PARLEMENT EUROPÉEN

1999 *2004*

Commission temporaire sur le système d'interception ECHELON

PROVISOIRE

18 mai 2001

PROJET DE RAPPORT

sur l'existence d'un système d'interception mondial des communication privées et économiques (système d'interception ECHELON)

Commission temporaire sur le système d'interception ECHELON

Rapporteur: Gerhard Schmid

SOMMAIRE

Page

PAGE RÉGLEMENTAIRE

Par lettre du 5 juillet 2000, le Parlement européen a décidé de créer une commission temporaire sur le système d'intersection ECHELON. Au cours de sa réunion constitutive du 5 juillet 2000, la commission temporaire a nommé Gerhard Schmid rapporteur.

Au cours de ses réunions des ..., elle a examiné le projet de rapport.

Au cours de la dernière de ces réunions, elle a adopté la proposition de résolution par ... voix contre ... et ... abstention(s)/à l'unanimité.

Étaient présents au moment du vote ... (président(e)/président(e) f.f.), ... (vice-président(e)), ... (vice-président(e)), ... (rapporteur), ..., ... (suppléant ...), ... (suppléant ... conformément à l'article 153, paragraphe 2, du règlement), ... et ... .

Le rapport a été déposé le ....

Le délai de dépôt des amendements sera indiqué dans le projet d'ordre du jour de la période de session au cours de laquelle le rapport sera examiné/a été fixé au ... à ... heures.

PROPOSITION DE RÉSOLUTION

Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)

Le Parlement européen,

– vu la décision du Parlement européen du 5 juillet 2000, relative à la création d'une commission temporaire sur le système d'interception ECHELON, ainsi que le mandat de ladite commission,

– vu le traité CE, qui vise la mise en place d'un marché commun présentant un degré élevé de compétitivité,

– vu le traité sur l'Union européenne, en particulier l'article 6, paragraphe 2, de celui-ci, qui prévoit l'obligation de respecter les droits fondamentaux, ainsi que le titre V dudit traité, qui reprend les dispositions concernant une politique étrangère et de sécurité commune,

– vu la Charte des droits fondamentaux de l'UE, dont l'article 7 garantit le respect de la vie privée et familiale et prévoit le droit au respect des communications,

– vu la Convention européenne relative aux droits de l'homme, en particulier l'article 8 de celle-ci, qui protège la vie privée, ainsi que les nombreux autres traités internationaux qui protègent la vie privée,

– vu le rapport de la commission temporaire sur le système d'interception ECHELON (A5-..../2001),

en ce qui concerne l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)

A. considérant que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doutes; qu'il apparaît vraisemblable, eu égard aux indices disponibles, qu'il est dénommé ECHELON, cet aspect étant toutefois d'une importance secondaire,

B. considérant qu'il est utilisé pour intercepter des communications privées et économiques, mais non militaires, et que l'analyse menée dans le cadre du rapport a montré que la puissance de ce système ne peut être aussi grande, tant s'en faut, que ce que certains médias supposent,

en ce qui concerne les limites du système

C. considérant que le système de surveillance repose sur l'interception de communications par satellite, mais que, dans les régions à forte densité de communications, seule une très modeste partie des communications s'effectue par satellite; que la majeure partie des communications ne peuvent être interceptées par des stations au sol mais uniquement par branchement sur câble ou par écoute radio, ce qui, comme les investigations effectuées dans le cadre du rapport l'ont montré, n'est possible que dans des limites très étroites; que le personnel nécessaire pour analyser les communications interceptées détermine d'autres

limites, que les pays membres d'ECHELON n'ont, par conséquent, accès qu'à une partie très restreinte des communications par câble ou par radio et ne peuvent en évaluer qu'une partie limitée,

en ce qui concerne l'existence d'autres systèmes d'interception

D. étant donné que l'interception des communications est un moyen d'espionnage traditionnel des services de renseignements et qu'un tel système pourrait être exploité par d'autres pays à condition qu'ils disposent des moyens financiers et des conditions géographiques nécessaires, que la France serait en mesure, du moins en ce qui concerne les conditions géographiques – elle est en effet le seul État membre de l'UE à posséder des territoires outremer – de mettre sur pied à elle seule un système d'écoute mondial et qu'il ressort de certains indices que la Russie pourrait également exploiter un tel système,

en ce qui concerne la compatibilité avec le droit de l'UE

E. considérant que, s'agissant de la compatibilité d'un tel système avec le droit de l'UE, il y a lieu de distinguer deux cas: si ledit système n'est utilisé qu'à des fins de renseignements, il n'y a aucune contradiction avec le droit de l'UE, dans la mesure où les activités qui relèvent de la sécurité de l'État ne sont pas couvertes par le traité CE mais ne relèvent que des titres V du traité UE (PESC), qui ne contient encore aucune disposition en la matière, de sorte qu'une base fait défaut. En revanche, si le système est utilisé de manière abusive pour espionner la concurrence, il y a manquement à l'obligation de loyauté et atteinte à l'idée d'un marché commun où la concurrence est libre; si un État membre participe à une telle démarche, il viole le droit de l'Union,

en ce qui concerne la compatibilité avec le droit fondamental au respect de la vie privée (article 8 de la Convention relative aux droits de l'homme)

