d'enregistrer des données saisies au clavier. Un bureau du FBI se charge en outre de l'application de la loi *Communications assistance for law enforcement act*, qui impose aux opérateurs l'installation du système de surveillance Carnivore. L'Union européenne n'a pas été oubliée dans la planification américaine : depuis février 2003, la Commission a cédé aux pressions des Etats-Unis concernant « *l'obligation de transmission préalable des listes de passagers aux services des douanes américaines, pour toute compagnie aérienne assurant des vols internationaux à destination du territoire américain* » ; en contrepartie, les douanes américaines – pourtant intégrées dans le DHS – se sont engagées à ne pas retransmettre ces données à d'autres agences fédérales. Le système Apis, entré en vigueur en janvier 2002, permet également de suivre à la trace des industriels français et de savoir dans quels pays des contrats vont être signés.

(63) Thomas STANCTON, « Deux maisons, deux histoires : un statu hors normes », *Le Monde*, 16-17 juin 2002, p. 14.

(64) Joseph HENROTIN, « This could be another Vietnam : la stratégie militaire US à l'épreuve de l'après-11 septembre », *Diplomatie*, n° 5, septembre-octobre 2003, pp. 38-41.

Le TIA (*Total information awareness*), devenu *Terrorism Information Awareness*, a été mis en place pour surveiller et détecter des dangers potentiels, en particulier le terrorisme. Il s'articule autour de *l'Information Awareness Office* (IAO) et de l'*Information Exploitation Office* (IEO). Ce dispositif contrôle les échanges électroniques dans le grand système de données généralisées : toute transaction électronique, tout *e-mail*, tout site visité, tout dépôt bancaire doit être enregistré dans la base, propriété des Etats-Unis. Des entreprises comme Microsoft et AOL auraient collaboré pleinement avec les services de sécurité. Les citoyens américains, comme les étrangers, sont ainsi fichés et le fichage est devenu mondial. C'est John Poindexter, amiral en retraite et ancien conseilleur de Reagan, qui, bien qu'impliqué dans le scandale Iran-Contra, a été choisi pour la mise au point de ce contrôle informatique total. Même refusé par le Sénat, le TIA ne forme-t-il pas un « système des systèmes » ? La dominance informationnelle vise à intégrer tous les décideurs du renseignement et facilite la rapidité du repérage et des interventions. Elle dénie toute initiative à l'adversaire et favorise « *l'intégration inter-armes, inter-agences, inter-alliés, la 'civilianisation' des innovations technologiques et la synergie industrialo-militaire* » (65). Au C4ISR, s'intègrent des sous-systèmes qui conditionnent le fonctionnement, les armements, la recherche et le développement, la production, l'acquisition, la logistique, les infrastructures, les réseaux humains et les systèmes culturels, politiques et juridiques soutenant la puissance.

Parallèlement à ces dispositifs organisationnels, les techniques de protection des messages ont été renforcées.

Le renforcement des techniques de cryptage

En raison des problèmes organisationnels, mais surtout des évolutions des technologies informatiques, la NSA s'est trouvée contrainte de réadapter tout son système antérieur d'interception SIGINT (66). COMINT se trouvant dépassé par la « *réception de mille milliards de bits toutes les douze heures* », elle a dû accroître la puissance de traitement (67) et installer un système de protection inédit contre l'effet TEMPEST (68), qui empêche l'émission de signaux radio révélant l'activité de surveillance elle-même. Elle a édicté la norme « Nacsim 5100 A », qui fait autorité en matière de tests de protection.

(65) Saïda BEDAR, *op. cit.*, 2001.

(66) « *Today*, SIGINT continues to play an important role in maintaining the superpower status of the United States ». *Cf.* le site Internet www.nsa.gov/about–nsa/indes.html.

(67) Soit « *l'équivalent en informations de l'ensemble de la bibliothèque du Congrès américain* ». *Cf.* Jacques BAUD, *op. cit.*, p. 491.

(68) « Transient Electro Magnetic Pulse Emanation Surveillance Technology », système d'écoute du rayonnement informatique qui se base sur les ondes électromagnétiques s'échappant de tout matériel électrique et intercepte ces ondes à distance. La protection nécessite un espace faradisé. *Cf. Quand la tempête souffle sur nos ordinateurs*, février 2000, sur le site Internet de Zataz, www.zataz.com/zatazv7/tempest.htm.

