COMITE PERMANENT DE CONTROLE

DES SERVICES DE RENSEIGNEMENTS

RAPPORT COMPLEMENTAIRE SUR LA MANIERE DONT LES SERVICES BELGES DE RENSEIGNEMENT REAGISSENT FACE A L'EVENTUALITE D'UN RESEAU "ECHELON" D'INTERCEPTION DES COMMUNICATIONS

Rue de la Loi 52 - 1040 Bruxelles

Tél 02/286.28.11 -- Fax 02/286.29.99

CHAPITRE 1 : *RAPPORT COMPLEMENTAIRE SUR LA MANIERE DONT LES SERVICES BELGES DE RENSEIGNEMENT REAGISSENT FACE A L'EVENTUALITE D'UN RESEAU «ECHELON» D'INTERCEPTION DES COMMUNICATIONS*

1. INTRODUCTION

D'une manière générale, il convient de rappeler que le Comité permanent R s'est déjà penché par le passé sur la protection des systèmes informatiques et de communication. Dans ce cadre il avait recommandé, dès 1994, qu'un organisme officiel soit chargé de concevoir et d'appliquer une politique globale de sécurité pour l'ensemble des systèmes d'information de la fonction publique.

On doit encore citer dans le même ordre d'idées, l'étude et l'enquête réalisées en 1998 sur la participation des services de renseignement belges, spécialement le SGR, à des programmes satellitaires de renseignement. L'intérêt du Comité pour cette question répondait à une préoccupation politique concrétisée e.a. dans la déclaration gouvernementale du 28 juin 1995 exprimant la volonté de notre pays de « contribuer activement à l'élaboration d'une architecture de sécurité européenne en vue de promouvoir la stabilité du continent européen et d'éviter de nouveaux clivages » (Rapport d'activités 1998 - p. 130 et suivantes).

L'existence d'un réseau « ECHELON », qui aurait été mis en place par les Etats-Unis et par la Grande Bretagne notamment, en vue d'intercepter toutes les télécommunications civiles européennes, a été révélée en septembre 1998 par un rapport destiné au Parlement européen. La diffusion de ce rapport par les médias a éveillé l'attention de certains gouvernements, français notamment, ainsi que celui du Parlement belge.

Le 31 janvier 2000, les commissions permanentes de la Chambre des représentants et du Sénat, respectivement chargées du suivi des Comités permanents P et R, se sont réunies pour examiner le rapport annuel d'activités de ce dernier, incluant l'enquête que le Comité R a consacré à la manière dont *« les services belges de renseignements réagissent face à l'éventualité d'un système américain « Echelon » d'interception des communications téléphoniques et fax en Belgique »*. Cette enquête avait été ouverte sur l'initiative de membres du Parlement fédéral. Ces derniers posaient également la question suivante : « *Nos services cherchent-ils à établir l'existence du système Echelon, et le cas échéant, à protéger les entreprises et les citoyens belges contre ces interceptions ? ".*

Il ressort des conclusions de ce premier rapport[1] que les services de renseignement belges ont globalement répondu par la négative à ces questions invoquant principalement le fait qu'ils ne disposaient pas des possibilités techniques qui leur permettraient d'établir eux-mêmes le constat de l'existence du système « Echelon ». Leur connaissance du sujet résultait donc seulement des informations provenant de la consultation de sources ouvertes.

La Sûreté de l'Etat n 'avait donc pas été en mesure de confirmer l'existence de pratiques d'interceptions de télécommunications. Ce service se déclarait confronté à un manque de moyens tant sur le plan du personnel que sur le plan du matériel technique. Ses moyens d'investigation ne lui permettaient donc pas de vérifier l'existence du système « Echelon ».

La loi organique du 30 novembre 1998 des services de renseignements, en son article 7, assigne cependant une mission spécifique à la Sûreté de l'Etat : *« rechercher, analyser et traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel. »*

Le Service Général du Renseignement et de la Sécurité avait considéré quant à lui l'existence du système « Echelon » comme un fait acquis. Bien qu'ayant ciblé « les menaces auxquelles se voit confrontée notre société de l'information et de la communication, dont « Echelon » n'est qu'une illustration », le SGR n'effectuait cependant pas de recherche active sur ce réseau, se fondant, d'une part, sur le fait que la défense du potentiel scientifique et économique n'est pas une des compétences qui lui est attribuée par la nouvelle loi organique du 30 novembre 1998 sur les services de renseignements et, d'autre part, sur les restrictions légales qui lui sont imposées en matière de captage des radiocommunications.

Au terme de la loi organique, le SGR est investi d'une mission de protection des systèmes informatiques et de communications militaires ainsi que de ceux que gère le ministre de la Défense nationale. Une extension d'une telle mission à des intérêts autres que militaires n'est pas mentionnée explicitement dans la loi. Sans doute peut-on comprendre que ce type de mission rentre dans le cadre de la défense du potentiel scientifique ou économique qui est de la compétence de la Sûreté de l'Etat. Toutefois, le SGR, représenté au sein du Collège du Renseignement et de la Sécurité, se propose de contribuer aussi bien à la conception des structures fédérales qu'à l'établissement d'une politique générale en matière de sécurisation des réseaux informatiques.

Le rapport général d'activités 1999 du Comité permanent R comprenant les premiers résultats de l'enquête relative à la problématique d'« Echelon » a été approuvé le 14 février 2000 par les commissions réunies de la Chambre des représentants et du Sénat respectivement chargées du suivi des Comités permanents P et R.

Les Commissions permanentes de suivi ont en outre confié au Comité R la mission de poursuivre ses investigations en cette matière et de leur faire parvenir le présent rapport complémentaire pour la mi-mars 2000.

---

(1) Depuis la clôture, en août 99, de ce premier rapport d'enquête du Comité R, l'existence du réseau Echelon a été confirmée sur la base d'éléments que l'on trouvera repris et développés dans le rapport des experts mandatés par le Comité (voir p. 13 et suivantes)

2. PROCEDURE

Par courrier du 17 février 2000, le président du Comité permanent R a informé Madame Timmermans administrateur général a.i. de la Sûreté de l'Etat et le général-major Michaux, chef du SGR, que les commissions de suivi avaient demandé la poursuite de l'enquête sur le réseau « Echelon ».

Le 21 février 2000, le Comité R a reçu le courrier du président du Sénat daté du 14 février 2000 confirmant cette demande en ces termes : *« les commissions de suivi ont clairement exprimé le souhait que le Comité R poursuive l'enquête sur le système « Echelon », et qu'il s'informe, dans ce cadre, sur l'arrestation du major français « Bunel », afin de déterminer que les informations qui ont mené à son arrestation proviennent d'un système de surveillance électronique ».*

Le 22 février 2000, le Comité permanent R a donc décidé :

1. de poursuivre lui-même l'enquête sur le réseau « Echelon » en se faisant assister conformément à l'article 48 § 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, par deux experts à savoir :

   - le Professeur Yves Poullet, Docteur en Droit et directeur du Centre de Recherche Informatique et Droit des Facultés Universitaires Notre Dame de la Paix à Namur et membre de la Commission de protection de la vie privée;

     ainsi que son collaborateur,

   - M. Jean-Marc Dinant, Maître et Doctorant en Informatique,

     auteurs de plusieurs travaux de recherche sur le thème de la vie privée et de la sécurité des données personnelles sur Internet.

2. d'ouvrir une seconde enquête « sur la manière dont les services de renseignement ont participé à la découverte d'une affaire d'espionnage » et de charger le Service d'enquêtes de cette seconde investigation [(2)].

Le contrat définissant la mission des experts et reprenant la prestation de serment suivant la formule de la cour d'assises visée par l'article 48 § 3 de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement a été contresigné par les experts et par le président du Comité permanent R le 23 février 2000.

Deux membres du Comité R ont assisté à la réunion de la commission des libertés et des droits des citoyens, de la Justice et des affaires intérieures du Parlement européen, qui s'est tenue à Bruxelles les 22 et 23 février 2000. M. Dinant a également assisté à la réunion du 23 février au cours de laquelle a été entendu M. Duncan Campbell, auteur du rapport sur le réseau « Echelon ».

Les membres du Comité R ont entendu Madame Timmermans, administrateur général a.i. de la Sûreté de l'Etat, le jeudi 2 mars 2000. Celle-ci a apporté quelques précisions par courrier du 6 mars 2000.

---

(2) Au stade actuel de l'enquête, on peut déjà dire que ni la Sûreté de l'Etat, ni le SGR ne sont en mesure de soutenir l'existence d'un système de surveillance électronique, quel qu'il soit, à l'origine de la découverte des activités délictueuses du Major Bunel

Le 3 mars 2000, le Comité R a procédé à l'audition du Général-major Michaux, chef du SGR.

Les compte-rendus de ces entretiens figurant dans le présent rapport ont été rédigés en ayant égard aux remarques ultérieurement exprimées par écrit par les personnes auditionnées.

Les experts désignés par le Comité R ont déposé leur rapport le 7 mars 2000.

Une réunion de travail a été organisée le 9 mars 2000, qui a permis au Comité R de procéder à un échange de vues avec Messieurs les experts Poullet et Dinant.

Le 10 mars, le Président du Comité R a adressé une apostille au Chef du service d'enquêtes demandant qu'il soit procédé d'urgence à l'enquête concernant *« l'arrestation du major français Bunel afin de déterminer que les éléments qui ont mené à son arrestation proviennent d'un système de surveillance électronique »* (voir ci-dessus).

Le même jour, cette enquête a été notifiée par le Chef du Service d'enquêtes aux Ministres de la Justice et de la Défense nationale conformément à l'article 43 alinéa 1 de la loi organique du 18 juillet 1991.

Le présent rapport a été approuvé par le Comité permanent R le 13 mars 2000.

3. QUELQUES DERNIERES MANIFESTATIONS DE L'INTERET PARLEMENTAIRE CONCERNANT LA PROBLEMATIQUE DE L'EXISTENCE D'UN RESEAU « ECHELON ».

3.1. L'intérêt du Parlement Européen.

Le Traité d'Amsterdam a renforcé l'obligation de l'Union européenne d'assurer la protection des données personnelles dans le cadre du droit fondamental à la protection de la vie privée (article 8 de la Convention européenne des droits de l'homme reprise par l'article 6 du Traité UE).

Les 22 et 23 février derniers, la commission des libertés et des droits des citoyens, de la Justice et des affaires intérieures du Parlement européen s'est réunie à Bruxelles sur le thème « l'Union européenne et la protection des données ».

Le but des auditions prévues à cette occasion était de passer en revue les questions sensibles de la stratégie de l'Union européenne, qu'elle agisse dans le cadre de ses compétences communautaires et, en particulier celui de la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci, (JO L 281 du 23.11. 1995 p. 31) ou dans celui d'autres politiques et formes de coopération (IIème pilier: politique étrangère et de sécurité commune, IIIème pilier : coopération policière et judiciaire en matière pénale).

La réunion du mercredi 23 février était notamment consacrée aux « *atteintes à la protection des données en dehors de la coopération judiciaire et policière : le problème des interceptions des télécommunications (ECHELON) ».* M. Duncan Campbell, auteur de l'étude commandée par le Parlement européen, y a présenté son rapport sur la problématique des interceptions des télécommunications et des conditions institutionnelles, politiques et opérationnelles qui les rendent possibles.

A l'issue de la discussion de ce rapport, les parlementaires du groupe des « Verts » du Parlement européen ont entrepris les actes de procédure nécessaires pour créer une commission d'enquête sur le sujet.

3.2. L'intérêt des parlementaires belges.

Comme on l'a dit plus haut, outre les initiatives parlementaires qui sont à l'origine de l'enquête initiale sur le système Echelon, il convient de souligner que depuis les révélations sur le réseau Echelon récemment apparues dans les médias, le sujet a donné lieu, dans notre pays, à un renforcement de l'intérêt des représentants de la nation pour ce sujet sensible et préoccupant à plusieurs égards.

Le complément d'enquête qui fait l'objet du présent rapport, ainsi que les questions posées par plusieurs parlementaires (*voir compte rendu analytique de la réunion publique de commission des relations extérieures en date du 22/02/2000 – « CRA 50 – COM 130 »*) en sont l'illustration.

3.3. L'intérêt de l'Assemblée Nationale française.

Selon le compte-rendu n° 27 de la Commission de la Défense nationale et des Forces Armées du mardi 29 février 2000 (*http://www.assemblee-nationale.fr*), son Président Paul Quilès, après avoir fait référence au débat engagé dans plusieurs Parlements étrangers et au Parlement européen, ainsi que dans le public, sur le réseau dit « Echelon », a souligné qu'il appartenait à la Commission de la Défense de mener une enquête sur un système d'interception des communications dans le monde qui, en raison de son caractère d'organisation en réseau très étendu, de sa reconversion partielle vers l'espionnage industriel et de la participation d'un Etat membre de l'Union européenne, n'était pas sans poser de questions pour la sécurité du pays et la politique de défense, en particulier au moment où une politique européenne commune de sécurité et de défense était instituée.

Il a alors proposé la nomination d'un rapporteur d'information sur « les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale » en associant aux activités de ce rapporteur un groupe de travail dans lequel chaque groupe politique désignerait un représentant.

A l'unanimité, la Commission a accepté cette proposition et nommé M. Arthur Paecht rapporteur de la mission d'information sur « les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale ».

3.4. L'intérêt du Congrès américain.

Dans son rapport de 1999, le Comité R avait signalé qu'une disposition de l'*Intelligence Authorisation Act for Fiscal Year 2000* requérait que le *Director of Central Intelligence,* le *Director of the National Security,* et l'*Attorney General* présentent aux commissions parlementaires, dans les soixantes jours suivant la promulgation de cette loi, un rapport dans deux versions (classifiée et non classifiée), *« describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance »*.

Selon l'édition du 26 août 1999 du périodique français « le Monde du Renseignement » cette disposition traduisait les craintes du Congrès américain que les droits constitutionnels des citoyens américains soient atteints par le réseau «Echelon ».

Le Comité R a tenté d'obtenir la version non classifiée de ce rapport. A ce jour, seule la version classifiée semble avoir été déposée au Congrès américain. Le Comité R n'a donc pas encore été en mesure de prendre connaissance du contenu du document non classifié, mais il ne manquera pas de suivre l'évolution de ce dossier au sein du Congrès américain.

3.5. L'intérêt du Parlement britannique.

Outre les questions parlementaires citées dans le rapport des experts (cf. point 1.2 de leur rapport), le Comité permanent R a pris connaissance du rapport annuel de l' « Intelligence and security committee »[(3)] déposé par le Premier ministre devant le Parlement britannique le 25 novembre 1999.

Ce rapport indique les quatre priorités actuelles des services de renseignement du Royaume Uni, à savoir :

- le renseignement comme appui aux missions de maintien de la paix des forces armées ;
- la prolifération des armes de destruction massive,
- les attaques terroristes et la croissance du crime organisé.
- le rapport souligne également…la menace croissante de l'espionnage économique.