F. considérant que toute interception de communication constitue une atteinte grave à la vie privée, que l'article 8 de la Convention relative aux droits de l'homme, qui protège la vie privée, n'autorise que des ingérences destinées à sauvegarder la sécurité nationale, à condition que le droit national prévoie les dispositions afférentes, que celles-ci soient accessibles à tous et déterminent les circonstances et conditions d'intervention de la puissance publique, que les ingérences doivent en outre être proportionnées, ce qui suppose une mise en balance des intérêts, et que, en vertu de la jurisprudence de la Cour des droits de l'homme, il ne suffit pas qu'elles soient opportunes ou souhaitables,

G. considérant qu'un système de renseignements qui intercepterait les communications sans garantir le respect du principe de proportionnalité serait incompatible avec la Convention relative aux droits de l'homme, que, dans le même ordre d'idées, il y aurait violation de ladite Convention si les dispositions en vertu desquelles la surveillance des communications s'effectue sont dépourvues de base légale, si celle-ci n'est pas accessible à tous ou si elle est formulée de telle manière que la personne ne peut en appréhender les conséquences, que les dispositions sur la base desquelles des services de renseignements américains opèrent à l'étranger sont en grande partie confidentielles, de sorte que le respect du principe de proportionnalité est à tout le moins douteux et qu'il y a manquement au principe d'accès au droit et de prévisibilité de ses effets énoncé par la Cour des droits de l'homme,

H. considérant que les États membres ne peuvent se soustraire aux obligations qui leur incombent au titre de la Convention relative aux droits de l'homme en faisant intervenir sur leur territoire les services de renseignements d'autres pays soumis à des dispositions moins rigoureuses car cela reviendrait à priver de ses effets le principe de légalité et ses deux composantes – accès au droit et prévisibilité de ses effets – et viderait de sa substance la jurisprudence de la Cour des droits de l'homme,

I. considérant que la conformité des activités légales de services de renseignements avec les droits fondamentaux suppose en outre que soient prévus des systèmes de contrôle suffisants parant au risque que comporte l'action secrète d'une partie de l'administration; que la Cour européenne des droits de l'homme a souligné expressément l'importance d'un système de contrôle efficace dans le domaine des activités des services de renseignements, ce qui fait qu'il apparaît préoccupant que certains États membres ne disposent pas d'organe de contrôle parlementaire de leurs services secrets,

en ce qui concerne la question de savoir si les citoyens de l'UE sont suffisamment protégés face aux services de renseignements

J. considérant que la protection des citoyens de l'UE dépend des situations juridiques qui existent dans les États membres, lesquelles sont très différentes et, dans certains cas, caractérisées par l'absence d'organe de contrôle parlementaire, ce qui fait que l'on ne saurait parler de protection suffisante; que les citoyens européens tiennent absolument à ce que leurs parlements nationaux disposent d'un organe de contrôle dûment et spécialement structuré pour surveiller et contrôler les activités des services de renseignements; que, même dans les pays où il existe un organe de contrôle, la tentation est grande de s'intéresser davantage aux activités intérieures des services de renseignements qu'à leurs activités extérieures, étant donné que, normalement, les citoyens du pays ne sont concernés que dans le premier cas,

K. considérant qu'en cas de coopération entre services de renseignements dans le cadre de la PESC, les institutions seraient appelées à mettre en place des dispositions de protection suffisantes pour les citoyens européens,

en ce qui concerne l'espionnage économique

L. considérant qu'il relève des missions des services de renseignements à l'étranger de s'intéresser aux données économiques telles que développement de branches, évolution du marché des matières premières, respect d'embargos, respect des dispositions relatives à l'approvisionnement en biens à usage mixte, etc., et que c'est la raison pour laquelle les entreprises exerçant des activités dans ces domaines sont fréquemment surveillées,

M. considérant qu'il est toutefois intolérable que des services de renseignements soient utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales, mais qu'il n'est pas prouvé, même si cela est souvent avancé, que le système d'interception mondial soit utilisé à cette fin,

N. considérant que les données sensibles se trouvent principalement à l'intérieur des entreprises, de sorte que l'espionnage consiste principalement à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées ou encore en pénétrant dans les réseaux informatiques, que ce n'est que lorsque les données sensibles sont acheminées vers l'extérieur par câble ou par radio (satellite), qu'un système de surveillance des communications peut être utilisé pour espionner, trois cas pouvant se présenter:

– entreprises travaillant dans trois zones horaires, de sorte que les résultats intérimaires

peuvent être envoyés d'Europe en Amérique puis en Asie,

– vidéoconférences d'entreprises multinationales se déroulant par satellite ou par câble,

– négociations de marchés importants sur place (construction d'usines, d'infrastructures de télécommunications, de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place,

en ce qui concerne les possibilités de protection

O. considérant que la sécurité des entreprises ne peut être assurée qu'en protégeant l'ensemble de l'environnement de travail ainsi que tous les moyens de communication servant à transmettre des informations sensibles, que les systèmes de cryptage sûrs à prix abordable sont suffisamment nombreux sur le marché européen, que les particuliers doivent, eux aussi, être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe, que, sur Internet, on trouve des systèmes conviviaux qui sont mis à la disposition des particuliers, parfois même gratuitement,

en ce qui concerne la coopération entre services de renseignements de l'UE

P. considérant que l'UE est convenue de coordonner la collecte du renseignement dans le cadre du développement d'une politique de sécurité et de défense tout en poursuivant la coopération avec d'autres partenaires dans ces domaines,