Il a fallu aussi veiller à la protection des systèmes cryptologiques, après un débat public (69) qui gagna la société civile et le Congrès (70). Les tentatives visant à imposer aux utilisateurs d'outils de cryptologie le dépôt de clefs de déchiffrement auprès d'une autorité gouvernementale, ont conduit à une pénétration du secteur privé par les entreprises d'Etat. C'est notamment le cas de Communications-Electronics Security Group (CESG) du GCHQ britannique ou encore de la firme IN-Q-Tel de la Central Intelligence Agency (CIA) (71). Le processus a révélé ses limites. La compagnie helvétique Crypto AG, qui fournit des moyens de cryptage à plus de cent vingt Etats, a ainsi été soupçonnée de fournir des clefs à la NSA : l'affaire éclata suite à l'arrestation, en 1992, d'un de ses attachés commerciaux par l'Iran; le VEVAK, service de renseignement iranien, aurait découvert dans ses programmes, une *back-door*, sorte de cheval de Troie de la NSA. Autre cas de figure, celui de la société Inslaw, qui avait mis au point le logiciel de base de données, PROMIS pour le ministère américain de la Justice. Lorsqu'elle a été mise en faillite, on s'aperçut que les codes sources et les droits associés de l'entreprise avaient été récupérés frauduleusement (même criminellement) et que des versions piégées avaient été vendues, avec l'aide des Israéliens, à des pays et des organisations cibles, surtout au Moyen-Orient, en Amérique latine, mais aussi en France (72), ce qui permettait de surveiller depuis Washington, le contenu des ordinateurs mis en réseau.

Après les attentats du 11 septembre 2001, la puissance informatique au niveau du criblage et de l'interconnexion de fichiers a été également améliorée. Cependant, l'apparition des réseaux de fibres optiques, depuis dix ans, rend difficiles les interceptions, un accès physique aux câbles devenant nécessaire. Le réseau doit en effet appartenir à un pays collaborateur ou le traverser. La Commission Bremer a en outre dénoncé la faiblesse des moyens affectés à l'analyse des interceptions électroniques et des ordinateurs des organisations terroristes ou de leurs membres, lesquels disposent de crypto-systèmes puissants. Elle a déploré aussi le niveau peu élevé des capacités linguistiques de la communauté du monde du renseignement, du fait de la rareté des effectifs de traducteurs et d'analystes dans certaines langues peu parlées (73). Autre point d'achoppement identifié, celui du collectage : il pâtit toujours du volume incontrôlable d'informations, la capacité humaine ne pouvant en faire usage correctement. Des milliers d'heures de bandes magnétiques audio et de pages de texte s'accumulent ainsi sans être examinées ni traduites. La surveillance se heurte enfin au silence du fait de la méfiance adverse : initiée, celle-ci utilise en effet des *talkies-walkies* ou

(69) *Cf.* le site Internet www.nsa.gov/about–nsa/mission.html.

(70) « Harvest of Schame '99 : trade secrets », *Mojowire*, novembre-décembre 1999, sur le site Internet www.motherjones.com/mother_jones/ND99;outfront.html (dernière consultation le 3 novembre 2000).

(71) Jacques BAUD, *op. cit.*, p. 191.

(72) Fabrizio CALVI/Thierry PFISTER, *L'Œil de Washington*, Albin Michel, 1997, 363 p.

(73) Bremer Commission on international terrorism, *Countering the Changing Threat of International Terrorism. Pursuant to Public Law 2777*, 5 juin 2000, p. 13, cité par Jean GUISNEL, *op. cit.*, p. 293.

des moyens ancestraux de boîtes aux lettres et de « bouche à oreille ». La dominance cybernétique en tant que tactique informationnelle révèle donc certaines failles. Pourtant, même si elle s'est complexifiée et si elle doit sans cesse s'adapter aux nouvelles techniques, elle reste incontournable en raison de l'enjeu que représente la maîtrise d'un nouveau territoire stratégique : l'espace cybernétique.