Le « Committee » consacre une section de son rapport au fonctionnement du GCHQ (General Communication Headquarter), qui serait, d'après le rapport Campbell, le service opérationnel britannique participant au réseau « Echelon ». Il est signalé que le GCHQ a joué un rôle significatif dans la lutte contre le crime organisé et qu'il a fourni des renseignements en appui des missions de maintien de la paix des forces armées. Ces renseignements ont été adressés au gouvernement, à des commandements militaires alliés et à celui de l'OTAN. Le « Committee » appelle à une plus grande rigueur budgétaire de la part du GCHQ.

Il n'est pas sans intérêt de souligner qu'à propos de la cryptographie, le « Committee » approuve la volonté du gouvernement de légiférer en matière de commerce électronique et de cryptographie afin, notamment, d'ordonner la production de clés permettant le déchiffrement de messages.

(3) « The Intelligence and Security Committee » institué par « the Intelligence Services Act 1994 » exerce le contrôle parlementaire des services de renseignement britanniques ; voir rapport d'activités du Comité R pour l'année 1998, p. 29.

Le rapport du « Committee » (dont la présentation de certains passages indique toutefois qu'une partie du contenu n'est pas rendue publique) ne fait aucune mention de l'existence d'un système « Echelon » qui serait orienté vers des opérations d'espionnage économique.

4. LE POINT DE LA QUESTION SUR LES EVENTUELLES INITIATIVES ENTREPRISES PAR LES SERVICES DE RENSEIGNEMENT DEPUIS LA CLÔTURE DU RAPPORT D'ENQUÊTE PRÉCÉDENT, LE 5 AOÛT 1999.

4.1. L'audition de Madame Timmermans, administrateur général a.i. de la Sûreté de l'Etat.

Le jeudi 2 mars 2000, les membres du Comité R ont entendu Madame Timmermans, administrateur général a.i. de la Sûreté de l'Etat. Celle-ci a apporté quelques précisions à ses déclarations par courrier du 6 mars 2000. Le présent compte-rendu tient compte de ces précisions.

Le Comité R a demandé si, depuis le dépôt du premier rapport du Comité en 1999, la Sûreté de l'Etat avait cherché à s'informer davantage sur le système « Echelon » .

Madame Timmermans a répondu par la négative. Elle ne peut que confirmer ce que le précédent administrateur de la Sûreté de l'Etat avait déclaré au Comité R à l'époque de la première enquête, à savoir :

- que la Sûreté de l'Etat ne connaissait l'existence du système « Echelon » que par le biais de divers articles de presse. Les quelques démarches informelles d'information qu'elle a entreprises depuis lors auprès de ses correspondants étrangers n'avaient pas été contributives;

- que la protection du potentiel économique et scientifique, cible supposée du système « Echelon », n'entrait pas à l'époque dans les missions attribuées à la Sûreté de l'Etat;

- que ce service manquait toujours de moyens, tant en personnel qu'en matériel, pour pouvoir vérifier la réalité de l'existence du système « Echelon », aucun agent de la Sûreté de l'Etat ne disposant des compétences techniques nécessaires pour analyser cette menace;

- que la Sûreté de l'Etat ne procédait pas au recueil de renseignements par satellites et qu'elle n'avait aucun accès à ce type de source d'information;

- que la Sûreté de l'Etat ne disposait d'ailleurs d'aucune possibilité légale de procéder à des interceptions de communications et donc à des écoutes via des satellites; cette situation étant d'ailleurs préjudiciable à la Sûreté de l'Etat dans ses rapports avec des services étrangers qui, eux, disposent d'une telle capacité;

- que l'existence du système « Echelon » lui était par conséquent impossible à démontrer;

- qu'à part la communication des éléments précités au ministre de la Justice en vue de lui permettre de répondre à des interpellations parlementaires, la Sûreté de l'Etat n'a jamais produit aucun rapport ni aucune note sur le système « Echelon ».

Madame Timmermans a confirmé également que la Sûreté de l'Etat n'avait jamais entretenu jusqu'alors aucune discussion à ce sujet avec le Service Général du Renseignement et de la Sécurité des Forces armées, ni d'ailleurs avec aucun autre service de renseignement européen. Madame Timmermans s'engage cependant, vu les développements récents concernant Echelon, à interroger les services correspondants étrangers sur l'existence du système « Echelon ».

En ce qui concerne les objectifs économiques que viserait le système « Echelon », Madame Timmermans a précisé que son service n'avait pas encore reçu d'instructions du Comité ministériel du Renseignement en matière de protection du potentiel scientifique et économique.

La Sûreté de l'Etat formulera des propositions à soumettre au Comité ministériel du renseignement.

A ce jour, deux agents seulement travaillent sur ce sujet au sein de la Sûreté de l'Etat.

Cette matière apparaît par ailleurs comme relevant de la défense d'intérêts strictement nationaux. Selon Madame Timmermans, il n'existe donc aucun échange d'information de quelque nature que ce soit entre services de renseignement européens où le cloisonnement reste la règle dans ce domaine.

Interrogée sur la connaissance éventuelle par la Sûreté de l'Etat de l'existence « d'Opidium », Madame Timmermans a déclaré que rien ne lui était connu de plus que ce qu'en disent les sources ouvertes. Elle pense toutefois qu'il faudrait considérer l'existence d'un tel système comme une réponse aux pratiques américaines.

Madame Timmermans a aussi déclaré que, contrairement au SGR, la Sûreté de l'Etat n'avait aucune compétence technique ou légale pour s'occuper de problèmes de sécurité des communications.

Interrogée sur la possibilité de mettre en oeuvre à l'avenir des moyens de recherche tels que l'exploitation en commun des sources ouvertes avec le SGR ou le recours à des experts en vue de missions ponctuelles, Madame Timmermans s'est montrée réservée. En matière d'experts, la seule alternative qui soit ouverte à la Sûreté de l'Etat consiste soit à recruter de nouveaux agents statutaires, soit à engager des agents contractuels de niveau I. Mais les recrutements sont toujours soumis aux contraintes budgétaires, et notamment à l'avis de l'inspecteur des finances : une extension de 25 unités pour les services extérieurs demandée dans le cadre du contrôle budgétaire a récemment été refusée.

Concernant les rencontres ILETS **(**International Law Enforcement Telecommunications Seminar) dont il est aussi question dans le rapport STOA, Madame Timmermans confirme qu'un commissaire divisionnaire de la Sûreté de l'Etat a bien participé à quelques unes de ces réunions organisées depuis 1997 à l'initiative du FBI américain. Assistaient également à ces réunions, des représentants de la Gendarmerie, du SGAP, ainsi qu'un représentant du cabinet du ministre de la Justice. L'objet de ces rencontres était l'harmonisation des standards d'écoutes européens et américains.

4.2. L'audition du Général major Michaux, chef du SGR .

Les membres du Comité R ont entendu le général-major Michaux, chef du SGR le vendredi 3 mars 2000.

Le président du Comité a demandé au général Michaux si, depuis le dépôt du rapport du Comité R en 1999, le SGR a cherché à s'informer davantage sur le sujet.

Le général Michaux répond que le SGR ne suit pas le système « Echelon ». En effet, la menace engendrée par « Echelon » se situe principalement au niveau de l'ordre économique, politique et juridique, matières qui sortent des attributions du SGR. S'agirait-il même d'un système d'espionnage militaire, qui lui relève de la compétence du SGR, ce service n'a pas pour priorité de suivre l'espionnage émanant des alliés de la Belgique. En cette matière, d'autres pays poursuivent des activités bien plus menaçantes pour les intérêts militaires belges.

Le SGR ne dispose pas des moyens techniques et humains nécessaires pour déceler l'existence du réseau « Echelon ». Pour le général Michaux, suivre un système technique comme « Echelon » serait d'ailleurs illégal en Belgique vu l'absence de législation dans notre pays sur les écoutes de sécurité.

Cela ne signifie pas que le SGR reste inactif en la matière.

Le SGR travaille avec l'hypothèse que les interceptions de communications existent réellement, et, quelque soit le pays qui les pratique, qu'il faut s'en prémunir. Le SGR considère également que n'importe quel système de chiffrement informatique est susceptible d'être cassé.

Etant chargé de la sécurité des communications des forces armées, le SGR a élaboré différentes règles destinées à assurer la confidentialité des données classifiées transmises par télécommunication ou traitées par des réseaux informatiques.

Le SGR a également pris l'initiative de porter le sujet de la sécurité informatique et de la cryptologie à l'ordre du jour du Collège du Renseignement et de la Sécurité. Ce collège a désigné des experts chargés de déposer un rapport au Comité ministériel du Renseignement et de la Sécurité.

Le SGR a formulé aux membres du Collège du Renseignement et de la Sécurité la proposition de créer une agence fédérale pour la protection de l'information, chargée de la politique du chiffrement en Belgique.
Cette proposition est encore à l'étude à ce jour.

Pour sa part, le SGR est favorable à l'idée de créer une agence fédérale pour la protection de l'information ou de charger un organisme existant de mener cette politique du chiffrement en Belgique. La Belgique compte d'ailleurs d'éminents spécialistes de la cryptographie.

Le SGR suit de très près le développement de la législation en matière de cryptographie en Belgique. Le problème de la cryptographie est cependant très complexe vu qu'il se situe au croisement de plusieurs intérêts divergents :

- les intérêts économiques en jeu sont énormes : pour pouvoir se développer, le commerce par l'Internet a besoin d'être sûr, il nécessite donc un système de chiffrement fort ;

- les organisations criminelles utilisent aussi abondamment l'Internet : elles aussi ont besoin d'un système de chiffrement fort ;

- de nombreuses entreprises développent des systèmes de cryptographie qu'elles souhaitent mettre librement sur le marché ;

- par contre, les services de police et de renseignement n'ont pas d'intérêt à la diffusion de systèmes de chiffrement forts .

Ces intérêts divergents donnent lieu aux Etats-Unis à de fortes luttes d'influence entre la NSA et le lobby des utilisateurs de l'Internet.

Le Comité R demande au général Michaux si le SGR considère la menace « Echelon » comme plausible et s'il a connaissance de l'existence d'autres réseaux d'écoutes étrangers (russes, français, suisses, etc.…).

Le général Michaux répond qu'il n'a pas connaissance de l'existence de réseaux d'interceptions autrement que par les sources ouvertes, dans lesquelles on trouve de l'information mais aussi de la désinformation. Le SGR considère la menace venant des grands pays comme plausible et il applique donc le principe de précaution.

Le président demande si des informations s'échangent entre le SGR et la Sûreté de l'Etat et d'une manière plus générale entre les services de renseignement européens au sujet d'Echelon ou bien au sujet de l'espionnage économique.

Le général Michaux répond qu'il n'existe pas de guerre de l'information entre les deux services de renseignements belges. Tout ce que le SGR apprend d'intéressant pour la Sûreté de l'Etat est communiqué à ce service.

Avant de proposer la création d'une agence fédérale de protection de l'information au Collège du Renseignement, le prédécesseur de l'actuel chef du SGR en avait fait part à l'administrateur général de la Sûreté de l'Etat. Des réunions périodiques ont eu lieu entre les informaticiens des deux services.

A ce propos, le général Michaux souligne le caractère peu attractif du statut financier offert aux informaticiens des forces armées et à ceux de la fonction publique en général. Les salaires offerts par les firmes privées sont bien plus avantageux et certains informaticiens quittent les forces armées pour des motifs financiers évidents. La mise en place du système informatique du SGR en subit les conséquences.

Le général Michaux signale d'autre part que depuis les travaux de la commission Rwanda, le SGR a intensifié ses rapports bilatéraux avec d'autres services de renseignement militaires ou extérieurs des pays européens. Ces services procèdent à des échanges quotidiens sur des questions d'intérêt commun, mais jamais ils ne parlent d'espionnage économique. Bien sûr, tout ne s'échange pas ; on garde certaines informations pour soi en fonction de ses intérêts nationaux propres. Une règle est aussi de ne rien dire de ses contacts avec des services tiers. S'il n'est pas facile de construire une armée européenne, il sera encore plus difficile de construire un service commun européen de renseignement .

Il faut enfin regretter que, les secteurs de l'armement ou lié à la Défense nationale mis à part, les autres entreprises belges soient très peu sensibilisées à l'Intelligence économique.

Le général Michaux ne connaît personne qui, par sa profession ou son appartenance passée à un service de renseignement, aurait acquis une connaissance personnelle et directe du système « Echelon ». Il convient de se méfier par ailleurs des « révélations » que de soi-disant anciens membres des services de renseignement font à la presse. Il convient de toujours examiner ces déclarations à la lumière des circonstances qui ont présidé au départ de ces personnes de leur service.

Interrogé sur les rencontres ILETS, le général Michaux déclare que le SGR ne participe pas à ces réunions.

Le président demande si le SGR envisage d'avoir recours à des spécialistes ou a des experts extérieurs dans les matières où il ne dispose pas de personnel compétent. Le général Michaux répond que le SGR y a déjà songé et qu'il envisage favorablement cette possibilité pour des collaborations ponctuelles. En attendant, le SGR a récemment recruté de nouveaux analystes qui sont actuellement en phase de formation. A cet égard, le SGR fournit actuellement un surcroît d'efforts pour former ces analystes.

5. LE RAPPORT DES EXPERTS DESIGNES PAR LE COMITE PERMANENT R

Le Comité a estimé, vu l'ampleur de la problématique posée par le réseau « Echelon » et l'urgence d'en poursuivre une approche dynamique, de ne pas se contenter d'élaborer une synthèse des informations les plus récentes parues dans ce domaine dans les sources ouvertes de diverses origines, mais de demander à des experts d'en faire une analyse critique permettant e.a. de faire la distinction entre information et désinformation, et de préciser sur des bases objectives la probabilité d'une menace globale dont le système « Echelon » ne serait qu'une manifestation exemplative.

Interpellé par les problèmes rencontrés par nos services de renseignement et pour tenter de proposer des solutions alternatives au manque de moyens auxquels ils se trouvent confrontés, le Comité R a également voulu mettre en évidence et en pratique la possibilité de recourir à des experts issus du monde universitaire.

Comme dit plus haut, le Comité a fondé son initiative d'une part sur les possibilités que lui donne la loi organique du contrôle des services de police et de renseignement du 18 juillet 1991 (article 48 §3) de faire appel à des experts et d'autre part sur sa double mission de contrôle de la coordination et de l'efficacité des services de renseignements et de sécurité et de la protection des droits que la Constitution et la loi confèrent aux personnes.

Le Comité R a également demandé aux experts de faire des recommandations permettant notamment d'envisager les moyens à mettre en œuvre et les éventuelles mesures à prendre pour répondre à ce type de menace.

Les missions que le Comité permanent R a confié aux experts se trouvent reprises dans le corps du rapport déposé le 7 mars 2000 et dont le contenu est intégralement reproduit ci-après.

Le réseau Echelon

Existe-t-il ?

Que peut-il faire ?

Peut-on et doit-on s'en protéger ?