Q. considérant qu'une coopération entre services de renseignements de l'UE apparaît souhaitable car, d'une part, une politique commune de sécurité excluant les services secrets serait absurde et, d'autre part, cela comporterait de nombreux avantages d'ordre professionnel, financier et politique, que cela serait en outre conforme à l'idée d'un partenarait à égalité de droits avec les États-Unis et pourrait regrouper l'ensemble des États membres au sein d'un système mis sur pied dans le respect de la Convention des droits de l'homme; qu'un contrôle par le Parlement européen devrait, dans ce cas, être assuré,

R. considérant que le Parlement européen est sur le point de se doter de dispositions relatives à l'accès aux informations et documents confidentiels et sensibles,

en ce qui concerne la conclusion et la modification de traités internationaux en matière de protection des citoyens et des entreprises

1. invite le Secrétaire général du Conseil de l'Europe à proposer au comité des ministres de déterminer s'il serait opportun d'adapter la protection de la vie privé garantie à l'article 8 de la Convention relative aux droits de l'homme aux méthodes de communication et aux possibilités d'interception modernes, et ce dans un protocole additionnel ou dans le contexte de la réglementation relative à la protection des données, dans le cadre d'une révision de la Convention afférente, étant entendu que cela ne saurait déboucher sur un abaissement du niveau de protection assuré par la Cour des droits de l'homme ni sur une réduction de la souplesse nécessaire pour suivre l'évolution;

2. invite les États membres à mettre en place une plateforme européenne appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications, à

se mettre d'accord sur un texte commun garantissant la protection de la vie privée, telle qu'elle est définie à l'article 7 de la Charte européenne des droits fondamentaux, à tous les citoyens européens sur le territoire des États membres et garantissant en outre que les activités des services de renseignements s'effectuent dans le respect des droits fondamentaux et, partant, des conditions énoncées au chapitre 8 du rapport, en particulier du point 8.3.4, en vertu de l'article 8 de la Convention relative aux droits de l'homme;

3. invite les États membres du Conseil de l'Europe à adopter un protocole additionnel permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme ou d'envisager d'autres moyens d'éviter les conflits de jurisprudence entre la Cour européenne des droits de l'homme et la Cour de justice européenne;

4. invite le Secrétaire général des Nations unies à charger l'organe compétent de l'Organisation de présenter des propositions visant à adapter l'article 17 de la Convention internationale relative aux droits civils et politiques, qui garantit la protection de la vie privée, aux innovations techniques;

5. invite les États-Unis à signer le protocole additionnel à la Convention internationale relative aux droits civils et politiques afin de rendre possibles, en cas de violation, les recours individuels devant la commission des droits de l'homme prévue par la Convention; invite les ONG américaines compétentes, notamment l'ACLU (American Civil Liberties Union) et l'EPIC (Electronic Privacy Information Center) à faire pression en ce sens sur le gouvernement américain;

en ce qui concerne l'action législative nationale en matière de protection des citoyens et des entreprises

6. invite les États membres à vérifier la conformité aux droits fondamentaux de leur législation relative aux activités des services de renseignements;

7. invite les États membres à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements en fonction du niveau de protection national le plus élevé, les citoyens concernés par les activités d'un service de renseignements étranger appartenant généralement à un autre pays, c'est-à-dire aussi à un autre État membre;

8. invite les institutions de l'UE, en cas de coopération entre services de renseignements dans le cadre de la PESC, à prévoir des garanties suffisantes pour les citoyens européens; le Parlement européen, organe de contrôle tout indiqué, doit, d'une part, créer les conditions nécessaires à la surveillance de ce domaine très sensible pour qu'il soit réaliste et responsable de réclamer les pouvoirs de contrôle nécessaires;

en ce qui concerne les mesures de lutte contre l'espionnage économique

9. invite les États membres à examiner si des dispositions du droit européen et international permettraient de lutter contre l'espionnage économique et la corruption visant à obtenir des marchés, notamment si une réglementation dans le cadre de l'OMC serait possible, qui tiendrait compte des distorsions de concurrence causées par de telles pratiques, par exemple en prévoyant la nullité de tels marchés;

10. invite les États membres à s'engager, dans une déclaration commune, à ne pas pratiquer l'espionnage économique entre eux, proclamant ainsi le respect de l'esprit et de la lettre du traité CE;

en ce qui concerne l'application du droit et le contrôle de celle-ci

11. lance un appel aux parlements nationaux qui ne disposent pas d'organe de contrôle parlementaire des services de renseignements pour qu'ils se dotent d'un tel organe;

12. invite les organes de contrôle nationaux des services secrets à accorder une grande importance, dans l'exercice de leur pouvoir de contrôle, à la protection de la vie privée, que la surveillance concerne les ressortissants nationaux, les citoyens d'autres États membres de l'UE ou ceux de pays tiers;

13. invite l'Allemagne et le Royaume-Uni à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité, que la base juridique soit accessible et que les effets soient prévisibles pour les personnes et qu'un contrôle efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire;

en ce qui concerne la promotion de la protection des citoyens et des entreprises

14. invite la Commission et les États membres à élaborer des programmes de sensibilisation des citoyens et des entreprises aux problèmes de sécurité et, simultanément, à offrir une aide pratique pour la conception et la mise en œuvre de formules de protection globale;