Le contrôle du cyberespace

Après la terre, la mer, l'air et l'espace, le « cybermonde » forme un cinquième espace géostratégique. La mise en œuvre de stratégies globales de contrôle doit permettre aux services de défense de « *couvrir l'ensemble de la planète de leur réseau satellitaire, électronique et optique, tout en créant l'environnement informationnel nécessaire aux nouvelles projections de forces militaires* » (74). Le concept d'« *information dominance* » se trouve au cœur de l'action de l'*US Army* et de l'*US Air Force*. De même, le système sécuritaire spatial américain a-t-il été restructuré autour du Space Com de l'US Air Force. Les satellites du NRO (75), de la NSA et de la NIMA (76) surveillent les activités humaines, civiles et militaires. Les agences météorologiques, cartographiques et environnementales, ainsi que les actions offensives comme « *cyberdouleur* » (isolant informationnellement un gouvernement ou un état-major et bloquant les infrastructures vitales d'un pays), ou défensives (le « *parapluie informationnel* ») dans le cyberespace devraient être supervisées par *Space Com* (77). Le projet *Nextview*, qui englobe et dépasse les deux anciens concepts d'imagerie spatiale et de cartographie, a inauguré une nouvelle forme d'intelligence géospatiale, GEOINT (78).

En parallèle à la « cyberguerre » de type militaire, la domination du cyberespace se réalise à travers une *netwar* (79). L'information multiforme devient un élément-clef des rapports de force stratégiques et transforme les formes de la guerre. Ces mutations ont favorisé la privatisation de la force armée, du terrorisme, du mercenariat, du rôle des ONG et de toutes les

(74) Jean-Michel VALANTIN, « Militarisation de l'espace et puissance américaine », *Diplomatie*, n° 1, janvier-février 2003, pp. 50-52.

(75) Le *National Reconnaissance Office*, basé à Chantilly en Virginie et créée en 1961, est un service du Département de la Défense qui planifie et conduit la reconnaissance par satellites, gère, conjointement avec la NSA, des stations réceptrices de renseignement électronique d'origine satellitaire et les stations de réception satellitaire dédiées à la surveillance et à l'espionnage.

(76) *National Imagery and Mapping Agency*, créée en 1996 et basée à Faiwax. *Cf.* le site Internet www.nima.mil. Depuis le 24 novembre, NIMA a rejoint le club très sélect des agences de renseignement en trois lettres (CIA, DIA, NSA), en devenant la *National Geospatial-Intelligence Agency* (NGA). *Cf.* « La Nima est morte, vive la NGA », *Intelligenceonline*, n° 464, 28 novembre 2003 ; « NIMA changes name to National Geospatial-Intelligence Agency », *DoD news*, n° 881-03, 24 novembre 2003, sur le site Internet www.defenselink.mil/releases/2003/nr20031124-0684.html.

(77) *Ibidem*.

(78) « Le projet NextView lance l'intelligence géospatiale », *Intelligenceonline*, n° 462, 17 octobre 2003, sur le site Internet www.intelligenceonline.fr.

(79) « *Conflits de société, nés de l'émergence des nouvelles idées poussés dans les réseaux de communication interconnectés* ». *Cf.* Jean GUISNEL, *Guerre dans le cyberespace : services secrets et Internet*, La Découverte, Paris, 1997, p. 218.