Rapport d'expertise rédigé
à l'attention du Comité Permanent de contrôle des services de renseignements

le 7 mars 2000

Par
Yves Poullet (yves.poullet@fundp.ac.be)
Docteur en Droit
Professeur et Directeur du Centre de Recherche Informatique et Droit (FUNDP)
&
Jean-Marc Dinant (jmdinant@fundp.ac.be)
Maître et doctorant en Informatique
Chargé de recherche au Centre de Recherche Informatique et Droit de l'Université de Namur

Les auteurs s'expriment ici à titre personnel et n'engagent aucune institution

Introduction

Le 23 février 2000, le comité permanent de contrôle des services de renseignements a confié aux experts signataires les missions suivantes :

1. *examiner, analyser et commenter tous les documents disponibles issus de sources ouvertes qui traitent de l'existence du réseau Echelon destiné à intercepter des communications, notamment à des fins économiques ;*

2. *évaluer la fiabilité de ces documents et la vraisemblance de ces hypothèses, notamment en la confrontant à l'avis des opérateurs de télécommunications ;*

3. *situer l'existence possible du réseau Echelon dans un contexte élargi de mise en œuvre au niveau international de technologies de surveillance ;*

4. *dans la mesure du possible, établir une description des technologies utilisées et préciser la nature des messages interceptés ;*

5. *décrire l'environnement juridique en la matière ;*

6. *formuler, le cas échéant, des recommandations.*

Le présent rapport reprend ces différents points, en tire les conclusions et formule certaines recommandations. Les auteurs tiennent à souligner que ce document a du être rédigé dans des délais extrêmement brefs. Les éléments décrits dans ce rapport l'ont néanmoins été avec toute la rigueur scientifique possible mais certaines analyses n'ont pu être menées de manière aussi approfondie qu'il eût fallu. C'est en particulier le cas pour l'analyse de l'importance et de la nature des télécommunications potentiellement vulnérables à l'interception par le réseau Echelon.

1. ANALYSE DES DOCUMENTS ISSUS DE SOURCES OUVERTES

1.1. Les rapports du STOA

Le premier rapport du STOA a été publié en 1998 et a déjà, à l'époque, suscité de nombreuses réactions, dont une recommandation du parlement européen. Seulement deux pages (19-20) de ce premier rapport décrivent le réseau échelon en se basant sur trois sources distinctes :

- les travaux de Duncan Campbell menés dans les années 70 ;
- le livre "the Puzzle Palace" de James Bamford ;
- le livre "the Secret Power" de Nicky Hager.

Ce dernier ouvrage est celui qui détaille le mieux le réseau Echelon, énumère ses bases dans le monde entier et explique que ce réseau espionne les satellites Intelsat utilisés pour convoyer la majorité des communications satellitaires mondiales de type téléphone, fax, télex, Internet (dont les courriers électroniques).

Il serait donc erroné, bien que cela ait été souvent écrit dans la presse, de prétendre que ce réseau peut capter tous les appels téléphoniques effectués en Europe. Ce réseau serait principalement capable de capter tous les messages transitant par les satellites Intelsat.

Ce premier rapport fait état d'un document du 25 octobre 1995 qui resterait toujours secret. Le groupe de travail 29[(1)] a émis le 8 mai 1999 une recommandation concernant le respect de la vie privée lors de l'interception des télécommunications[(2)]. Cette recommandation confirme l'existence de ce document classifié.

"*Les préoccupations du groupe de travail portent également sur le champ d'application des mesures prévues par la résolution du Conseil du 17 janvier 1995[(3)]. Une version non publiée du document précité et postérieure à celui-ci (en date du 25 octobre 1995), prévoit que les signataires du texte pourront prendre contact en ce qui concerne les spécifications en matière d'interception des télécommunications avec le directeur du « Federal Bureau of Investigation » des Etats-Unis. Le texte prévoit également que, sous réserve du consentement des « participants », d'autres Etats peuvent participer à l'échange d'informations, à la révision et à la mise à jour des spécifications. Le groupe s'inquiète du fait que des mesures techniques d'interception des télécommunications soient mises au point en concertation avec des Etats non soumis aux exigences de la convention européenne des droits de l'homme et des directives 95/46 et 97/66.* »

Le deuxième rapport du STOA, publié au début de l'an 2000, est plus fouillé et est divisé en deux parties.

La première partie, assez technique, présente quatre études :

- *L'état de l'art dans la surveillance des communications* (par Duncan Campbell)

- *Chiffrement, cryptosystèmes et surveillance électronique* (par F. Leprévost, professeur à l'université technique de Berlin)

- *La légalité des interceptions des communications électroniques* (par Chris Elliott, juriste et ingénieur spécialisé dans les télécommunications)

- *La perception des risques économiques dérivés de la vulnérabilité potentielle des médias commerciaux par rapport aux interceptions* (Cabinet d'Etudes ZEUS, entouré de l'avis de 49 experts en technologies de la télécommunication).

La deuxième partie, plus juridique, analyse la protection des données et les droits de l'homme dans l'Union Européenne et le rôle du parlement européen.
Au niveau technique, les éléments décrits dans la première partie sont exposés avec soin et précision et l'ensemble du travail a été réalisé de manière professionnelle. Suite à l'audition par le Parlement Européen de l'auteur Duncan Campbell, aucune critique sérieuse de ce rapport n'a d'ailleurs été formulée, même si l'auteur est en défaut d'apporter des preuves formelles de tous les éléments de son rapport. Certains éléments de son rapport sont d'ailleurs basés sur des coupures de presse. En dehors de ce rapport, d'autres éléments apportent des preuves de l'existence du réseau Echelon.

---

(1) Ci-après dénommé Groupe 29. Ce groupe est créé par l'article 29 de la Directive 95/46 et regroupe l'ensemble des commissions nationales de protection des données de l'Union Européenne.

(2) disponible sur le serveur de l'Union Européenne http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp18fr.pdf

(3) J.O. C329 du 14 novembre 1996

1.2. Les questions parlementaires au Royaume-Uni

L'existence de la base anglaise de Menwith Hill, considérée comme le nœud du réseau Echelon au cœur de l'Europe, peut être établie par plusieurs questions parlementaires à la Chambre des Lords du Royaume-Uni, telles que publiées sur le site officiel du parlement britannique[(4)].

Ci-dessous figure la traduction de quelques questions et de leurs réponses.

29 Mars 1994, Brian Sedgemore : « *Mon honorable ami a mentionné la station de Menwith Hill. Je crois qu'il s'agit d'une station du GCHQ. Mon honorable ami peut-il expliquer pourquoi les Chemins de Fer Britanniques veulent l'imposer sur base de sa valeur imposable ? »*

Réponse : « …*Menwith Hill est une station d'écoute et d'espionnage … située sur 125 hectares de terrain, avec 21 radomes ».*

25 Mars 1994, Mr Cryer *: « Quels droits les individus ou les firmes possèdent-ils s'ils croient être espionnés par Menwith Hill ? Par exemple, le Ministre peut-il nous donner l'assurance formelle que Menwith Hill n'intercepte pas le trafic commercial ? …Finalement, si le Ministre est tellement confiant dans la démocratie, m'autorisera-t-il, moi et d'autres membres du parti travailliste à visiter la base ? »*

Réponse : « …*Comme la Chambre le sait, j'ai visité la station le 27 janvier. J'ai reçu des briefings concernant son rôle actuel de la part du personnel senior américain et anglais travaillant là-bas, celui-ci incluant le chef de la base… Le travail effectué là-bas est très sensible et classifié secret. Je crois très fermement que si je commentais en détail les activités que j'ai vu menées là-bas, cela ne serait pas dans l'intérêt national et nuirait en tout cas à l'objectif véritable de ce travail… Il y a actuellement 600 employés britanniques servant à chaque niveau de la base et 1200 employés américains. L'honorable Membre pour Bradford Sud a mentionné des visites de Menwith Hill par des membres du Parlement et des Membres du Parlement Européen. Des demandes antérieures pour de telles visites ou conférences n'ont pas été approuvées sur base des dérangements [que cela causerait] dans le fonctionnement opérationnel de la base et pour des raisons de sécurité. J'ai déclaré qu'il en serait de même tant pour les membres du parti conservateur que pour les membres du parti travailliste. Il n'entre pas dans la pratique du Ministère de la Défense d'organiser des visites guidées des installations de travail de Menwith Hill. Dans ma réponse à la Chambre le 8 mars, j'ai dit que ces restrictions s'appliqueraient à tous [les parlementaires]. »*

Le 3 juin 1996, Lord Jenkins of Putney: « *Des interceptions de télécommunications sont-elles effectuées par la NSA américaine à Menwith Hill ? Et, dans l'affirmative, quels messages sont interceptés et pour quelle finalité ? »*

Réponse *: « Il n'entre pas dans la politique du gouvernement de commenter les opérations détaillées menées à Menwith Hill. En tous cas, aucune activité considérée comme hostile aux intérêts britanniques n'est, -ou ne serait-, permise dans cette station. »*

(4) En annexe se trouvent les questions et réponses originales en Anglais, telles qu'imprimées à partir d'Internet

Le 6 avril 1998, Norman Baker: « *Quel mécanisme est en place pour garantir que l'information glanée des interceptions des télécommunications par les forces américaines à Menwith Hill n'est pas utilisée de manière préjudiciable aux intérêts du Royaume-Uni ? »*

Réponse du Ministre des Forces Armées : « *Du personnel anglais est intégré à chaque niveau de Menwith Hill et nous pouvons donc être confiant dans le fait qu'aucune activité préjudiciable aux intérêts du Royaume-Uni ne se déroule là-bas. »*

Mr Baker : « *Le Ministre [des forces armées] peut-il confirmer la véracité ou d'autres aspects des éléments contenus dans le rapport préparé pour le Parlement Européen « Assessing the Technologies of Political Control » qui suggère que toutes les communications téléphoniques, fax et courriers électroniques à travers l'Europe sont couramment surveillées par les forces américaines basées à Menwith Hill ? Etant donné qu'une telle activité se développe à toute vitesse et étant donné que la guerre froide est terminée, est-il raisonnable de supposer que cela est réalisé à des fins non militaires ? Le Ministre peut-il confirmer que le gouvernement anglais a accès à toutes les interceptions à Menwith Hill ? S'il ne le peut, comment peut-il donner l'assurance qu'il vient de donner ? »*

Réponse de John Reid, Ministre des Forces Armées : « *L'honorable gentleman ne devrait pas s'attendre à ce que ce que je commente un rapport que je n'ai jamais vu et dont je n'ai entendu que très peu de garanties eu égard à sa véracité. Menwith Hill est une installation de communications et il y a là-bas une intégration totale entre le personnel américain et anglais.*
En cette matière, il y a un droit de regard par le parlement mais aussi par le biais du comité « Intelligence and Security » et notamment par l'honorable gentleman. Parmi les milliers de questions qu'il a déposées depuis qu'il est entré au Parlement – à £600 livres par question-, plus d'une vingtaine sur ce sujet ont déjà reçu mon attention personnelle. »

Le 9 mars 1999, Lord Kennet : « *Quand, pour la dernière fois, un Ministre a-t-il été à Menwith Hill, la base américaine située dans le Royaume-Uni ? Combien de temps y est-il resté ? A-t-il pu voir et comprendre toutes les activités menées là-bas par le personnel des Etats-Unis ? »*

Réponse *: « Depuis le premier mai 1997, aucun Ministre de notre administration n'a visité Menwith Hill. Toutefois, les Ministres concernés restent tenus informés de toutes ses activités.*

Question : « *S'ils [les ministres concernés] surveillent les activités qu'ils permettent aux Etats-Unis de mener à Menwith Hill, y compris les activités de maintien de l'ordre menées par le personnel américain afin de s'assurer qu'elles ne compromettent pas les droits et intérêts, commerciaux, sociaux ou autres, des citoyens et entreprises du Royaume-Uni et de l'Union Européenne »*

Réponse : « *Le gouvernement de Sa Majesté est conscient des activités menées par le personnel américain à Menwith Hill. Le maintien de l'ordre à la station RAF de Menwith Hill est assuré par la police du Ministère de la Défense »*

1.3. Les documents déclassifiés par la NSA

Le rapport STOA fait état de documents déclassifiés sur base du “Freedom of Information Act ”[5]. La lecture de ces documents (dont certaines parties sont illisibles ou censurées) reste sibylline mais le nom “Echelon” y apparaît et ces documents confirment donc l’existence de ce réseau même s’ils n’apportent que peu de renseignements relatifs à son fonctionnement.

2. ANALYSE DE LA VRAISEMBLANCE DES HYPOTHÈSES AVANCÉES PAR LE STOA

2.1. Quelques éléments concernant la National Security Agency

Il est intéressant de noter, sur le site de la NSA lui-même, l’idéologie affichée de ce service

- « la menace par rapport à nos systèmes d’information grandira dans les années futures au fur et à mesure que les technologies permettant l’attaque de ces systèmes prolifèreront et que de plus en plus de pays et de groupes développeront des stratégies incluant de telles attaques »[6] .

- « Ces pages décrivent le plan stratégique de la NSA/(CSS) pour le 21ème siècle et comment nous comptons atteindre notre but : la supériorité américaine en matière d’information»[7].

Selon plusieurs sources convergentes, la NSA posséderait un personnel d’environ quarante mille personnes et un budget de l’équivalent de 160 milliards de francs belges en 1997. A titre de comparaison, un géant industriel comme Belgacom a dépensé la même année 131 milliards de francs belges et son personnel comptait environ vingt six mille personnes[8].

Les capacités de décryptage de la NSA sont importantes quoique non connues avec certitude et donc sujettes à spéculation. A titre d’illustration, le système DES 56 bits recommandé par le gouvernement américain pour chiffrer les documents gouvernementaux non classifiés a été présenté en 1998 par les services américains comme impossible à casser sans utiliser 14.000 PC Pentium pendant 4 mois. Quelques mois après cette déclaration, l’Electronic Frontier Fundation a réalisé une machine effectuant ce cassage de la clé 56 bits en moins de deux jours[9].

---

(5) Le Freedom of Information Act de 1966 (5 USC, section 552) est la loi américaine obligeant les Administrations à la transparence et créant au profit des citoyens un droit d'accès aux documents détenus par l'Administration.

(6) http://www.nsa.gov:8080/programs/ncs21/goal1.html

(7) http://www.nsa.gov:8080/programs/ncs21/index.html

(8) Source : rapport annuel de Belgacom 1998

(9) http://www.eff.org/pub/Privacy/Crypto-misc/DESCracker/HTML/19980716-eff-descracker-pressrel.html

Le coût d'une telle machine s'élève à huit millions de FB. On peut difficilement croire qu'une organisation possédant depuis plusieurs années des capacités en personnel et en budget supérieures à celles de notre opérateur national de télécommunications n'ait jamais pu réaliser une telle machine voire une machine nettement plus performante que celle réalisée par des amateurs avec des moyens et un budget ridicules.

Par ailleurs, il est intéressant de noter[10] que cet algorithme, conçu à l'origine par IBM était doté d'une clé de 128 bits.

Il est donc évident que les capacités de décryptage de la NSA sont énormes et que les déclarations publiques américaines concernant cette capacité tendent volontairement à la minimiser d'un facteur énorme.