15. invite la Commission et les États membres à élaborer des mesures de promotion, de développement et de fabrication de matériels et de logiciels de cryptage européens et surtout à soutenir les projets visant à développer des logiciels de cryptage conviviaux dont le texte-source soit publié;

16. invite la Commission et les États membres à promouvoir des projets de logiciels dont le texte-source soit publié, étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de "backdoors" ("open-source software");

17. invite les institutions européennes et les administrations publiques des États membres à recourir systématiquement au cryptage du courrier électronique afin de faire de celui-ci la règle, à terme;

en ce qui concerne d'autres démarches

18. invite les entreprises à coopérer davantage avec les services de contre-espionnage, à leur signaler les attaques extérieures relevant de l'espionnage économique, afin d'accroître leur efficacité;

19. invite la Commission à proposer la création d'un service de conseil européen en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;

20. estime opportun d'organiser un colloque non limité à l'Union sur la protection de la vie privée face à la surveillance des télécommunications afin de créer une plateforme permettant aux ONG d'Europe, des États-Unis et d'autres pays d'examiner les aspects transfrontaliers et

internationaux et de coordonner les activités et démarches;

21. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission, aux gouvernements et aux parlements des États membres, ainsi qu'aux pays candidats à l'adhésion et au Conseil de l'Europe.

EXPOSÉ DES MOTIFS

1. Introduction

1.1. Motif de la constitution de la commission

Le 5 juillet 2000, le Parlement a décidé de constituer une commission temporaire sur le système ECHELON. À la base de sa décision, le débat auquel donnait lieu l'étude que le STOA[1] avait commandée sur le système appelé ECHELON[2] et que son auteur, Duncan Campbell, avait présentée à l'occasion d'une audition de la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures ayant pour thème l'Union européenne et la protection des données.

1.2. Affirmations formulées dans les deux études du STOA sur un système d'interception mondial appelé ECHELON

1.2.1. Premier rapport du STOA de 1997

Dans un rapport ayant pour thème l'évaluation des techniques de contrôle politique, dont le STOA[3] avait, au nom du Parlement européen, confié en 1997 la réalisation à la Fondation Omega, une description du système ECHELON est aussi proposée au chapitre "Réseaux nationaux et internationaux d'interception des communications". L'auteur de l'étude y affirme que toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la NSA (Service américain de renseignement extérieur)[4]. Ce rapport a attiré l'attention de toute l'Europe sur l'existence d'ECHELON, réputé être un système d'interception polyvalent à l'échelle mondiale.

1.2.2. Rapports du STOA de 1999

Pour en apprendre davantage sur ce thème, le STOA commanda en 1999 une étude en cinq parties, portant sur le développement des techniques de surveillance et les risques d'utilisation abusive d'informations économiques. Le volume 2/5, qui est de la main de Duncan Campbell, est consacré à l'étude des capacités de renseignement actuelles et en particulier du fonctionnement d'ECHELON[5].

Une affirmation contenue dans ce rapport devait susciter un émoi particulier: ECHELON ne poursuivrait plus l'objectif qui était le sien au départ, à savoir la défense contre l'Est, et serait désormais un instrument d'espionnage économique. Cette thèse est étayée dans le rapport par des

[1] STOA (Évaluation des choix scientifiques et techniques), service de la Direction générale des études du Parlement européen qui confie des travaux de recherche à l'extérieur.
[2] The state of art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepting broadband multilanguage leased or common carrier system, and its applicability to COMINT argeting and selection, including speech recognition (octobre 1999).
[3] Évaluation des choix scientifiques et techniques.
[4] Steve Wright, Une évaluation des techiques de contrôle politique (1998), p. 20.
[5] Manfred Fink, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart 1996.

exemples d'espionnage économique présumés, qui auraient été la cause de préjudices notamment pour Airbus et Thomson CFS.

À la suite de l'étude du STOA, ECHELON a fait l'objet de discussions dans quasiment tous les parlements des États membres; en France et en Belgique, des rapports ont même été établis à ce sujet.

1.3. Mandat de la commission

Par sa décision portant constitution d'une commission temporaire, le Parlement européen a également fixé son mandat. Aux termes de celui-ci, la commission temporaire est chargée de:

" - vérifier l'existence du système d'interception des communications connu sous le nom d'Echelon et dont l'activité est décrite dans le rapport STOA sur le développement des technologies de surveillance et le risque d'abus d'informations économiques;

- vérifier la compatibilité d'un tel système avec le droit communautaire, en particulier l'article 286 du traité CE et les directives 95/46/CE et 97/66/CE, et avec l'article 6, paragraphe 2, du traité sur l'Union européenne, sur la base des questions suivantes:

- les droits des citoyens européens sont-ils protégés contre les activités des services secrets ?

- le cryptage constitue-t-il une protection adéquate et suffisante pour protéger la vie privée des citoyens ou faut-il prendre des mesures complémentaires et, dans l'affirmative, de quel ordre ?

- comment renforcer la prise de conscience des institutions européennes à l'égard des risques suscités par ces activités, et quelles mesures peut-on prendre ?

- vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne,

- proposer, le cas échéant, des initiatives politiques et législatives."