organisations en réseau, impliquant un effacement relatif de l'Etat territorial dans les démocraties occidentales (80). D'où la nécessité pour les Etats-Unis de renforcer le réseau créé en 1994, INTELINK, hautement sécurisé, réservé à l'usage exclusif de leurs services de renseignements, par lequel transitent les images numérisées prises par les satellites espions du NRO. Les nouvelles techniques de protection ont été particulièrement favorisées par le budget fédéral et ont connu un développement plus important que celui de la diplomatie (81). Elles ont facilité également le rapprochement entre les processus RMA et RBA (*revolution in business affair*s). Ainsi, la *Defence Advanced Research Projects Agency* du Pentagone (DARPA), dirigée par Anthony Tether, a été dotée en 2003 d'un budget de 2,685 milliards de dollars. Elle finance de nombreuses recherches sur des créneaux technologiques porteurs issus des réflexions sur la sécurité, le concept de « guerre infocentrée », les ruptures et les transferts de technologies. Elle passe des contrats avec des chercheurs extérieurs et contribue au développement de sociétés actives dans les technologies de l'information. Le Pentagone finance quant à lui les recherches dans des disciplines de pointe comme les MEMS (*microelectronics, microbiology et microelectromecanical systems*) (82). Avec le *Cyber Security Act*, George W. Bush a alloué, fin 2002, 900 millions de dollars sur cinq ans à l'enseignement supérieur pour stimuler la recherche dans les technologies de sécurité et de surveillance électronique. L'agence de recherche *Homeland Security Advanced Research Projects Agency*, créée dans le cadre du *Homeland Security Bill*, prévoit de distribuer près de 500 millions de dollars pour la lutte contre le terrorisme, vu sous l'angle des technologies. En misant de gros budgets sur la *high-tech* en matière de *space power* et d'armement, en privatisant les secteurs où la concurrence étrangère est forte, les Etats-Unis déploient ainsi une stratégie d'épuisement des ressources de l'adversaire, en particulier des concurrents étatisés.

Dans ce dispositif global, les techniques de sécurisation des réseaux stimulent la coopération entre les agences de sécurité, l'administration et les entreprises *high-tech*. La NSA s'assure de la transparence des solutions, stimule la demande par sa participation à l'ILETS en libéralisant les exportations cryptographiques et en menant des actions de *lobbying* intense (83). Dans l'industrie géospatiale américaine, dépendante des commandes gouvernementales, s'affrontent deux blocs de l'imagerie commerciale : Space Imaging, liée *à* Lockeed Martin et Raytheon, et DigitalGlobe, lié à Boeing et BAE Systems, qui se voit octroyer la totalité de NextView au risque de sup-

(80) Bruno TERTRAIS, « Faut-il croire à la 'révolution dans les affaires militaires' ? », *Politique étrangère,* n° 3, 1998, pp. 611-629.

(81) Amiral (c.r.) Pierre LACOSTE / François THUAL, *Services secrets et géopolitique*, Lavauzelle, 2001, pp. 113-115.

(82) « Bienvenue dans l'économie kaki », *Enjeux,* novembre 2003, pp. 62-84.

(83) Loup Francart, *Infosphère et intelligence stratégique*, Economica / IHEDN, Paris, 2002, p. 290.

primer toute concurrence (84). Un nouveau programme de sécurité des systèmes d'information a mis récemment l'accent sur les relations public/privé. En janvier 1999, la CIA a créé In-Q-Tel, société de capital-risque à but non lucratif, chargée de détecter et d'investir dans les nouvelles technologies permettant de collecter, d'analyser et de diffuser le renseignement. In-Q-Tel a déjà investi dans dix-huit sociétés, parmi lesquelles Mohomine, instituée en 1999, dont une « brique » logicielle contribue au système d'information Accord, développé par le consortium Accenture-Peoplesoft pour le ministère de l'Economie, des Finances et de l'Industrie français (85). Des fonds d'investissements américains comme Texas Pacific Group ou Carlyle Group s'efforcent de prendre le contrôle de sociétés françaises et européennes qui maîtrisent les technologies de la cryptologie.

Les services américains exercent également une tutelle effective sur *Internet*, notamment en raison du fait que les infrastructures se concentrent aux Etats-Unis. Internet Society (ISOC) a la charge depuis 1982 de la concession des noms de domaines en « .org » (deux millions d'adresses) et collabore avec AFILIAS, autre entreprise américaine, qui, elle, s'occupe du domaine « .info ». Le Département de la Défense assure un contrôle étroit sur l'ICANN (*Internet Corporation for Assigned Names and Numbers*), qui gère les adresses IP, les protocoles et les noms de domaines. De plus, l'industrie *Internet* comprend des sociétés comme Cisco, IBM, Sun, AOL, Microsoft, Yahoo... Les opérateurs et les fournisseurs d'accès principaux sont américains. La nécessité d'une gestion intergouvernementale de l'*Internet*, après avoir été discutée lors du sommet mondial de l'information (SMI) à Genève, fin 2003, doit être évoquée à nouveau à Tunis en 2005.