2.2. Que fait le réseau Echelon ?

Il nous est impossible de répondre à cette question de manière certaine.

James Bamford, auteur du livre « The Puzzle Palace » a pour sa part déclaré[11] : « En tant que l'une des rares personnes extérieures à avoir suivi l'agence (la NSA) pendant des années, je pense que les craintes sont fort exagérées. Me basant sur tout ce que je sais de l'agence, et sur d'innombrables conversations que j'ai eues avec des membres actuels ou anciens de la NSA, je suis certain que la NSA n' outrepasse pas son mandat. Mais cela ne signifie pas qu'elle ne le fera jamais. Mon véritable souci est que les technologies qu' elle développe à huis clos, ainsi que les méthodes qui ont éveillé de telles craintes, ont donné à l'agence la capacité d'étendre son réseau d'écoutes de manière presque illimitée. Alors que la NSA fonce dans le développement de satellites et d' ordinateurs assez puissants pour passer au crible des montagnes de données interceptées, les lois fédérales (à présent vieilles d'un quart de siècle) qui régissent l'agence n'en sont encore qu'à leurs prémices ».

Néanmoins, il est certain que ce réseau, -et en particulier la station de Menwith Hill dans le Yorkshire anglais, près d'Harrogate-, existe et possède des moyens importants d'écoute de tout le trafic satellitaire reçu sur le territoire de l'Union Européenne.

Au niveau technique, un satellite n'est rien d'autre qu'un ensemble de plusieurs transpondeurs qui, recevant une onde radio de la terre, la renvoient dans un certain faisceau. En général, les faisceaux d'onde descendant vers la terre ne sont pas focalisés vers un lieu précis (une ville voire un pays entier) mais englobent plusieurs pays.

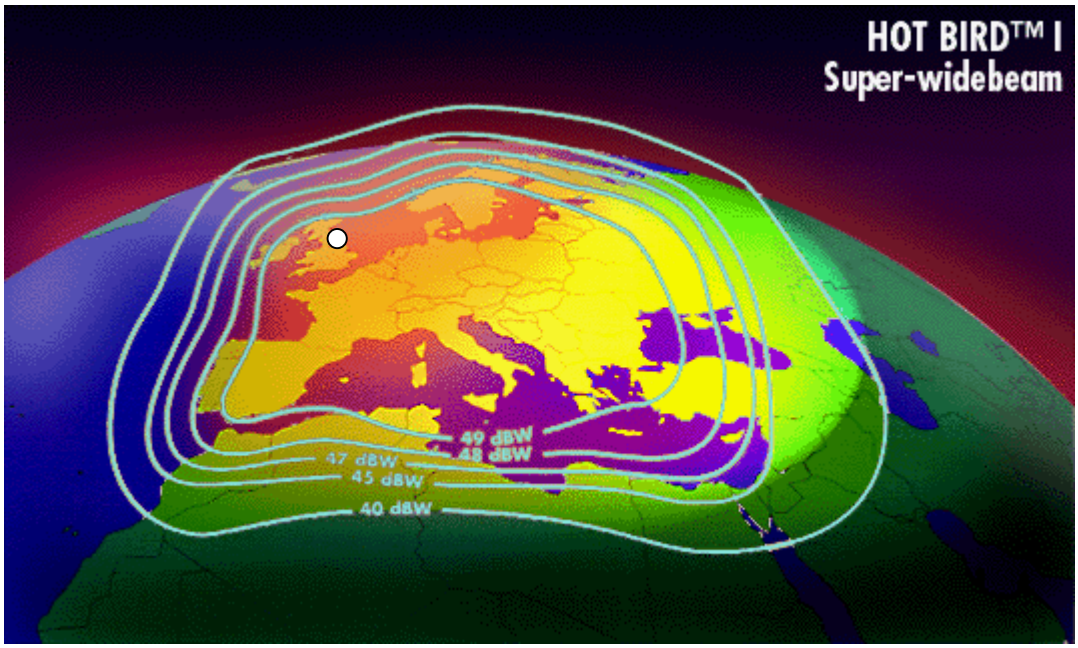
---

(10) Chaque bit ajouté à une clé multiplie par deux le nombre de clés possibles et donc le temps nécessaire pour trouver la bonne clé. Une clé 128 bits est donc environ quatre mille milliards de milliards de fois plus sûre qu'une clé à 56 bits. C'est à la demande de la NSA que l'algorithme DES a vu sa longueur de clé réduite à 56 bits au lieu des 128 prévus initialement. (Voir à ce sujet Bruce Schneier, *Cryptographie appliquée*, International Thomson Publishing France, Paris, 1997, p. 283)

(11) James Bamford, *« Loud and Clear – the most secret of secret agencies operates under outdated laws », Washington Post, 14 novembre 1999.*

Les faisceaux satellitaires descendant des réseaux Intelsat (téléphonie et fax principalement) et Eutelsat (connexions Internet point à point ou multipoint fournies par Belgacom) montrent que Menwith Hill est judicieusement positionnée pour capter le maximum de satellites. A titre d'exemple nous montrons le faisceau descendant d'un satellite utilisé par Belgacom pour le trafic Internet.

Il semble certain que la quasi totalité des informations transitant par Intelsat ou Eurosat viennent frapper l'une des 23 (Duncan Campbell parle de 26) antennes situées à Menwith Hill. La position de ces antennes est masquée par l'utilisation de radomes (sphères opaques perméables aux ondes électromagnétiques), ce qui interdit de pouvoir vérifier leur orientation.



2.3. Les avis des experts européens en la matière.

Les auteurs du présent rapport font leurs les conclusions des trente experts européens de tous pays, de tout âge et de tous secteurs interrogés dans le cadre du 4ème rapport du STOA et en particulier les trois assertions suivantes qui ont récolté l'assentiment quasi unanime des personnes interrogées, à savoir :

1. Jusqu'à présent toute l'information économique est échangée par le biais de moyens électroniques (téléphone, téléfax, courrier électronique). Tous les appareils informatiques et les commutateurs offrent des possibilités croissantes d'écoute. En conclusion, nous devons considérer la protection de la vie privée dans un environnement de réseaux internationaux.

2. L'importance des systèmes d'information et de communication pour la société et l'économie globale s'intensifie parallèlement à la quantité et à la valeur croissante des données qui sont stockées ou transmises dans ces systèmes. Simultanément, ces systèmes et ces données deviennent de plus en plus vulnérables face à des menaces variées comme l'accès ou l'usage non autorisé, la mésappropriation, l'altération et la destruction.

3. La cryptographie est un composant essentiel de la sécurité de l'information ainsi que des systèmes de communication et des applications incorporant des méthodes cryptographiques pour assurer la sécurité des données ont été développées.

En résumant, nous pourrions dire que l'informatisation croissante de tous les secteurs fait que :

1. chaque activité humaine laisse de plus en plus de traces ;

2. le détenteur, la nature et le lieu de stockage de ces traces deviennent de moins en moins visibles par l'individu qui les laisse le plus souvent malgré lui ;

3. dans le même temps, la captation de ces traces invisibles laisse de moins en moins de traces visibles.

En d'autres termes, l'individu communiquant a conscience de laisser de plus en plus de traces mais sans pouvoir les identifier avec précision et sans connaître leurs destinataires réels. Ceci se manifeste par la réponse à la question 18 de l'étude précitée. Face à l'assertion *« Il est largement évident que les grands gouvernements utilisent la surveillance des communications pour procurer des avantages commerciaux aux entreprises et organisations* », 40% des experts interrogés en sont persuadés, 30% sont persuadés du contraire et les 30% restants ne peuvent pas se prononcer. Il est probable que cette répartition d'opinion en trois tiers se retrouvera parmi le grand public et parmi…les lecteurs de ce rapport.

2.4. L'avis de Belgacom

Selon l'avis de plusieurs ingénieurs de Belgacom, le trafic Intelsat (principalement fax et téléphonie) ne serait pas crypté par l'opérateur. Toutefois, seulement un pourcent du trafic téléphonique International transiterait par satellite, principalement pour assurer la connexion vis-à-vis de pays ne possédant pas une bonne infrastructure filaire terrestre (les exemples de certains pays d'Afrique et de l'Inde ont été cités).
Les liaisons fournies dans le cadre des services V-STAR[(12)], utilisant le réseau Eurosat ne sont pas systématiquement cryptées par l'opérateur mais elles peuvent l'être lorsque Belgacom fournit l'applicatif au client. Par ailleurs le trafic V-link se déroule suivant un protocole propriétaire, propre à Belgacom, ce qui compliquerait le décodage des informations transmises.

Dans tous les cas, l'interception physique de la télécommunication ne pose aucun problème et peut s'effectuer à l'aide d'un équipement limité à une antenne et un décodeur. Dans le cas d'Intelsat, le candidat intercepteur trouvera même sur Internet les programmes permettant de pointer en permanence son antenne vers le satellite désiré.

(12) Les services de communications de données par satellites sont dénommés V-star (http://www.belgacom.be/satellite). Ils englobent les services V-Star pour des liaisons multipoints et V-Link pour des liaisons point à point

Dans le très court délai (12 jours) qui leur a été imparti, les experts n'ont pu faire une analyse plus détaillée des télécommunications internationales et/ou satellitaires effectuées par les opérateurs nationaux. Une telle étude exhaustive nous semble un élément indispensable à une meilleure sécurisation des télécommunications véhiculées sur le territoire belge.

3. ECHELON DANS LE CONTEXTE ÉLARGI DE LA SURVEILLANCE DES TÉLÉCOMMUNICATIONS

Ce point a déjà été esquissé (supra n° 2). Une caractéristique majeure des nouvelles technologies de l'information et de la communication se situe dans les traces que chaque télécommunication laisse, généralement à l'insu de la personne qui communique. C'est un phénomène global et le réseau Echelon n'est qu 'une manifestation de ce qui est possible à partir de la surveillance des satellites.

Hormis les problèmes de confidentialité liés aux êtres humains, la technologie moderne de télécommunication repose sur une chaîne de trois éléments distincts et complémentaires, chacun possédant ses propres vulnérabilités.

1.- le hardware de communication (les routeurs, les circuits intégrés, les processeurs, les antennes, etc.)

2.- le software de communication (le programme qui commande le hardware)

3.- le support de communication (le câble, la fibre optique, l'onde radio, etc.)

3.1. Les vulnérabilités du hardware et du software

Tant le hardware que le software peuvent offrir ce que l'on appelle en sécurité informatique des judas (peep hole), des portes dérobées (backdoors) ou des fonctions cachées (non signalées dans la documentation). Dans tous ces cas de figure, l'utilisateur d'un routeur ou d'un processeur ignore certaines fonctionnalités qui peuvent être utilisées, de manière invisible et de plus en plus souvent à distance par un tiers les connaissant. Le premier rapport du STOA cite ainsi une fonctionnalité des centraux RNIS permettant d'écouter ce qui se dit dans une pièce via un téléphone raccroché.

En juillet 1999, Richard Smith un consultant en sécurité a mis en évidence que RealJukebox, un logiciel gratuit d'écoute de CD musicaux diffusé en Europe à des millions d'exemplaires transmettait à la maison mère américaine, de manière cryptée et à intervalles réguliers les index des CDROM qui étaient insérés dans le lecteur du PC[(13)].

Le même Richard Smith avait détecté, quelques mois auparavant, que le logiciel d'inscription en ligne de Windows 98 transmettait à Microsoft le détail de l'équipement de l'internaute en ce et y compris certains numéros de série.

(13) http://www.thatworld.com/news/realjukebox.html

Dans les versions de Microsoft Office 1997, chaque document Word, Excel ou Powerpoint était marqué d'un numéro de série unique composé en partie du numéro de série de la carte Ethernet de l'ordinateur. Ceci permettait à Microsoft de retrouver l'auteur de n'importe quel document Word, Excel ou Powerpoint 97, pour peu que celui-ci se soit enregistré en ligne.

Grâce à l'utilisation de cookies dans des hyperliens invisibles et au bavardage invisible des programmes de navigation (p.e. Internet Explorer ou Netscape Communicator), implémentés en contradiction avec les normes mondiales, des entreprises inconnues de cybermarketing parviennent à collecter et à stocker sur une base individuelle l'ensemble des mots-clés tapés sur certains grands moteurs de recherches par chaque Internaute européen.

DoubleClick, une entreprise de cybermarketing américaine utilise à elle seule ce procédé plus d'un demi-milliard de fois par jour.

La liste de ce qui se passe sur le réseau Internet à l'insu de l'utilisateur est longue et les quelques cas relevés ci-dessus n'ont valeur que d'exemples non sujets à caution[14].

3.2. La vulnérabilité des supports de communication

En ce qui concerne le support de communication, chaque support rayonne une part de l'information qu'il transporte. Cela est clair pour le satellite qui transmet à l'Europe entière l'information destinée à une antenne particulière dans un pays déterminé. Le courant circulant dans les câbles de télécommunication produit une onde électromagnétique dont une partie se déploie à l'extérieur du câble et peut donc être capturée sans rupture de celui-ci. La fibre optique elle-même laisse passer une quantité infime de lumière. Il est possible de la polir légèrement ou de la courber afin de capturer une partie significative de lumière de façon à pouvoir reconstituer le message. Néanmoins, à ce jour, la fibre optique reste de loin le support le plus difficile à espionner. Par ailleurs, grâce à la cryptographie quantique[15] associée à ce média, il semble qu'il serait possible de détecter automatiquement et systématiquement toute écoute du signal transitant sur une fibre optique, ce qui ferait de la fibre un support non sujet à des écoutes invisibles.

4. DESCRIPTION DES TECHNOLOGIES UTILISÉES ET NATURE DES MESSAGES INTERCEPTÉS

Nous ne pouvons ici que tout d'abord renvoyer aux études de Leprévost et Campbell précitées qui nous paraissent d'un excellent niveau scientifique.

Toutefois, nous voulons souligner un point présent dans ce rapport, infirmer un élément présent dans la présentation orale de Campbell au Parlement Européen en Février 2000 et introduire un nouvel élément absent des rapports précités.

---

(14) Les cas exposés ci-dessus ont fait l'objet d'une étude dans le cadre du projet européen Eclip. Le rapport détaillant quelques technologies « privacides » se trouvent sur http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf

(15) Voir le rapport STOA de F Leprévost, point 6.2 et Bruce Schneier, op. cit. pp 584-586.

4.1. Prononcer le mot « bombe » au téléphone ne déclenche pas d'écoute

Pour ce faire, il faudrait tout d'abord que la communication internationale passe par satellite, ce qui semble être le cas d'un pourcent seulement des communications internationales (cfr supra). Même dans ce cas de figure, la technologie actuelle de reconnaissance vocale universelle n'est pas suffisamment au point pour permettre la reconnaissance vocale en temps réel. Par contre, il est possible actuellement de réaliser un dispositif capable de reconnaître l'empreinte vocale d'une personne particulière et d'initier un processus d'enregistrement et de traitement à ce moment. La recherche de mots-clés sensibles contenus dans un dictionnaire reste néanmoins possible lors de la surveillance des courriers électroniques ou du trafic Internet en général (si celui-ci circule par satellite[16]) ainsi que lors de la surveillance des téléfax, dans la limite des performances des logiciels de reconnaissance de caractère (les caractères envoyés doivent être clairs et non manuscrits).