1.4. Pourquoi n'avoir pas opté pour une commission d'enquête?

Si le Parlement européen opta donc pour la constitution d'une commission temporaire, c'est que la constitution d'une commission d'enquête n'est possible qu'aux fins d'examiner des violations du droit communautaire dans le cadre du traité CE (article 193 TCE) et que dès lors, une commission d'enquête ne peut se saisir que des matières qui y sont visées. Les domaines qui ressortissent au titre V (PESC) et au titre VI TUE (Coopération policière et judiciaire en matière pénale) sont exclus. De plus, selon la décision interinstitutionnelle[6], une commission d'enquête ne peut exercer les droits spécifiques qui sont les siens en matière d'audition et de consultation des dossiers que dans le cas où des motifs de secret ou de sécurité publique ou nationale ne s'y opposent pas, ce qui empêche d'inviter des membres des services secrets à comparaître. De même, une commission d'enquête ne peut étendre ses travaux à des pays tiers, dès lors que, par définition, ceux-ci ne peuvent violer le droit de l'Union européenne. Comme la constitution d'une

[6] Décision du Parlement européen, du Conseil et de la Commission, du 19 avril 1995, portant modalités d'exercice du droit d'enquête du Parlement européen (95/167/CE, Euratom, CECA), art. 3, paragraphes 3, 4 et 5.

commission d'enquête aurait impliqué des des limites quant au travail de fond, sans donner des droits supplémentaires, la majorité des députés au Parlement européen a rejeté cette solution.

1.5. Méthode et plan de travail

Pour pouvoir exercer pleinement et entièrement son mandat, la commission a opté pour la procédure suivante. Un programme de travail, proposé par votre rapporteur et adopté par la commission, dressait une liste des grands thèmes concernés:

1. connaissances sûres relatives à ECHELON,
2. discussion dans les parlements et gouvernements nationaux,
3. services de renseignement et activités de ceux-ci,
4. systèmes de communication et possibilité de les intercepter,
5. cryptage,
6. espionnage économique,
7. objectifs de l'espionnage et mesures de protection, et
8. cadre juridique et protection de la sphère privée.

Ces thèmes ont ensuite été étudiés au cours de différentes réunions, l'ordre de leur examen étant dicté par des points de vue pratiques et non par la plus ou moins grande importance attachée à chacun d'eux. Pour préparer chacune des réunions, votre rapporteur a consulté et exploité de façon systématique la documentation existante. Compte tenu des nécessités liées à l'examen du point concerné, furent invités aux différentes réunions des représentants des administrations nationales (et notamment des services secrets) ainsi que des parlements nationaux, qui sont les organes de contrôle des services secrets, tout comme des experts juridiques et des experts dans les domaines des techniques de communication et d'interception, de la sécurité des entreprises et des techniques de cryptage, experts appartenant tant au monde scientifique qu'au monde des affaires. Des journalistes qui avaient effectué des travaux de recherche sur ce thème furent également invités. En règle générale, les réunions étaient publiques, ce qui n'empêche que le huis clos a également été décidé, quand il pouvait être utile pour obtenir des informations. De plus, le président de la commission et votre rapporteur se sont rendus, ensemble, à Londres et à Paris, pour y rencontrer des personnes, qui, pour différentes raisons, ne pouvaient pas participer aux réunions de la commission, mais qu'il semblait toutefois utile d'associer aux travaux de celle-ci. Pour les mêmes raisons, le bureau de la Commission, les coordinateurs et votre rapporteur se sont rendus aux États-Unis. Par ailleurs, votre rapporteur a également eu de nombreux entretiens individuels, parfois confidentiels.

1.6. Caractéristiques attribuées au système ECHELON

Le système désigné sous le nom de code "ECHELON", se distingue des autres systèmes de renseignement par le fait qu'il présente deux caractéristiques lui conférant un niveau de qualité tout particulier.

La première qu'il est réputé avoir, c'est la capacité d'exercer une surveillance pour ainsi dire totale. Par l'intermédiaire surtout de stations de réception satellitaire et de satellites–espions, toute communication d'une personne transportée sur n'importe quel support – téléphone, téléscripteur, réseau Internet ou courrier électronique – peut être interceptée aux fins de prendre connaissance de son contenu.

La deuxième, c'est que le système "ECHELON" exerce ses activités à l'échelle planétaire grâce à la coopération de plusieurs États (Royaume-Uni, États-Unis, Canada, Australie et Nouvelle-Zélande), ce qui constitue un plus par rapport aux systèmes nationaux: les pays parties au système ECHELON (pays ECHELON) peuvent se partager l'utilisation de leurs installations d'interception, les tâches en résultant et les renseignements obtenus. Cette coopération internationale est justement essentielle pour la surveillance à l'échelle mondiale des communications par satellite, car elle seule permet, dans les communications internationales, d'intercepter les deux parties d'une conversation. Il est parfaitement évident que compte tenu de leurs dimensions, des stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment. L'accord réciproque et la coopération – dans une mesure plus ou moins grande – de plusieurs pays situés en différents points du monde est en l'occurrence indispensable.