Notons encore que les télécommunications constituent un terrain sensible. Un exemple récent le prouve : la démission, le 28 mars 2003, de Richard Perle, de la direction du *Defense Advisory Board* du Pentagone, s'expliquerait par le fait qu'il assurait le *lobbying* de Global Crossing. Cette société, spécialisée dans les réseaux optiques, cherchait à se faire racheter par des investisseurs de Hong-Kong et de Singapour, mais la transaction, impliquant de la haute technologie, fut évidemment mal perçue par le Pentagone et le FBI. Des pare-feux ont été établis pour protéger le patrimoine technologique des Etats-Unis. Le *National Security Telecommunications Advisory Board*, créé par Reagan en 1982, conseille le Président en matière de sécurité nationale et de technologies. L'OPIC, petite agence fédérale, créée en 1971 (*Overseas Private Investment Corporation*) assiste les industriels des télécoms dans leur conquête de marché à l'export ; elle couvre également le risque-pays et octroie des prêts. Le CFIUS (*Committee on Foreign Invesment in the*

(84) Consulter l'infographie « L'affrontement de deux 'petits 4 géants du géospatial' », *Intelligenceonline*, n° 462, 17 octobre 2003, sur le site Internet intelligenceonline.fr.

(85) *Cf.* « The 18 gold Nuggets Found by the CIA », *Intelligenceonline*, n° 458, 31 juillet 2003 ; Bernard CARAYON, *Intelligence économique, compétitivité et cohésion sociale : rapport au Premier ministre*, juin 2003, p. 48, sur le site Internet www.bcarayon-ie.com.

United States), dirigé par le Secrétaire du Trésor, regroupe des hauts responsables d'une dizaine d'agences fédérales, dont la NSA. Son efficacité a été démontrée : quand, en mai 2001, il eut à examiner le risque d'absorption de la société américaine Lucent par le français Alcatel, équipementier de télécoms et pour l'*Internet* haut débit, susceptible d'aboutir à la naissance d'un *leader* étranger mondial dans un domaine sensible, une déstabilisation, bien orchestrée à travers les médias, évita qu'une entreprise étrangère ne contrôle les technologies d'accès aux fibres optiques, favorisant ainsi la connexion physique nécessaire au bon fonctionnement de SIGINT (86).

Le contrôle des normes logistiques et informationnelles, la connexion des réseaux, l'« interopérabilité » des systèmes

Sous prétexte de favoriser la coopération internationale et la libre commercialisation, les Etats-Unis veulent limiter le développement des concurrents « sérieux » *(peer competitors)* en renforçant les moyens de leur sécurité. Une « domination centre-périphérie » s'exerce (87) par la maîtrise des facteurs de l'interdépendance, par le contrôle et la sécurisation des territoires échappant à toute souveraineté, qui se focalise sur les normes dans les champs logistiques et informationnels, sur la connexion des réseaux, sur « l'interopérabilité » des systèmes.

Les industriels américains se placent tous dans une logique de « guerre économique » qui manœuvre avec les opportunités et les menaces induites par l'« interopérabilité » (88). Le concept est devenu à la mode depuis William Cohen, ancien Secrétaire à la Défense de l'Administration Clinton. Ainsi, le succès de Loockeed Martin dans la vente d'avions de guerre à la Pologne a fragilisé la politique de défense commune européenne, d'autant que les Etats-Unis forment les pilotes et verrouillent le marché futur de la maintenance. De même, le déploiement du service de certification *Identrus*, infrastructure mondiale de gestion de clefs publiques pour sécuriser les communications et les transactions interbancaires ou commerciales inter-entreprises, déjà contrôlé par les Etats-Unis, risque également de placer les grandes institutions financières en situation de dépendance, malgré les avantages d'interopérabilité, de développement accru des échanges et de réduction des délais.

(86) Nicolas MOINET, *Les Batailles secrètes de la science et de la technologie : Gemplus et autres énigmes,* Lavauzelle, Pamazol, 2003, p. 44.