En d'autres termes, la surveillance exploratoire et généralisée sur base de renifleurs (snifer) de mots-clés sensibles n'est possible que sur une partie du trafic satellitaire. Il semble aussi ou ainsi possible de détecter l'auteur d'une communication téléphonique sur base de son empreinte vocale.

4.2. La NSA_KEY de Microsoft

Internet s'est enflammé lors de la découverte, dans la base de registre du système d'exploitation Windows d'une variable appelée NSA_KEY. Nombreux furent ceux qui prétendirent alors que cette clé secrète permettait à la NSA de lire tous les messages encryptés à l'aide des fonctions de chiffrement fournies par Microsoft.

1. Cette hypothèse a été contredite par Microsoft alors que les « failles » évoquées supra (point 3.1) ont été admises par lui.

2. On imagine mal une clé secrète de déchiffrement stockée dans un endroit aussi visible que la base des registres

3. On imagine encore plus mal que le nom de cette clé soit « NSA_KEY ».

Cette fausse alerte ne doit cependant pas faire croire que les fonctions de chiffrement fournies par Microsoft soient sûres. Les signataires de ce rapport partagent avec de nombreux experts l'opinion selon laquelle toute exportation d'outils de chiffrement hors des USA n'est autorisée que lorsque les services américains possèdent la capacité technique de casser le chiffrement. De toutes façons, il est actuellement généralement admis dans le monde de la cryptographie qu'un logiciel de chiffrement n'est fiable que lorsque l'on dispose de son code source.

(16) Le présent rapport concerne Echelon. D'autres techniques d'écoute des réseaux terrestres existent…

4.3. Des clés faussement 128 bits

Il existe au moins deux manières de faire croire à un utilisateur même averti qu'il utilise un mode chiffrement à 128 bits[17] alors que son chiffrement effectif se limite à quarante bits.

La première technique aurait été réalisée par Lotus Notes et est décrite par Campbell. Elle consiste à transmettre les 88 derniers bits de la clé dans le corps du message, en clair. Cette technique est détectable.

La deuxième technique est plus subtile et consiste à conditionner le générateur de clés secrètes inclus dans le logiciel de chiffrement[18] de telle manière que celui-ci ne puisse générer que des clés incluses dans un espace de chiffrement limité à quarante bits. Sans accès au code source du logiciel de chiffrement, cette dernière technique est difficilement détectable car il faudrait générer plusieurs centaines de milliards de clés pour s'apercevoir de la supercherie. Selon un expert de Belgacom, cette dernière technique serait largement répandue dans les logiciels de chiffrement américains autorisés à l'exportation.

5. LA LÉGALITÉ DISCUTABLE DES PRATIQUES DU RÉSEAU ECHELON - COUP D'ŒIL SUR L'ENVIRONNEMENT JURIDIQUE DES "INTERCEPTIONS DE TÉLÉCOMMUNICATIONS"[19]

Le système Echelon tel que décrit ci-avant soulève de nombreuses questions quant à la légalité des interceptions de télécommunications auxquelles il est procédé.

Notre propos est dans un premier temps de rappeler à cet égard les principes tirés de la Convention européenne des Droits de l'Homme. Dans un deuxième temps, on rappelle la position européenne à cet égard qui progressivement a fait sienne les principes de la Convention européenne. Dans un troisième temps, on souligne combien la Belgique, en particulier lors du vote de la loi organique des services de renseignement et de sécurité, a traduit également de manière certaine ces principes, même si la loi reste malheureusement silencieuse dans la matière qui nous occupe.

Enfin, un quatrième et dernier temps démontre qu'il est loin d'être évident que le principal protagoniste des écoutes, les Etats-Unis, respecte les principes européens.

---

(17) Pour rappel, une clé à 128 bits est des milliers de milliards de milliards de fois plus sûre qu'une clé 56 bits

(18) Notons que ce risque n'existe pas si la clé secrète est conçue par un tiers de confiance ayant conçu lui-même son propre générateur de clés secrètes, en respectant les règles de l'art

(19) Le lecteur se réferera également à l'étude du Professeur Elliot, The legality of the interception of electronic communications. A concise survey of the principal legal issues and instruments under international, European and national law, working document for the STOA Panel, Luxembourg, oct. 1999, PE 168.184/Vol. 4/5. L'auteur y décrit d'autres sources nationales et internationales.

5.1. Premier temps: Les principes de la convention européenne des Droits de l'Homme s'opposent aux pratiques dénoncées propres au système Echelon

L'interception de messages transmis par télécommunications représente un danger tant pour la vie privée des personnes mises sur écoutes que pour leur liberté d'expression. Ces deux libertés représentent des libertés essentielles dont la protection est assurée par nombre de textes internationaux dont la Convention européenne des Droits de l'Homme[20]. Certes, des impératifs légitimes de sécurité de l'Etat justifient que les Etats disposent de moyens techniques efficaces permettant l'interception légale des télécommunications peu importe, le réseau ou le medium utilisé et peu importe qu'il s'agisse de la prise de connaissance du contenu des messages ou simplement de certains éléments de ceux-ci (ex: origine ou destination de l'appel, localisation de celui-ci).

Cependant comme le notent l'arrêt Klass[21] et l'arrêt Leander, il est nécessaire de disposer "*de garanties suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre*".

Quatre conditions dès lors limitent l'immixtion possible de l'Etat. Ces quatre conditions applicables en matière d'interception des télécommunications ont été maintes fois rappelées par la jurisprudence de la Cour européenne des droits de l'Homme. Ainsi, il importe:

1° que l'interception n'ait lieu que dans le cadre des objectifs d'intérêt vital de l'Etat énumérés par la Convention elle-même tant dans l'article 8 que dans l'article 10;

2° que ces finalités soient prévues par la loi, c'est-à-dire par un texte réglementaire accessible au public et rédigé de façon suffisamment précise pour que le citoyen puisse y répondre par un comportement adéquat (arrêt Kruslin 24 avril 1990);

3° ensuite, que la mesure prise soit strictement proportionnée à l'objectif poursuivi. A cet égard, comme le répètent notamment les arrêts Klass (arrêt du 6 septembre 1978) et Leander (arrêt du 25 février 1987), une surveillance exploratoire ou générale effectuée sur une grande échelle est prohibée;

4° enfin selon l'arrêt Leander rendu à propos de la contestation d'un citoyen convaincu d'être fiché par la sûreté de l'Etat et se voyant opposer lors de sa demande d'accès à son dossier, le dogme du secret indispensable à la sécurité de l'Etat, il importe qu'une balance soit opérée entre d'une part la protection de la vie privée et d'autre part les impératifs de sécurité et d'ordre public qui fondent la mission des services de renseignements et de sûreté; importe plus encore, ajoute l'arrêt, que cette balance soit opérée par une autorité indépendante[22].

---

[20] Cf. également le Pacte International du 19 décembre 1966 relatif aux droits civils et politiques qui prescrit en son article 17 que: *"Personne ne sera soumis à des interférences arbitraires et illégitimes qui iraient à l'encontre de sa vie privée". "Chacun a le droit à une protection légale contre de telles interférences*".

[21] Klass v. Germany (1978), 2HRR, p. 214; cf. également Malone v. UK (1984), 7 EHRR, p. 14.

[22] Comme peut l'être en Belgique, le Comité R, comité permanent de contrôle des services de renseignements dépendant du Parlement.

A propos des interceptions de télécommunications, précisément, la recommandation R(95)14 du Comité des Ministres du Conseil de l'Europe adoptée le 11 septembre 1995 "relative à la procédure pénale en rapport aux technologies de l'information" préconise entre autres que les lois pénales soient modifiées pour permettre l'interception en cas d'investigation lors d'attaques sérieuses contre les systèmes d'information et de télécommunications et que des mesures soient prises pour minimiser l'impact négatif de la cryptographie sans remettre en cause son utilisation au-delà de ce qui est nécessaire.

Ainsi, sous réserve de ce que nous dirons pour les Etats-Unis et leur situation réglementaire (cf. infra 5.4), pour qu'il y ait conformité aux exigences des principes du Conseil de l'Europe, il faut :

- que la (ou les) finalité(s) d'Echelon soi(en)t définie(s) par des textes réglementaires, clairs et accessibles au public[23].

- que les interceptions réalisées dans le cadre d'Echelon n'aient pas lieu sur base de la recherche systématique de mots clés ou selon d'autres critères généraux, mais, comme le prescrit la jurisprudence de la Cour européenne des droits de l'Homme, en fonction de critères spécifiques liés à des infractions précises ou à leurs auteurs supposés.

- qu'un tel système limite strictement la collecte de données à ce qui est nécessaire aux finalités de sûreté de l'Etat.

- qu'il soit analysé si un contrôle des écoutes par une autorité indépendante est prévu[24] conformément à l'exigence de l'arrêt Léander de la Cour européenne des Droits de l'Homme.

5.2. Deuxième temps: La position européenne: de l'ambiguïté à des propositions concrètes

L'article 6 du Traité sur l'Union européenne affirme: *"L'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'état de droit, principes qui sont communs aux états membres. L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, en tant que principes généraux du droit communautaire*".

(23) A tel point qu'il est évoqué l'utilisation du réseau Echelon à des fins d'espionnage industriel, ce qui est difficilement compatible avec les impératifs de la sûreté de l'Etat.

(24) Cf. à ce propos le rapport d'enquête "sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système américain " Echelon" d'interception des communications téléphoniques et fax en Belgique, rapport présenté par le Comité R au Sénat de Belgique le 14 février 2000, p.8 et les remarques à propos de l' Amendement proposé par le représentant au Congrès Bob Barr à l'Intelligence Authorization Act réclamant précisément les bases légales de l' intervention de la N.S.A. américaine en matière de surveillance électronique et d'interception de télécommunications.

Le traité d'Amsterdam[25] complète cette disposition de principe étendant par son article 46 la compétence juridictionnelle de la Cour de Justice des Communautés européennes à l'action des institutions: il s'agit de vérifier le respect des droits fondamentaux garantis à travers la référence que l'article 6 fait à la CEDH. Emerge dans l'ordre juridique communautaire un système commun de protection des droits fondamentaux.

C'est sur base de cet élargissement des compétences techniques que deux directives, l'une dite générale relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci, l'autre, spécifique[26]; concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, ont été prises et doivent être transposées dans les divers Etats membres.

Cet élargissement des axes fondateurs de la compétence européenne justifie également dans les directives dites "Télécommunications", l'ajout, parmi les "exigences essentielles", du respect de la protection des données.

Cet ajout impose ce respect à la fois pour l'agréation des équipements terminaux[27], pour la fourniture des réseaux ouverts[28] et de manière générale pour les autorisations générales et les licences individuelles dans les Etats Membres[29] . Surtout, il autorise la prise de mesures nationales et européennes pour assurer cette protection[30]. En ce sens, le rapport STOA[31] préconisait l'adoption par les pays européens d'un encryptage généralisé comme mesure de protection contre des écoutes ou des mesures de surveillance contraires aux principes déjà décrits[32].

Pour bien comprendre la position européenne à propos de la légitimité des "interceptions" de télécommunications, il faut tenir compte du fait que la préoccupation européenne en faveur des Droits de l'Homme et son acceptation des principes déjà évoqués de la jurisprudence de la Cour européenne des Droits de l'Homme est récente.

---

[25] signé le 2 octobre 1997 (J.O.C.E. C. 103, 24 avril 1977).

[26] Directive 95/40/CE du 24 octobre 1995, J.O., L 281 du 23 novembre 1995, p. 31.

[27] Directive 99/5/CE du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, L. 91/10, 7.4.99 art. 3.3. qui prévoit des possibilités de mesures prises par la Commission en matière d'équipements radio.

[28] Directive du Conseil 90/387/CEE du 28 juin 1990 telle que modifiée par la directive 97/51/CE du Parlement européen et du Conseil du 6 octobre 1997 en vue de les adapter à un environnement concurrentiel dans le secteur des télécommunications, J.O. n° L 295/23, 29.10.1997 dite "directive ONP Amendment".

[29] Il s'agit de la directive 97/13/CE du Parlement européen et du Conseil du 10 avril 1997 (J.O.C.E., L. 117, mai 1997).

[30] Ainsi, l'article 3.3. de la directive 99/15/CE: "Conformément à la procédure prévue à l'article 15, la Commission peut décider que les appareils relevant de certaines catégories d'équipements ou certains types sont construits de sorte:
b) qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés; …

[31] Il s'agit de la partie 4/4 des rapports STOA présentés au Parlement européen en avril et mai 1999 et réalisés à sa demande. Cette partie est intitulée : « *The State of the Art in communication Intelligence (COMINT) for intelligence purpose of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT Targeing and Selection, including speech recognition* » et surtout du Rapport STOA présenté au Parlement en octobre 1999 (PE 168 184/Vol. 1 à 5) et *intitulé "Development of Surveillance Technology and Risk of Abuse of economic Information*".

[32] Le rapport plaide également pour une libéralisation de la cryptographie dans la politique européenne en matière de cryptographie, dans les accords de Wassenaar et les réglementations des Etats membre, cf. le site de B.J. Koops: Crypto Law Survey, http:// CWIS. Kab.nl/ /friv/people/cls2.htm.

Ainsi, c'est dans une totale méconnaissance de ces préoccupations que le Conseil de la Communauté européenne a adopté, sous la pression américaine, le 17 janvier 1995, une résolution[33] visant à faciliter les écoutes téléphoniques.

La résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications détaille les conditions techniques nécessaires à l'interception des télécommunications, sans aborder la question des conditions dans lesquelles de telles interceptions devraient avoir lieu. Le texte de la résolution prévoit une obligation dans le chef des opérateurs de réseaux ou des fournisseurs de services de fournir en clair aux "services autorisés" les données interceptées.

Ces données visent les appels téléphoniques mobiles ou non, les courriers électroniques, les télécopies et messages télex, les flux de données Internet, tant au niveau de la prise de connaissance du contenu des télécommunications que des données de trafic, mais également tout signal émis par la personne faisant l'objet de la surveillance.

Les données concernent la personne surveillée ainsi que les personnes qui appellent ou qui sont appelées par cette personne.

La résolution prévoit également que la localisation géographique de l'utilisateur mobile constitue une donnée à laquelle les services autorisés doivent avoir accès.

Cette résolution prise à la hâte et sans contrôle parlementaire a été remise en question récemment par le Parlement, qui tire en la matière, les conséquences de l'adoption par l'Union européenne du traité d'Amsterdam. Il est intéressant de noter que la Résolution du Parlement européen prise le 16 septembre 1998 visait précisément les relations transatlantiques et le système Echelon en particulier et qu'elle conclut que, nonobstant l'importance de telles relations et des objectifs supposés du système Echelon, "*il est essentiel que l'on puisse s'appuyer sur des systèmes de contrôle démocratique en ce qui concerne le recours à ces technologies et les informations obtenues*".

Ses recommandations sont plus nettes encore .