Les risques que pourrait présenter, pour la sphère privée et les milieux économiques, un système du type ECHELON ne résultent pas uniquement du très grand potentiel de ce système de surveillance, mais procèdent bien davantage du fait qu'il fonctionne dans un espace qui échappe, pour l'essentiel, à toute règle juridique. Un système d'interception des communications internationales ne vise pas la plupart du temps les habitants du pays qui l'exploite. De par son statut d'étranger, la personne dont les messages sont interceptés ne dispose ainsi d'aucune protection juridique intérieure. Aussi, l'individu est-il entièrement à la merci du système. Dans ce domaine, le contrôle parlementaire est également insuffisant, dès lors que les électeurs, qui partent du principe qu'ils ne sont pas concernés et que "seules" sont concernées des personnes à l'étranger, ne manifestent pas un intérêt particulier pour cette question, et que pour les élus, ce qui compte avant tout, ce sont les intérêts de leurs électeurs. Aussi ne faut-il pas s'étonner que les auditions sur les activités de la NSA, qui ont eu lieu au sein du Congrès américain, aient porté uniquement sur la question de savoir si des citoyens américains étaient également victimes de ce système, dont l'existence même n'a pas suscité de véritables réserves. Il est dès lors d'autant plus nécessaire d'engager un débat en la matière à l'échelle européenne.

2. Activité des services de renseignements extérieurs

2.1. Introduction

Pour garantir la sécurité de l'État, la plupart des gouvernements font appel non seulement à la police mais aussi aux services de renseignement. Ceux-ci, dès lors que leur activité est, la plupart du temps, secrète, sont également appelés services secrets. Ces services ont pour mission:

– de recueillir des informations permettant de parer à tout danger pour la sécurité de l'État,
– de se livrer, en règle générale, au contre-espionnage,
– de parer aux risques susceptibles de menacer les forces armées, et
– de recueillir des informations sur des développements à l'étranger.

2.2. Que faut-il entendre par espionnage?

Pour les gouvernements, il est essentiel de recueillir et d'exploiter de façon systématique des informations sur certains développements dans d'autres pays. Ce qu'ils recherchent en l'occurrence, ce sont des bases pour des décisions à prendre dans le domaine des forces armées, de la politique étrangère, etc. Aussi se sont-ils dotés de services de renseignement extérieur. Dans un premier temps, ces services s'emploient à exploiter systématiquement des sources d'information librement accessibles. D'après ce qui lui a été dit, votre rapporteur considère que cette activité représente en moyenne au moins 80 % de l'activité des services de renseignement[7]. Il n'empêche que des informations particulièrement importantes dans ces domaines sont tenues secrètes par les gouvernements ou les entreprises, et que chacun n'y a donc pas accès. Celui qui veut pourtant se les approprier, il doit les voler. L'espionnage n'est rien d'autre que le vol organisé d'informations.

2.3. Objectifs de l'espionnage

Les objectifs classiques de l'espionnage sont les secrets militaires, les secrets d'autres gouvernements ou des informations concernant la stabilité des gouvernements ou les risques auxquels ils sont exposés. Sont visés, par exemple, les nouveaux systèmes d'armement, les stratégies militaires, ou des informations concernant le stationnement des troupes. Non moins importantes sont les informations relatives à des décisions imminentes en matière de politique étrangère, les décisions monétaires ou les informations d'initiés concernant des tensions au sein d'un gouvernement. Parallèlement, un intérêt est également manifesté pour des informations importantes du point de vue économique, qui peuvent être non seulement des informations sectorielles mais aussi des renseignements précis sur de nouvelles technologies ou des contrats avec l'étranger.

[7] Dans son rapport "Preparing for the 21st Century: An Appraisal of U.S. Intelligence", la "Commission on the Roles and Capabilities of the US Intelligence Community" constate que 95 % de tous les renseignements d'ordre économique proviennent de sources publiques (chapitre 2 "The Role of intelligence").

2.4. Méthodes de l'espionnage

L'espionnage signifie se procurer un accès à des informations que leur propriétaire souhaite justement préserver de la curiosité des tiers. Aussi faut-il venir à bout de cette protection et la jeter bas. Il en va exactement ainsi pour l'espionnage politique comme pour l'espionnage économique. C'est pourquoi l'espionnage dans ces deux secteurs pose les mêmes problèmes et les mêmes techniques d'espionnage sont mises en œuvre. Du point de vue logique, il n'y a pas de différence, hormis le niveau de protection, qui est dans le monde économique la plupart du temps moindre, ce qui explique que l'espionnage économique se révèle souvent plus simple. La conscience du risque auquel expose l'utilisation de communications pouvant être interceptées est notamment moins nette dans le milieu économique que celle de l'État dans les domaines ressortissant à la sécurité.

2.4.1. Recours à l'être humain dans l'espionnage

La protection des informations secrètes se conçoit toujours de la même façon:

- le nombre de personnes, jugées sûres, ayant accès aux informations secrètes est limité;
- des prescriptions strictes régissent l'usage de ces informations;
- normalement, les informations ne sortent pas du secteur protégé, et si elles le font toutefois, c'est uniquement de façon sûre ou en étant codées. Aussi l'espionnage organisé s'attache-t-il tout d'abord à obtenir, par l'intermédiaire de **personnes** (ce qu'il est convenu d'appeler le renseignement humain), un accès direct et sans détour aux informations souhaitées. Il peut s'agir en l'occurrence:
    - de membres infiltrés (agents) du service/de l'entreprise, ou
    - de personnes recrutées au sein de la cible.