(87) Saïda BEDAR, 2003, *op. cit.*

(88) « *The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together* ». *Cf.* Joint Chiefs of Staff, *Joint Vision 2020*, US Government Printing Office, Washingthon DC, juin 2000, sur le site Internet www.dtic.mil/jv2020. Certains analystes affirment à ce sujet : « *l'objectif est de pouvoir planifier le déploiement synchronique ou diachronique de systèmes d'armes complexes, sans qu'aucune défaillance n'advienne dans aucune des interactions des systèmes entre eux* [...]. *Celle-ci s'appuie non plus sur la maîtrise du secret ou la gestion des sources ouvertes, mais sur la maîtrise des standards d'interopérabilité interne (coordination nationale) et externe (maîtrise des barrières à l'entrée sur les marchés mondiaux* ».

L'enjeu n'est plus celui d'une expansion territoriale étatique, mais celui d'une emprise spatiale renforcée, de type « extra-territorial » et social. La conquête de l'espace orbital et atmosphérique, du cyberespace, l'investissement de nouvelles sphères par la privatisation des secteurs étatiques, dont la sécurité, illustrent ainsi la nouvelle stratégie. Tout ce dispositif de contrôle élargi s'appuie sur des sociétés de renseignement, sur des cabinets de *lobbying* et d'audit et sur des réseaux d'entreprises par le biais des NOC (*Non Official Cover*), agents qui utilisent souvent la couverture d'hommes d'affaires et qui cherchent des informations auprès de fonctionnaires de gouvernements étrangers, particulièrement dans le secteur des industries sensibles.

Le complément, la diplomatie américaine, par le biais de ses ambassades et consulats, forme un appareil d'information important au service de ses industriels. Les APP (*American Presence Posts*), sous l'égide des ambassadeurs, ont été créés pour amplifier l'influence des Etats-Unis auprès des milieux économiques. Les stratégies offensives s'exercent encore par infiltration financière ou par forte présence dans les organisations internationales et la communauté bancaire. On apprend ainsi que Desmond Perkins, fonctionnaire d'origine britannique, chef du bureau chargé de crypter les communications de la commission européenne, a confié à la NSA la vérification des systèmes de chiffrement de l'Union (89)... De même, la dénommée « *Never Say Anything* » reconvertit ses agents et étend son influence dans le privé par un programme de *soft landing*.

L'arsenal offensif en matière de conquêtes de marchés a été également renforcé par le biais de l'intelligence humanitaire. Cette approche a été mise au point par l'*United States Special Operation Command* et expérimentée dans le cadre des Nations Unies au Cambodge, en Somalie, en Bosnie, à Haïti... Elle consiste à assister au redémarrage économique d'un Etat antérieurement au conflit, à influencer et rafler les marchés à leur source.

Parallèlement aux objectifs politiques, militaires, technologiques et économiques, les Etats-Unis imposent leurs vues en maîtrisant les connaissances, en amont, à travers divers circuits éducatifs et, en aval, à travers les médias traditionnels et *Internet* (90). Ils participent à des forums comme Davos, produisent et utilisent la majorité des sources ouvertes. Pionniers dans les concepts du *management*, ils sont assurés d'un mimétisme conformiste de la part de plusieurs cénacles et institutions de diffusion et d'influence au niveau international ; ils ouvrent à l'étranger, en particulier en Europe, des succursales de fondations et des instituts de recherche financés par le mécé-

(89) Laurent ZECCHINI, « Les curieuses accointances du responsable des opérations de cryptage de Bruxelles », *Le Monde*, 3 janvier 2001.

(90) Christian HARBULOT / Nicolas MOINET / Didier LUCAS, « La guerre cognitive : à la recherche de la suprématie stratégique », communication présentée au forum « Intelligence économique » de l'Association aéronautique et astronautique française, le 25 septembre 2002, à Menton, consultable sur le site Internet www.infoguerre.com/fichiers/3AF25092002.pdf (dernière consultation le 15 octobre 2002).

nat. Les réseaux privés de recherche universitaire attirent les meilleurs chercheurs de l'ancienne Europe de l'Est et de la CEI. Ils y gagnent des informations et des expertises, ainsi que l'estime et la reconnaissance (91). Les fondations financent aussi des réunions des services secrets de leurs anciens adversaires. Par *social learning*, ils socialisent les futures élites d'un pays visé, formatent leurs esprits et s'assurent de collaborations futures (92). Des milliardaires contrôlent des fondations, des *think tanks* ou des groupes influents (93). Ces entités fournissent des idées et imposent progressivement leurs conceptions. Elles mènent en parallèle des travaux pour sécuriser l'architecture informationnelle des pays, mais aussi pour valoriser la prépondérance diplomatique, économique, scientifique et culturelle américaine. Ces réseaux du savoir, en apparence pluralistes, ont pour fonction de faciliter la diffusion de la stratégie globale des Etats-Unis, sous le contrôle d'Echelon et des services secrets.