Le Parlement européen :

"12 …… demande que de telles technologies de surveillance fassent l'objet d'un réel débat ouvert, tant au niveau national qu'à celui de l'Union européenne, et soient soumises à des procédures garantissant une responsabilité sur le plan démocratique;

13 ……réclame l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus;

---

[33] Résolution du Conseil 17/1/95, J.O. C. 329 du 4 novembre 1996 p. 1 à 6 (à noter que la publication fut tardive et que la résolution fut prise sans l'avis du Parlement). Cette résolution est suivie par une déclaration commune d'intervention signée tant par les autorités américaines que celles européennes concernant la surveillance légale des télécommunications qui prévoit l'échange d'informations et de recommandations relatives aux spécifications en matière d'interception à destination tant de la direction du FBI américain que du Secrétariat général du Conseil de l'Union européenne (Doc. ENFOPOL 112 - Bruxelles 25 octobre 1995).

14……. estime que l'importance croissante du réseau Internet, et, plus généralement, des télécommunications à l'échelle mondiale et en particulier le système Echelon, ainsi que les risques de leur utilisation abusive appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace;

15…….. charge son Président de transmettre la présente résolution, à la Commission, au Conseil et au Congrès américain."

Le 3 mai 1999, le groupe de Protection des personnes à l'égard du traitement des données personnelles(34) émettait une recommandation concernant le respect de la vie privée dans le contexte de l'interception des télécommunications(35).

Cette recommandation rappelle le principe du secret des communications et note que celui-ci est garanti par la directive 97/66/CE qui crée pour les Etats membres une obligation de garantir le secret des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessibles au public.

Dans son article 14 paragraphe 1, la directive 97/66/CE précise que les Etats membres ne peuvent limiter l'obligation de confidentialité des communications sur des réseaux publics que lorsqu'une telle mesure constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales. Ainsi, si exception il y a, celle-ci est de stricte interprétation et suppose que l'écoute soit le moyen indispensable à l'objectif recherché.

Au-delà, la recommandation insiste sur les obligations des opérateurs et fournisseurs de télécommunications de prévoir toutes les mesures de sécurité(36) ainsi que le cryptage systématique des messages afin de rendre techniquement difficile ou impossible, selon l'état actuel de la technique, l'interception des télécommunications par des instances non autorisées par la loi.

Le groupe souligne à cet égard que la mise en œuvre de moyens efficaces d'interception des communications à des fins légitimes, utilisant précisément les techniques les plus avancées, ne doit pas avoir pour conséquence d'abaisser le niveau général de confidentialité des communications et la protection de la vie privée des individus.
Ces obligations prennent un sens particulier dans le cas où les télécommunications entre des personnes situées sur le territoire des Etats membres transitent ou peuvent transiter hors du territoire européen notamment lors de l'utilisation de satellites ou d'Internet(37).

(34) Il s'agit du groupe créé par l'article 29 de la directive 95/46. Sa compétence est cependant purement consultative

(35) Recommandation 2/99 document 5005/99/final W.P. 18. La Commission belge de Protection de la Vie Privée fut à l'origine du processus qui mena à cette recommandation. Elle fut saisie dès 1998 par lettre du Ministre belge de la Justice de l'époque.

(36) Il s'agit du principe général de sécurité des données, affirmé par l'article 7 de la Convention du Conseil de l'Europe n° 108, par l'article 17 § 1 et § 2 de la directive 95/46 et par les articles 4,5 et 6 de la directive 97/66/CE.

(37) Sur ce point, la recommandation rappelle le prescrit de l'article 25 de la directive qui prévoit l'interdiction de tout flux transfrontiers vers des pays ne disposant pas d'une protection adéquate.

La recommandation s'achève par l'énumération d'une série de conditions relatives à toute interception de télécommunications. Nous la reprenons telle quelle.

"Il importe que le droit national précise de façon rigoureuse et dans le respect de toutes les dispositions susmentionnées :

- *Les autorités habilitées à permettre l'interception légale des télécommunications, les services habilités à procéder aux interceptions et la base légale de leur intervention ;*

- *les finalités selon lesquelles de telles interceptions peuvent avoir lieu, qui permettent d'apprécier leur proportionnalité au regard des intérêts nationaux en jeu ;*

- *l'interdiction de toute surveillance exploratoire ou générale de télécommunications sur une grande échelle;*

- *les circonstances et les conditions précises (par exemple éléments de fait justifiant la mesure, durée de la mesure) auxquelles sont soumises les interceptions, dans le respect du principe de spécificité auquel est soumise toute ingérance dans la vie privée d'autrui ;*

- *le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités publiques ne peuvent avoir accès à ces données qu'au cas par cas, et non de façon générale et proactive.*

- *Les mesures de sécurité en ce qui concerne le traitement et le stockage des données, et leur durée de conservation;*

- *en ce qui concerne les personnes impliquées de façon indirecte ou aléatoire dans les écoutes, les garanties particulières apportées au traitement des données à caractère personnel: notamment, les critères justifiant la conservation des données, et les conditions de la communication de ces données à des tiers;*

- *l'information de la personne surveillée, dès que possible;*

- *les types de recours que peut exercer la personne surveillée ;*

- *les modalités de surveillance de ces services par une autorité de contrôle indépendant;*

- *la publicité - par exemple sous forme de rapports statistiques réguliers - de la politique d'interception des télécommunications effectivement pratiquée;*

- *les conditions précises auxquelles les données peuvent être communiquées à des tiers dans le cadre d'accords bi- ou multilatéraux. "*

5.3. Troisième temps: la loi belge reprend les principes du Conseil de l' Europe mais les traduit insuffisamment en matière d'interception de télécommunications.

Sans vouloir revenir sur les péripéties de la naissance et du vote de la loi organique des services de renseignement et de sécurité (Sénat 1-758/10,11 et 15 MB, 18 décembre 1998)[38], on peut considérer que finalement le législateur belge a entendu faire siennes les demandes réitérées du Conseil d'Etat et de la jurisprudence belge qui depuis 1990 rappelaient avec énergie la jurisprudence constante de la Cour européenne des droits de l'homme pour dénier tout droit de la Sûreté de l'Etat et des services de renseignement à la collecte et aux traitements d'informations vis-à-vis de citoyens ou de manière plus large d'individus[39]: "*Considérant que l'article 8 § 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales permet l'ingérence de l'autorité publique dans l'exercice du droit de toute personne au respect de sa vie privée, pour autant que cette ingérence est conforme à la loi, qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, notamment à la sécurité nationale et à la sûreté publique, et que les textes qui la prévoient soient accessibles à l'intéressé et rédigés en termes assez clairs pour lui indiquer de manière adéquate quelles circonstances et sous quelles conditions, ils habilitent la puissance publique à s'y livrer, spécialement si l'ingérence présente un caractère secret*" (arrêt Wicart du Conseil d'Etat (30/6/95, arrêt n° 54-139).

Ainsi, la loi organique, par touches successives depuis le projet initial, a défini avec précision tant les activités qui menacent ou peuvent menacer la sécurité de l'Etat, que les intérêts qui doivent être protégés contre ces menaces[40]. Comme le notait d'emblée l'exposé des motifs du projet de loi organique : "*Les respect et la protection des droits et libertés individuels ainsi que le développement démocratique de la Société doivent toujours guider l'action des services de renseignements et de sécurité. Ce principe fonde la légitimité de leur action et est rappelé aux articles 6 et 8 du projet*"[41].

---

(38) A ce propos, Yves Poullet, B. Havelange, Secrets d'Etat et Vie Privée ou Comment concilier l'inconciliable?, Colloque international du 20 janvier 1999 organisé par le comité R, "Secret d'Etat ou Transparence, Bruxelles, publié in Droit des technologies de l'Information et de la Communication, Regards Prospectifs, E. Montero (ed.), Cahier du CRID n° 16, Bruylant, Bruxelles, 1999, p. 233.

(39) Cf. également l'avis de la Commission de Protection de la Vie Privée relative au projet de loi organique des services de renseignements et de sécurité, Avis n° 12/98 du 23 mars 1998.

(40) Cf. à ce propos, les réflexions apportées par Mr. B. Van Lysebeth, administrateur général de la Sûreté de l'Etat, lors de son audition au Sénat, Doc. Sénat, Session 1997-1998, Doc. I/758/10, p. 62 et s.

(41) Exposé des motifs. Projet de loi organique des services de renseignements et de sécurité, Ch. des Rep. Sess. ord. 2 juillet 1996, Doc. Parl. 638/1 95/96, p. 3.

Certes en ce qui concerne le sujet qui nous occupe, on regrettera avec le Comité R[42] que la loi organique, même si elle rappelle à suffisance les principes de la jurisprudence du Conseil de l'Europe, ne prenne soin d'appliquer ces principes de manière précise aux écoutes téléphoniques[43] par les services de renseignements et de sécurité voire établisse des principes communs à toutes les formes d'interception qu'elles soient opérées dans le cadre d'une instruction criminelle par les autorités de police, de gendarmerie ou judiciaires ou par les Services de renseignement et de sécurité[44].

5.4. Quatrième temps: Les Etats-Unis ne semblent pas respecter les principes ci-avant rappelés.

Le gouvernement américain[45] répond aux interrogations européennes du Parlement européen en faisant valoir sa soumission à l'Amendement n° 4 de la Constitution américaine compris dans le fameux Bill of Rights[46].

Cet amendement affirme: "*The right of the people to be secure in their persons, homes, papers and effects, against unreasonable searches and seizures shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*".

Il n'est pas certain que l'interprétation du texte de l'amendement n° 4 soumette la N.S.A. aux mêmes exigences que celles imposées par la jurisprudence européenne.

---

(42) A cet égard, les recommandations du Comité R, reprise dans le rapport annuel de 1996, Titre II, Chap. 2, p. 47. Dans le rapport annuel de 1997, 2ème partie, Chap. 1, Section 3, p. 99, enfin, dans le rapport annuel de 1998, IIe Partie, B, chap. I, p. 102. A noter en particulier déjà les conclusions du Rapport de 1996: " Ayant en vue l'efficacité des services de renseignements, le Comité ne peut qu' approuver la volonté de leur conférer des possibilités légales d'écoutes et d' interception de télécommunications. Ayant en vue la protection des droits des personnes, le Comité ne peut accepter ce moyen de recueillir le renseignement sans l'assortir de garanties rigoureuses et de modalités de contrôle."

(43) A ce stade, on notera cependant l'exception que constitue l'article 44 de la loi organique qui autorise et limite la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service général du renseignements et de la sécurité des Forces Armées, à des fins militaires, de radiocommunications militaires émises à l'étranger. A propos de cette exception et du raisonnement a contrario auquel invite cette seule exception légale à propos d' autres cas d'écoutes par les services de renseignement ou de sûreté, lire Y.Poullet et B.Havelange, article cité.

(44) A noter la recommandation du Comité R dans son rapport de 1997. Nous (Y. Poullet, B. Havelange, art. cité.) plaidions dans le même sens.

(45) "*In Washington, State Department spokesman James P. Rubin denied any involvement in commercial espionage by the National Security Agency. 'The National Security Agency is not authorized to provide intelligence information to private firms. That agency acts in strict accordance with American law," Rubin said. "US.intelligence agencies are not tasked to engage in industrial espionage or obtain trade secrets for the benefit of any U.S. company or companies*". (CBS News: "US Accused of Industrial espionage, document repris du site: http://cbsnews.cbs.com/now/story/o,1597, 164465.412,00.Shtml.

(46) Le texte du Bill of Rights est disponible sur le site http://lcweb2.loc.gov/const/bor.html.

De l'analyse des documents présentant la N.S.A.[47], il ressort certes que les activités de la N.S.A. sont soumises à la fois à la Constitution, la loi fédérale[48], les réglementations de l'exécutif et du département de la défense et qu'une procédure "effective" de surveillance menée à la fois par le Président's Intelligence Oversight Board (IOB) et les Comités de contrôle des congrès (composés à la fois de représentants du Sénat et de la Chambre des Représentants) permet à ces organes d'être informés des activités de la N.S.A. et veille en particulier au respect du droit à la vie privée des citoyens américains.

L'information de tels organes et leur contrôle est-il direct ? Cela n'est point certain dans la mesure où des sources que nous avons pu consulter, il semble que c'est à travers l ' « Office of the Inspector General » (OIG) que s'exerce ce contrôle. C'est cet office qui conduit les inspections, investigations et audits nécessaires pour vérifier l'exécution conforme à la loi des opérations menées par la N.S.A. et dresse rapport de ses missions aux autorités rappelées ci-dessus.

En conclusion, la protection des citoyens, à supposer qu'elle soit comparable, équivalente ou adéquate vis-à-vis des exigences européennes, n'existe que pour les citoyens américains. Cette limite est d'autant plus significative que les législations américaines protectrices des citoyens, ainsi le Privacy Act de 1974 et le Freedom of Information Act de 1966, ne concernent également que les seuls citoyens américains[49].

---

(47) Cfr. en particulier, le site du N.S.A. et en particulier les pages relatives aux F.A.Q. http://www.NAS.gov/about_nsa/faq8_.internet.html. Nous reprenons ci-après le texte de la réponse à deux questions essentielles dans le contexte qui nous occupe:

"How are the activities of NSA/CSS regulated?

The US Constitution, federal law, executive order and Executive Branch and Department regulations, govern NSA/CEE activities. They are designed to balance the government's need for foreign intelligence information and individual privacy rights in a reasonable way. The House Permanent Select Committee on Intelligence (HPSCI) ensures adherence by the Agency to laws and regulations, espcially with regard to protection of U.S. citizen's right to privacy (including military civilian Agency employees --who are all U.S. citizens).

How is compliance with the regulations monitored?

An effective oversight process involving the Executive Legislative, and Judicial Branches is in place to ensure that NSA/CSS complies with the regulations. At the very top, the President's Intelligence Oversight Board (IOB) and the Congressional Oversight Committees (both Senate and House of Representatives) keep fully informed of our intelligence activities. In addition to those entities, the National Security Council (NSC), the Department of Defense (DoD) and the Department of Justice also provide oversight".

(48) Il s'agit du Foreign Intelligence Surveillance Act (FISA) de 1978. Cette législation concerne les opérations d'espionnage et de contre espionnage (Intelligence and Counterintelligence). Elliott (rapport cité, p. 12) les opérations d'écoutes peuvent être autorisées par un "Présidentiel Order" et s'il s'agit d'écoutes relatives à des puissances étrangères et les communications visées par de telles écoutes ne doivent pas nécessairement être liées à un "crime" (crime): attaques, sabotage, terrorisme, activités d'espionnage,…

(49) A cet égard, la réponse d-à la FAQ : « **Does NSA/CSS unconstitutionally « spy on » or garget ?** ». The NSA/CSS performs SIGINT operations against foreign powers or agents of foreign powers. We strictly follow laws and regulations designed to preserve every American's privacy rights under the Fourth Amendment to the United States Constitution. The Fourth Amendment protects U.S. persons from unreasonable searches and seizures by the U.S. Government or any person or agency acting on behalf of the U.S. Government". A noter , dans le même sens, la réponse du Ministre britannique interrogé à propos des interceptions et de la protection des citoyens, le Ministre se montre rassurant vis-à-vis de la protection des seuls citoyens anglais (supra, n°1, 2).