Ces dernières personnes travaillent pour des services/entreprises étrangers la plupart du temps pour les raisons suivantes:

- sexualité,
- corruption par l'argent ou par des positions lucratives,
- chantage,
- convictions idéologiques,
- conquête d'un statut ou d'un honneur particulier (appel au mécontentement ou sentiment d'infériorité).

Il existe un cas limite, celui de la coopération involontaire par "écumage". En l'occurrence, des collaborateurs d'autorités ou d'entreprises sont incités, en flattant leur vanité, et ce dans des conditions apparemment innocentes (conversations en marge de conférences, à l'occasion de congrès spécialisés, au bar d'un hôtel), à bavarder.

L'utilisation de personnes présente l'avantage d'offrir un accès direct aux informations souhaitées. Cette solution ne va toutefois pas sans inconvénients:

- l'attention du contre-espionnage se porte toujours sur les personnes ou les agents dirigeants;
- dans le cas de personnes recrutées, les points faibles qui ont incité à les recruter peuvent avoir un effet de boomerang;
- les personnes peuvent toujours commettre des erreurs et se retrouver donc, à un moment ou l'autre, prises dans les mailles du contre-espionnage.

Dès lors, on s'efforce, là où c'est possible, de substituer à l'utilisation d'agents ou de personnes recrutées un espionnage anonyme et non personnel. La solution la plus simple consiste à

exploiter les signaux hertziens d'installations ou de véhicules possédant une importance au point de vue militaire.

2.4.2. Exploitation des signaux électromagnétiques

Pour l'opinion publique, la forme la plus connue de l'espionnage par des moyens techniques, c'est l'utilisation de la photographie par satellite. Néanmoins, il existe parallèlement une interception et une exploitation des signaux électromagnétiques, quelle qu'en soit la nature (SIGINT, ou mesure de renseignement électronique).

2.4.2.1. Signaux électromagnétiques ne servant pas aux communications

Certains signaux électromagnétiques, par exemple, les rayonnements produits par les stations radar, peuvent, dans le domaine militaire, fournir des informations précieuses sur l'organisation de la défense aérienne d'un opposant (ELINT, ou mesure de recherche électronique). De plus, les rayonnements électromagnétiques qui fournissent des indications sur la position des troupes, des avions, des bateaux ou des sous-marins, constituent une source d'information très utile pour un service de renseignement. De même, l'observation des satellites-espions d'autres pays, qui prennent des photos, et l'enregistrement ainsi que le décodage des signaux de ces satellites ne sont pas sans intérêt.

Les signaux sont captés par des stations fixes, des satellites sur orbite basse ou des satellites SIGINT quasi géostationnaires. Cette partie de l'activité des services secrets touchant aux signaux électromagnétiques absorbe, quantitativement, une partie importante des capacités d'interception des services, les possibilités techniques n'étant cependant pas pour autant épuisées.

2.4.2.2. Exploitation des communications interceptées

Les services de renseignement extérieur de nombreux pays interceptent les communications militaires et diplomatiques d'autres pays. Bien de ces services surveillent également, dans la mesure où ils y ont accès, les communications civiles d'autres pays. Dans certains pays, les services ont le droit de surveiller également les communications qui pénètrent sur le territoire national ou qui en sortent. Dans les démocraties, la surveillance des communications du **ressortissant national** par les services de renseignement est subordonnée à certaines conditions d'intervention et à certains contrôles. Les juridictions nationales ne protègent toutefois que le citoyen qui se trouve sur son propre territoire. (cf. chapitre 8).

2.5. Activité de certains services de renseignements

C'est surtout l'activité d'interception des services de renseignement américain et britannique qui a déclenché le débat public. Les critiques visent l'ouverture et l'exploitation des communications (téléphonie vocale, téléscripteur, courrier électronique). Pour pouvoir émettre un jugement **politique**, il faut une aune permettant de juger cette activité. Un critère de comparaison peut être l'activité d'interception des services de renseignement extérieurs dans l'Union européenne. Le tableau 1 ci-après expose de façon succincte la situation. Il démontre que l'interception des communications privées par les services de renseignement extérieur n'est pas propre aux seuls services américain et britannique.

Pays	Communications extérieures	Communication publiques	Communications privées
Belgique	+	+	-
Danemark	+	+	+
Finlande	+	+	+
France	+	+	+
Allemagne	+	+	+
Grèce	+	+	-
Irlande	-	-	-
Italie	+	+	+
Luxembourg	-	-	-
Pays-Bas	+	+	+
Autriche	+	+	-
Portugal	+	+	-
Suède	+	+	+
Espagne	+	+	+
Royaume-Uni	+	+	+
États-Unis	+	+	+
Canada	+	+	+
Australie	+	+	+
Nouvelle-Zélande	+	+	+

Tableau 1: Activités d'interception des services de renseignement dans l'Union européenne et dans les pays ECHELON

Signification des différentes colonnes:

1re colonne: pays concerné
2e colonne: interception des communications extérieures
3e colonne: interception des communications publiques (militaires, diplomatiques, etc.)
4e colonne: interception des communications privées

3. Conditions techniques minimales requises pour l'interception des télécommunications

3.1. Possibilité d'interception des différents supports des télécommunications

Lorsque deux personnes se trouvant à une certaine distance l'une de l'autre souhaitent communiquer entre elles, elles ont besoin d'un support de communication, qui peut être:

– l'air (son),
– la lumière (clignotant morse, câble à fibres optiques),
– l'électricité (télégraphe, téléphone),
– une onde électromagnétique (la radio sous ses formes différentes).