Certains programmes de recherche regroupent des spécialistes de la gestion des connaissances, de l'extraction des données et de la modélisation de processus complexes. Philosophes, linguistes, mathématiciens, sociologues, informaticiens, universitaires du public ou du privé, réfléchissent ainsi à l'automatisation du sens, fascinante mais terrifiante, à partir d'une masse d'informations stockées. L'ARDA (*Advanced R & D Activity*), qui dépend de la NSA, gère des programmes liés aux technologies de l'information intéressant la communauté du renseignement. Elle a lancé en septembre 2002 le programme NIMD (*Novel Intelligence for Massive Data*) avec la NIMA, qui dispose d'un budget de subventions de 64 millions de dollars. Certains des organismes et sociétés ayant reçu un financement de la NIMA ont collaboré avec des centres universitaires comme le Rensselear Polytechnic Institute, la Carnegie Mellon University, le Palo Alto Research Center (94).

*
* *

Ces nouveaux dispositifs de rationalisation et de modernisation ont pour fonction de relier les réseaux techniques, isolés sur eux-mêmes, du temps du premier Echelon, et les réseaux organisationnels et sociaux. Tirant les leçons de la tragédie du 11 septembre, la puissance américaine veut exercer des actions d'entrisme, de déstabilisation d'entités économiques, d'encercle-

(91) Amiral (c.r.) Pierre LACOSTE / François THUAL, *op. cit.*, p. 165.

(92) Eric DENÉCÉ, *Le Nouveau Contexte des échanges et ses règles cachées : information, stratégie, guerre économique*, L'Harmattan, 2000, p. 92.

(93) Par exemple, Richard Scaife Mellon investit l'Allegheny Foundation et la Sarah Foundation ; la Carthage Foundation, subventionne l'Heritage Foundation, l'American Enterprise Institute et le Hoover Institute ; William Coors finance la Coors Foundation, l'Olin Foundation, la Lynde et Hary Bradley Foundation. ; l'empire Murdoch contrôle les médias. *Cf.* Thierry SERVAL, « Guerre de l'information et contexte du pouvoir », 28 octobre 2003, sur le site Internet Infoguerre www.infoguerre.com/article.php ?op = Print&sid = 671 (dernière consultation le 3 novembre 2003).

(94) *Cf.* « Qui sont les pionniers du nouveau renseignement : infographie de Charles B. », *Intelligenceonline*, n° 461, 2 octobre 2003.

ments de marchés et de territoires scientifiques et culturels, quand il ne s'agit pas d'Etats. Son *hard power*, visible dans sa guerre contre l'Iraq, s'imbrique dans des actions indirectes de *soft power*, sous-tendues par le cycle de l'intelligence qui, de la collecte à la diffusion de l'information, se targue d'anticiper les événements.

Echelon, dont les fonctions se trouvent aujourd'hui démultipliées, s'inscrit dans une dynamique nouvelle, à la fois défensive, offensive, et multifonctionnelle. Dans son évolution, il a préfiguré l'actuel système d'écoute, de collecte d'informations et de renseignements, plus vaste que jamais dans sa dimension mondialisée. Son histoire nous enseigne cependant qu'il ne faut jamais surestimer la cohérence et l'efficacité d'un système technique. Adapté à la « guerre de l'information » désormais engagée, le nouveau modèle de renseignement global et intersectoriel américian préfigure un monde de représentations et de comportements déteritorrialisés dans le cyberespace. L'avenir nous dira si la débauche de moyens actionnés est à la mesure des ambitions politiques qui se cachent derrière, qui peuvent s'effacer d'une équipe dirigeante à l'autre, ou être relativisées tant par le hasard des circonstances, que par la ruse humaine, sans limite et aussi forte que le secret.