6. CONCLUSIONS

6.1. De l'existence du réseau Echelon

Il nous semble évident que le réseau Echelon existe et qu'un maillon important de ce réseau est la base anglaise de Menwith Hill, dans le Yorkshire anglais. Sur cette base travaillent plus de mille ressortissants américains et un bon demi millier d'Anglais, présents à tous les niveaux de cette base. Ceci est présenté par l'exécutif du Royaume-Uni comme une garantie que rien d'hostile envers le Royaume-Uni ou envers des citoyens britanniques n'est accompli dans cette station. Cette base échappe au contrôle parlementaire sur le terrain même si, parfois dans l'histoire, certains ministres du Royaume-Uni ont accepté de répondre à certaines questions parlementaires.

6.2. De la capacité technique du réseau Echelon

Echelon peut capter la totalité du trafic satellitaire à destination de l'Europe. La NSA, un des services secrets américains qui serait présent sur la base anglaise possède un budget et un personnel plus important que Belgacom. Ses capacités de déchiffrement sont gigantesques et l'histoire récente tend à prouver qu'elles sont minimalisées d'au moins un facteur mille à dix mille dans les déclarations publiques des services américains. Par ailleurs, toute technologie américaine (software et hardware) licitement exportée vers l'Europe est considérée par de nombreux experts, -et nous partageons cet avis-, comme intrinsèquement et volontairement sujette à une surveillance aisée, à distance et discrète par les services américains.

La technologie actuelle permet la surveillance exploratoire et généralisée sur base d'un dictionnaire de mots-clés du courrier électronique non chiffré et, dans une certaine mesure du trafic téléfax, à la condition expresse que ces télécommunications utilisent des satellites. La technologie actuelle ne permet pas cette surveillance exploratoire et généralisée des communications téléphoniques satellitaires (environ un pour-cent des communications téléphoniques internationales) mais autorise la reconnaissance d'un locuteur particulier sur base de son empreinte vocale.

6.3. Des activités du réseau Echelon

Que font les 1800 personnes travaillant à Menwith Hill ? Les signataires du présent rapport sont incapables de répondre à cette question. Les cas d'espionnage industriel dévoilés principalement par la France vis-à-vis d'entreprises françaises n'ont pas à ce jour été démontrés. Ils ne le seront probablement jamais tant les technologies d'écoute actuelles laissent peu de traces. Tant les américains que les Anglais ont démenti que ce réseau soit utilisé à des fins d'espionnage économique (ce qui revient à admettre son existence et ses capacités à le faire).

Un doute important subsiste néanmoins tant dans l'esprit des parlementaires et de la population que des experts européens en télécommunications dont près d'un tiers croient à l'espionnage industriel organisé par les grandes puissances, les deux tiers restants n'y croyant pas ou ne pouvant pas se prononcer.

Nous tenons ici à souligner avec vigueur qu'il est impossible de connaître avec certitude ce que fait ou ce que ne fait pas le réseau Echelon. Selon Bamford[50], *« Il est hautement improbable qu'Echelon surveille tout le monde partout comme les critiques le proclament. Il serait impossible à la NSA d'intercepter toutes les communications. L'agence a connu d'importantes réductions de personnel au cours des cinq dernières années alors que ses cibles pour la sécurité nationale ont augmenté en nombre : le déploiement des missiles nord-coréens, les essais nucléaires en Inde et au Pakistan, la circulation de présumés terroristes, etc ... Etre à l'écoute du business européen en vue d'aider des sociétés américaines ne serait qu'une mission de faible priorité. Et transmettre le produit d' interceptions secrètes à des compagnies serait rapidement découvert »*.
Par contre, il est possible d'établir une évaluation raisonnable des possibilités minimales d'interception d'Echelon. Au nom des principes de précaution et de souveraineté, la description des capacités d'un tel réseau suffit ici amplement à justifier l'intervention de l'Etat.

6.4. De la légalité de l'interception des télécommunications

Il semble que les principes généraux de la jurisprudence du Conseil de l'Europe qui limitent strictement les interceptions de télécommunications aient été largement repris à la fois par l'Europe et par la Belgique;

Ces principes généraux exigent que les interceptions

- ✓ aient lieu sur base d'un fondement légal, définissant avec précision les finalités de telles interceptions;
- ✓ ne puissent en aucune manière être opérées de manière générale et exploratoire;
- ✓ menées dans ce cadre fassent l'objet d'un contrôle par une instance indépendante.

Il est loin d'être évident que le système réglementaire des Etats-Unis suive les mêmes principes et surtout permettent d'offrir une protection aux citoyens non américains.

6.5. Des enjeux de la sécurité des télécommunications

L'espionnage économique et la protection de la vie privée ont souvent été cités comme des enjeux importants et nous n'y reviendrons pas. Trois autres enjeux méritent d'être signalés.

(50) Cfr note 11

Le premier concerne l'écoute politique menée par des partis politiques au pouvoir ou des membres de ceux-ci afin d'espionner les adversaires politiques. On peut rappeler le scandale du Watergate ou les écoutes effectués par l'Elysée en France. Il reste extrêmement tentant pour un parti au pouvoir de surveiller ses adversaires démocratiques afin d'obtenir sur lui un avantage politique déterminant. Ce type d'écoute sape le jeu normal de la démocratie et tout état démocratique se doit de les empêcher.

Le deuxième enjeu est la confiance des citoyens dans leur réseau de télécommunication. Les pseudos capacités de ce réseau ont été amplifiées et déformées par la presse et il existe un risque croissant du développement d'une réticence à l'utilisation des réseaux, notamment dans le cadre du commerce électronique, mais aussi dans le cadre de l'utilisation d'Internet à des fins non commerciales. Nous pensons par exemple à l'utilisation d'Internet pour la recherche d'informations politiques, médicales, religieuses, philosophiques, scientifiques ou culturelles et à la participation à des forums publics de discussion. Le sentiment d'être espionné, même en l'absence de tout fondement scientifique raisonnable, risque d'être un obstacle majeur au développement de l'utilisation des réseaux de télécommunication.

Le troisième enjeu concerne le risque d'apparition anarchique de solutions techniques de cryptage de plus en plus performantes, rendant difficile voire impossible l'interception légale du contenu des télécommunications.

6.6. Des moyens d'augmenter la sécurité des télécommunications dans un contexte démocratique

La sécurité des communications se situe donc bien au-delà du contrôle du trafic satellitaire ou des câbles des réseaux de télécommunication mais passe obligatoirement par le contrôle des logiciels et du matériel, notamment d'origine étrangère, utilisé lors des télécommunications. Des instruments juridiques existent déjà à cet effet et même s'ils ont été sous-utilisés jusqu'à présent, il nous semble inutile de créer un nouveau dispositif légal contraignant. Des moyens techniques sont également disponibles. Les recommandations ci-après détaillent quelques-uns des raisons et des moyens d'agir.

Toutefois il ne faudrait pas, en tentant d'éviter la peste, attraper le choléra. Le réseau de télécommunication d'un état démocratique moderne doit pouvoir faire l'objet d'écoutes par des services autorisés, à certaines conditions et moyennant un certain contrôle. Il nous semble exclu qu'existe un contrôle a priori, général et exploratoire de toutes les écoutes et il nous apparaît important que le comité de surveillance ad hoc puisse être informé de manière certaine du volume, des services responsables et de la finalité générale (p.e. terrorisme, blanchiment,…) des interceptions légales des télécommunications. Un droit ponctuel de regard, par rapport à certaines interceptions particulières, devrait également lui être accordé. En bref, nous plaidons pour que les conditions légales qui président à l'interception légale des télécommunications s'appliquent, mutatis mutandis, à la surveillance légale de ces interceptions. Faut-il rappeler qu'il s'agissait, dès 1996, d'une recommandation du Comité R (cfr supra, point 5.3) ?

7. DE QUELQUES RECOMMANDATIONS

7.1. … et de leur double fondement

Nos recommandations (cf. le point 6.2.) s'appuient sur un double fondement : le principe de précaution récemment mis en exergue par l'Union Européenne et considéré par elle comme une règle coutumière de droit international[51] est le premier.

Il affirme le devoir d'agir de l'Etat lorsqu'un risque même incertain ou dont nous ignorons l'ampleur exacte menace ses citoyens.

Le principe de souveraineté "fonctionnelle" est le second fondement. Il représente "la manifestation de liberté et d'indépendance par laquelle l'Etat impose sa règle à ses nationaux et en impose le respect de la part des autres Etats"[52].

7.1.1. Le principe de précaution

"Le principe de précaution devrait aussi consolider l'approche préventive en forçant les pouvoirs publics à agir alors même qu'ils ne disposent pas de toutes les preuves justifiant le bien-fondé de leur action" écrit N. de Saedeleer[53] . L'auteur, à la suite d'une doctrine et d'une jurisprudence nombreuse, distingue ainsi la prévention de la précaution. "Alors que la certitude appelle une attitude de prévention, son incertitude requiert la précaution".

Plus précisément encore, ajoute l'auteur "la prévention consiste à prendre les mesures nécessaires à la non-survenance d'un événement prévisible ou, en tout cas, probabilisable. Elle est au cœur de toute une série de dispositions juridiques en matière d'environnement, de sécurité, de sécurité du travail notamment. La précaution consiste, quant à elle, à aller plus loin soit en multipliant, au-delà de ce que la probabilité rend nécessaire, les mesures de protection, soit en adoptant des mesures de protection à l'encontre des risques qui ne sont même pas probabilisables".

Les risques représentés aujourd'hui et demain par des systèmes de surveillance comme Echelon, sont difficilement mesurables. Ils dépendent de nombreux paramètres non connus, la puissance de cryptage, l'ampleur des moyens humains et techniques mis en place, etc. .. .

---

(51) Sur ce point, le lecteur lira avec intérêt les développements consacrés à l'argumentation européenne devant l'OMC par Kowilsky et Viney dans leur rapport au premier Ministre (français) remis le 15 octobre 1999, La documentation française, p. 115 et s. : "Le principal argument des Communautés européennes est que le principe de précaution est, ou est devenu, une règle coutumière générale de droit international ou du moins un principe général du droit… Les instances européennes estiment que l'application du principe de précaution signifie qu'il n'est pas nécessaire que tous les scientifiques du monde entier soient d'accord sur la possibilité et l'ampleur du risque de la même façon… Les Etats-Unis ne considèrent pas le principe de précaution comme une règle de droit international et coutumier et ils estiment qu'il s'agit d'une "approche" plus que d'un "principe"…".

(52) R. Wilkin, Dictionnaire du droit public, Bruxelles, Bruylant, 1963.

(53) N. de Sadeleer, Les principes du pollueur-payeur, de prévention et de précaution, Bruylant, 1999, 395

Sans doute, le principe de précaution est-il habituellement évoqué à propos des soucis de protéger la santé, la sécurité humaine et l'environnement[54] mais l'extension aux exigences de protection de l'information personnelle et économique véhiculées par les correspondances privées ne devraient pas poser de difficultés tant il est déjà reconnu par l'organisation mondiale du commerce que les exigences de la protection de la vie privée pouvaient, à l'instar des préoccupations sanitaires, sécuritaires et environnementales, justifier une restriction légitime à la liberté des échanges.

L'adoption du principe de précaution aurait les conséquences suivantes soulignées par le rapport de Kowilsky-Viney au Premier Ministre français :

« *Le principe de précaution définit l'attitude que doit observer toute personne qui prend une décision concernant une activité dont on peut raisonnablement supposer qu'elle comporte un danger grave pour la santé ou la sécurité des générations actuelles ou futures, ou pour l'environnement. Il s'impose spécialement aux pouvoirs publics qui doivent faire prévaloir les impératifs de santé et de sécurité sur la liberté des échanges entre particuliers et entre Etats. Il commande de prendre toutes les dispositions permettant, pour un coût économiquement et socialement supportable, de détecter et d'évaluer le risque, de le réduire à un niveau acceptable et, si possible, de l'éliminer, d'en informer les personnes concernées et de recueillir leurs suggestions sur les mesures envisagées pour le traiter. Ce dispositif de précaution doit être proportionné à l'ampleur du risque et peut être à tout moment révisé* »[55].

7.1.2. La souveraineté

La captation de messages transitant par satellites suscite des questions délicates. On sait que l'espace aérien (au-delà de 100 km) appartient au domaine public international et est affecté à l'usage commun de l'ensemble des Etats. Le droit international autorise chaque Etat à effectuer des actes d'utilisation sans distinction et sur une base d'égalité[56]. La captation des transmissions se fait cependant au sol. Il s'exerce dans le cadre des actes de "souveraineté territoriale"[57] même s'il suppose une utilisation de l'espace atmosphérique et peut concerner des messages n'ayant aucun lien avec le territoire où s'effectue la captation.

C'est précisément cette absence de lien potentiel entre le lieu de l'écoute et le message écouté, joint au pouvoir que donne la puissance des technologies de l'information et de la communication, de collecter et de traiter des milliers de message qui crée problème. Le Ministre de la Défense nationale lors du vote de la loi organique, mettait en évidence les périls que créaient ces technologies nouvelles: "les technologies de l'information et de la communication peuvent se muer en armes, devenir des moyens de destruction comme de dissuasion.

---

(54) Ainsi, le récent débat sur les O.G.M. (sur ce point, le rapport de Kowilsky et Viney, p. 74 et s.).

(55) Kowilsky-Viney, op. cit., p. 117.

(56) Cf. le traité entré en vigueur le 27 janvier 1967 approuvé par l'Assemblée Générale des Nations Unies, traité sur les principes régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique y compris la Lune et autres corps célestes.

(57) Il s'agit de la première conception de la notion de souveraineté telle qu'elle est défendue dans la célèbre affaire Lotus (décision du 7 sept. 1927, Cour Permanente de Justice internationale de la Haye publié notamment in Journal de droit international privé, 1927, p. 1002 et s.).

Voir les propos récents du Président Chirac à propos d'Helios: "la possibilité de voir au-delà de l'horizon est une nouvelle source de puissance géopolitique, comme l'arme atomique"[58].

Bref, la captation abusive de messages par une personne étrangère risque de remettre en cause la souveraineté des Etats en tant cette fois qu'expression du principe d'indépendance de chaque Etat dans l'ordre international[59]. Que devient l'indépendance d'un Etat, si les secrets de ses administrations, de son gouvernement, de ses entreprises, de ses citoyens peuvent être décryptés en des lieux inconnus au profit de puissances étrangères du seul fait qu'ils pénètrent l'espace extra atmosphérique ? L'absolue limitation des écoutes est fondamentale pour que survivent l'égalité et l'indépendance des Etats.
Enfin, la souveraineté des états n'est-elle pas remise en cause dans un autre sens encore ? L'appartenance d'un individu à un Etat lui donne le droit de bénéficier d'une protection par son Etat des garanties et libertés constitutionnelles qui lui sont octroyées[60]. Ces garanties et libertés ne peuvent être remises en cause du seul fait que les technologies de l'information et de la communication abolissent les frontières physiques et que l'envoi d'un courrier électronique de Namur à Bruxelles peut transiter par les Etats-Unis, au seul gré des réseaux et sans que l'utilisateur n'en soit ni conscient, ni averti. C'est sur base de telles considérations et au nom des valeurs essentielles que représente la défense des libertés des citoyens européens que la directive 95/46 relative à la protection des données interdit les flux vers les pays ne présentant pas un régime de protection adéquat.[61]

---

(58) Projet de loi organique, Exposé du Ministre de la Défense nationale, in Rapport fait au nom des Commission réunies de la Justice et des Affaires étrangères; Séance 9/7/98, Doc. Sénat 1.758/10, p. 7.

(59) A ce propos, la réflexion de R. de Bottini, Souveraineté et conflits de lois, in La Souveraineté au 20e siècle, Armand Colin (éd.), 1971, p. 145: « *La raison de cette opposition tient sans doute à l'ambiguïté de la notion de souveraineté, susceptible en l'espèce de recouvrir deux acceptions bien différentes. On peut y voir d'abord le principe d'une délimitation souveraine des compétences législatives de chaque Etat; elle permettrait de fixer unilatéralement dans le domaine spatial les frontières que chaque loi peut avoir par opposition à toutes les autres lois nationales. Mais on peut aussi faire appel à cette notion de souveraineté dans un sens plus banal, selon lequel elle ne serait alors que l'expression du principe d'indépendance de chaque Etat dans l'ordre international.* »

(60) " Il est vrai qu'il faut éviter toute pétition de principe et ne pas légitimer tout transfert, d'un point de vue constitutionnel, par le seul fait qu'il résulte d'un accord international en bonne et due forme. Il y a des limites objectives et des garanties nécessaires.
La première est qu'on ne peut transférer plus de pouvoir qu'on n'en a. La souveraineté nationale belge est limitée par les droits individuels. Il serait impossible de consentir par traité à des organes supranationaux, des pouvoirs qui limitent ces libertés" (P. Vigny, Propos institutionnels, Bruxelles, Bruylant, 1963, p. 117).

(61) L'article 25 est commenté comme suit dans les considérants de la Directive :
(56) considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;
(57) considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;
A propos de cet article, et en particulier de la notion de protection adéquate, lire Y .Poullet, B. Havelange « Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regards to the processing of personal data, European Commission, Annex to the annual report 1998 (XV D/5047/98) of the working party established by art 29 of the Directive 95/46/EC, DG XV, 1998

En conclusion, la souveraineté étatique apparaît alors comme une obligation mise à charge de l'Etat de garantir dans le cyberespace le respect des libertés individuelles de ses citoyens. Comme le note Wilkin[62], « *la souveraineté est une manifestation de liberté et d'indépendance par laquelle l'Etat impose la règle à ses nationaux et en exige le respect de la part des autres Etats. L'Etat dicte la volonté commune qu'il fait prévaloir contre les volontés particulières : il exprime à l'égard des nationaux et de l'étranger la souveraineté de la Belgique et veille à son respect. Vis-à-vis des autres Etats, la souveraineté est une manifestation d'indépendance ;…La souveraineté de l'Etat n'est pas en soi un point d'aboutissement ; elle est le moyen, pour les pouvoirs établis de pourvoir aux besoins des nationaux et d'assurer à ceux-ci et aux étrangers le libre exercice de leurs droits ; ».*

7.2. Le chiffrement

Tout chiffrement induit des coûts liés au choix de l'algorithme de chiffrement, à sa distribution, à la génération de clés sécurisées et au chiffrement/déchiffrement lui-même qui implique du temps de calcul et donc une lenteur dans la circulation de l'information. Même si un cryptage fort, combiné à l'utilisation de fibres optiques à chiffrement quantique, semble la voie royale menant à une sécurisation maximale des données, une telle solution ralentirait fortement le réseau et n'est pas envisageable partout dans le monde. Par ailleurs son coût risque d'être particulièrement élevé.

S'il incombe à l'opérateur de télécommunication de garantir la confidentialité des télécommunications, cette obligation générale est à mettre en balance avec l'état de la technique, le coût des solutions envisagées ainsi que la nature des informations à protéger. Par ailleurs, sous certaines conditions, l'opérateur de télécommunication doit pouvoir permettre le déchiffrement des messages aux services autorisés.

7.3. L'agréation des appareils terminaux

La directive 1999/5/CE du Parlement européen et du Conseil, du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité définit comme (art. 2 (b)) "équipement terminal de télécommunications", un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications. Un simple programme de navigation ou de courrier électronique ou encore un routeur peuvent donc être considérés comme équipements terminaux de télécommunication.

Dans son article 3 c (exigences essentielles), la même directive pose, que la Commission peut décider que les appareils relevant de certaines catégories d'équipements ou certains types d'appareils sont construits de sorte qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés. La commission Européenne possède donc là un instrument juridique contraignant et directement disponible.

---

(62) R . Wilkin, V° Souveraineté, Dictionnaire de droit public, Bruxelles, Bruylant, 1963.

7.4. Assigner de nouveaux objectifs à la Sûreté de l'état

Corollairement à ce qui se passe en Amérique[63], il conviendrait que la Sûreté de l'Etat et le SRG puissent conseiller et former en matière de sécurité des télécommunications les entreprises stratégiques qui le souhaitent.

7.5. Créer un organisme national de sécurité aux télécommunications.

Pour rappel, le groupe BELINFOSEC[64] avait produit, le 11 avril 1995, un document intitulé « *La sécurité des systèmes d'information, une préoccupation gouvernementale ?* » qui a été communiqué au Parlement ainsi qu'aux Ministres de la Justice et de la Défense Nationale le 25 juillet 1995.

Ce document recommandait : « *A l'instar des pays voisins, la Belgique devrait se doter d'une structure centrale de Sécurité des Systèmes d'Information qui, en collaboration avec les compétences existantes dans le pays, assumerait notamment les rôles suivants :*

- *réaliser les audits et l'évaluation des procédés de sécurité des systèmes d'information dans le secteur public ;*
- *déterminer les domaines d'application des procédés de cryptographie ;*
- *former les experts en sécurité du secteur public ;*
- *faire élaborer la réglementation et veiller à son respect ;*
- *favoriser le développement de la recherche et des compétences nationales dans ce domaine ;*
- *suivre les études de sécurité confiées par l'Administration à des entreprises privées.* »

Il nous semble toutefois que cette recommandation, écrite il y a cinq ans, devrait être réactualisée au regard de l'évolution rapide des télécommunications et des techniques d'écoute et, notamment, que le bénéfice d'une telle structure ne devrait pas être limité au seul secteur public

(63) « *The NSA/CSS INFOSEC mission provides leadership, products, and services to protect classified and unclassified national security systems against exploitation from interception, unauthorized access, or related technical intelligence threats* ». disponible sur http://www.nsa.gov/about_nsa/faqs_internet.html#overview.

(64) Ce groupe informel composé de scientifiques de haut niveau et de représentants de divers secteurs d'activité ne s'est plus réuni lors que la Belgique a libéralisé l'usage de la cryptographie. De plus amples informations sur ce groupe, sa structure et son fonctionnement se trouvent dans le rapport annuel 1995 du Comité R.

Cette structure pourrait par ailleurs avoir pour fonction l'établissement et la publication de standards cryptographiques qui pourraient alors être proposés, voire imposés, dans différents secteurs d'activité (banques, hôpitaux, administrations publiques, opérateurs de télécoms, …). Cette structure pourrait également établir des standards techniques d'interceptions légales des télécommunications par les services autorisés.

7.6. Les licences individuelles dans le secteur des télécommunications

La directive 97/13/CE[(65)] inscrit la protection des données dans la liste des « exigences essentielles ». Elle précise dans son art. 1d) que « *la protection des données peut comprendre la protection des données personnelles, la confidentialité des informations transmises ou stockées, ainsi que la protection de la vie privée* ». Il semble possible, sur base de cette directive, d'imposer la mise en place de certaines mesures de sécurité comme condition impérative à l'octroi d'une licence. Ceci est particulièrement pertinent dans le cas des opérateurs de mobilophonie, qui, selon Duncan Campbell, n'utiliseraient que 40 bits sur les 56 initialement prévus pour encrypter les télécommunications mobiles.

7.7. L'audit de la sécurité des télécommunications chez les opérateurs nationaux.

Cet audit nous semble une condition préalable à l'établissement de règles impératives à respecter en matière de cryptage des communications. Cet audit devrait être suffisamment technique pour pouvoir vérifier de manière certaine[(66)] et en présence d'experts la réalité ou l'absence de mesures de sécurité ainsi que leurs performances. En particulier, il y a lieu de vérifier si :

- les centraux numérique RNIS (ISDN) diffusés en Belgique ou certains d'entre eux permettent (et si oui, dans quels conditions) l'écoute des conversations dans une pièce, à l'aide d'un poste téléphonique raccroché.

- l'algorithme de chiffrement utilisé par les opérateurs de téléphonie mobile utilise un chiffrement à 40 bits ou à 56.

Cette phase préliminaire est indispensable à la mise en place de « bonnes » mesures de cryptage adéquates. En l'absence d'une telle étude il existe un risque important de prendre des mesures non performantes globalement, d'un coût excessif ou inhibant les écoutes légales.

---

(65) Directive 97/13/CE du Parlement Européen et du Conseil du 10 avril 1997 relative à un cadre commun pour les autorisations générales et les licences individuelles dans le secteur des services de télécommunications, JOCE, L117, mai 1997 (déjà cité supra 5.2.)

(66) pour ce faire il faut pouvoir observer le phénomène d'écoute et le reproduire. La loi sur les écoutes n'interdit pas le captage des conversations par leurs propres auteurs.

CONCLUSIONS ET RECOMMANDATIONS DU COMITE R.

Le Comité R se fonde sur les constatations des experts, Messieurs Poullet et Dinant pour conclure ce qui suit :

- **en ce qui concerne l'existence « d'Echelon » et ses activités :**

- quelle que soit la dénomination donnée à leurs systèmes (l'appellation « Echelon » n'apparaît jamais dans les documents officiels récents), il est évident que les Etats-Unis et la Grande Bretagne disposent de services officiels (la NSA et le GCHQ) chargés d'intercepter des télécommunications à des fins de sécurité, mais aussi « in the interest of the national well-beeing » (dans l' intérêt du bien-être national) des pays concernés ;

- les capacités techniques et en personnel de ces services sont énormes ;

- il existe des indices sérieux, mais aucune preuve certaine, que ces capacités d'écoutes peuvent être utilisées à des fins d'espionnage économique contre des pays de l'Union européenne ;

- les déclarations ambiguës des autorités américaines et britanniques à ce sujet ne permettent pas de lever le doute ;

- ainsi que le fait remarquer le journaliste américain James Bamford, qui est certain que la NSA n'outrepasse pas son mandat, « cela ne signifie pas qu'elle ne le fera jamais » ;

- les garanties pour le respect de la vie privée et les recours offerts par les législations américaine et britannique s'adressent uniquement aux citoyens de ces deux pays et non aux ressortissants des autres Etats ;

- **en ce qui concerne l'attitude des services de renseignement belges :**

- tant l'administrateur général a.i. de la Sûreté de l'Etat que le chef du SGR confirment que leurs services ne suivent pas le système « Echelon »; ils déclarent ne pas disposer des moyens humains et techniques nécessaires pour le faire ;

- la Sûreté de l'Etat n'a pas encore reçu d'instructions du Comité ministériel du Renseignement et de la sécurité en matière de protection du potentiel économique et scientifique ; elle n'a pas encore affecté de moyens importants à cette nouvelle mission ;

- ni l'espionnage économique, ni le système « Echelon » ne figurent à l'ordre du jour des rencontres entre représentants des services de renseignement européens ;

- le SGR déclare que l'espionnage militaire éventuel émanant de pays alliés à la Belgique ne constitue pas pour lui une priorité dans ses missions ;

- tant la Sûreté de l'Etat que le SGR regrettent de ne pas pouvoir procéder à des interceptions de sécurité dans un cadre légal ;

- le SGR travaille cependant avec l'hypothèse que les interceptions de communications existent réellement, et, quel que soit le pays qui les pratique, qu'il faut donc s'en prémunir ; le SGR considère également que n'importe quel système de chiffrement informatique est susceptible d'être cassé ;

- étant chargé de la sécurité des communications des forces armées, le SGR a élaboré différentes règles destinées à assurer la confidentialité des données classifiées transmises par télécommunication ou traitées par des réseaux informatiques ;

- le SGR suit de très près le développement de la législation en matière de cryptographie; il préconise qu'un organisme officiel soit chargé d'assurer la politique de sécurité de l'information en Belgique.

RECOMMANDATIONS

S'associant aux recommandations de MMS Poullet et Dinant, le Comité R recommande de surcroît :

- de considérer l'éventualité de systèmes d'interceptions de communications mis en œuvre par des pays étrangers à des fins contraires aux intérêts légitimes de la Belgique (notamment la protection du potentiel scientifique et économique) comme hautement vraisemblable, à défaut d'être prouvée ;
- de donner par conséquent comme mission aux services de renseignement belges de collaborer en vue de recueillir toute information disponible (de sources ouvertes et autres) sur la question ;
- de donner aux services de renseignement les moyens techniques et humains nécessaires pour accomplir cette mission (en leur permettant notamment de faire appel à des experts externes comme des informaticiens, des ingénieurs en télécommunications, des spécialistes en cryptographie, des analystes, etc …) ;
- de mettre en œuvre le principe général de précaution dans l'élaboration d'une politique globale et centralisée de sécurité de l'information ;
- d'envisager la mise en place d'un service chargé d'apporter une solution à l'ensemble de la problématique de la sécurisation de l'information.

LES DOCUMENTS « SOURCES ».

Les documents sur base desquels le présent rapport a été rédigé sont les suivants :

Documents du Parlement européen :

- Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control);

  - part 1/4 : the perception of economic risks arising from the potential vulnerability of electronic commercial media to interception (may 1999);

  - part 2/4 : the legality of the interception of electronic communications : a concise survey of the principal legal issues and intruments under international, european and national law (april 1999);

  - part 3/4 : encryption and cryptosytems in electronic surveillance : a survey of the technology assessment issues (april 1999);

  - part 4/4 : 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, and its applicability to COMINT targeting and selection, including speech recognition (april 1999);

  - vol 1/5 : 1) présentation des quatre études; 2) protection des données et Droit de l'Homme dans l'Union européenne et rôle du Parlement européen; (Octobre 1999) ;

  - vol 2/5 : 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, and its applicability to COMINT targeting and selection, including speech recognition (october 1999) – Duncan Campbell;

  - vol 3/5 : chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie (octobre 1999) – professeur Frank Leprévot;

  - vol 4/5 : the legality of the interception of electronic communications : a concise survey of the principal legal issues and intruments under international, european and national law (october 1999) – professeur Chris Elliot;

  - vol 5/5 : the perception of economic risks arising from the potential vulnerability of electronic