Le tiers qui s'assure un accès au support de la communication peut intercepter celle-ci. L'accès peut être aisé ou compliqué, possible de partout ou uniquement à partir de certaines positions. Ci-après, deux cas extrêmes sont examinés: les possibilités techniques pour un espion sur place, d'une part, et les possibilités pour un système d'interception fonctionnant à l'échelle mondiale, d'autre part.

3.2. Possibilités d'interception sur place[8]

Sur place, toute communication peut être interceptée, pour autant que l'espion soit résolu à commettre une infraction et que la victime de l'interception ne se protège pas.

– Dans des locaux, les **conversations** peuvent être interceptées en dissimulant des microphones (des mouchards) ou en analysant au moyen d'un laser les vibrations d'une fenêtre.

– Les **écrans** émettent des rayons qui peuvent être captés jusqu'à une distance de 30 m; ce qui apparaît sur l'écran est ainsi visible.

– Les **téléphones, téléscripteurs et courriers électroniques** peuvent être interceptés, si l'espion se branche sur le câble sortant du bâtiment.

– Un **téléphone portable** peut être intercepté jusqu'à une distance pouvant atteindre … km.

– Un **émetteur de radio interne** peut être intercepté dans la limite des ondes radio ultracourtes.

Sur place, les conditions d'utilisation des moyens techniques d'espionnage sont idéales, dès lors que les mesures d'interception peuvent être limitées à une seule personne cible ou à un seul objet cible, et qu'il est possible de capter pratiquement toute communication. Le seul inconvénient,

[8] Manfred Fink, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag Stuttgart, 1996.

c'est un certain risque de découverte, qui n'existe cependant que dans le cas du placement de "mouchards" ou du branchement sur le câble sortant du bâtiment.

3.3. Possibilités d'un système d'interception fonctionnant à l'échelle mondiale

Aujourd'hui, il existe, pour les communications intercontinentales, différents supports pour tous les types de communications (voix, fax et données). Les possibilités d'un système d'interception fonctionnant à l'échelle mondiale sont limitées par deux facteurs:

– l'accès limité au support de la communication,
– la nécessité de filtrer les communications intéressantes dans une masse gigantesque de communications effectuées.

3.3.1. Accès aux supports des télécommunications

3.3.1.1. Communications tributaires du câble

Le câble sert à acheminer toutes sortes de communications (voix, fax, courrier électronique, données). Les communications tributaires du câble ne peuvent être interceptées que dans le cas où un accès au câble est possible. Dans tous les cas, un accès est possible au point d'arrivée d'une liaison par câble, si celui-ci se situe sur le territoire de l'État qui fait procéder à l'interception. À l'intérieur des frontières d'un pays, toutes les communications par câble peuvent donc, **technique parlant**, être interceptées, à partir du moment où l'interception est autorisée par la justice. Les services de renseignement n'ont toutefois pas, la plupart du temps, un accès légal, aux câbles sur le territoire d'autres pays. Bien entendu, ils peuvent s'assurer, de façon tout à fait illégale, un accès ponctuel, en s'exposant à un grand risque de découverte.

À l'époque du télégraphe, les liaisons intercontinentales par câble avaient pour support des câbles sous-marins. Un accès à ces câbles est toujours possible là où ils ressortent de l'eau. Si plusieurs États exploitent en commun un réseau d'interception, alors, un accès est possible à toutes les extrémités des câbles sur le territoire de ces États. Historiquement, cela n'a pas été sans importance, les câbles télégraphiques sous-marins et les premiers câbles téléphoniques coaxiaux sous-marins entre l'Europe et l'Amérique ressortant de la mer à Terre-Neuve (Canada) et les liaisons avec l'Asie s'effectuant via l'Australie, des amplificateurs intermédiaires étant nécessaires. Aujourd'hui, les câbles à fibres optiques – qui peuvent être posés quel que soit le relief sous-marin – se voient équiper des amplificateurs intermédiaires nécessaires, ce qui permet un acheminement direct, c'est-à-dire sans relais en Australie ou en Nouvelle-Zélande.

S'agissant des câbles électriques, il est également possible de faire, entre les extrémités d'une liaison, un branchement par induction (c'est-à-dire par un procédé électromagnétique dans lequel une bobine est disposée sur le câble), sans réaliser une liaison électroconductrice directe. Cette technique peut également mise en œuvre, non sans lourdes dépenses, au départ des sous-marins, dans le cas de câbles électriques sous-marins. Les États-Unis y ont eu recours pour se brancher sur un certain câble sous-marin soviétique, par lequel des ordres non codés étaient transmis aux sous-marins atomiques. Une telle technique ne saurait être généralisée, ne serait-ce qu'en raison de son coût.

Dans le cas des câbles à fibres optiques de l'ancienne génération actuellement utilisés, un branchement par induction n'est possible qu'au niveau des amplificateurs intermédiaires. Ceux-ci transforment le signal optique en un signal électrique, l'amplifient et le retransforment ensuite en un signal optique. Se pose toutefois la question de savoir comment la quantité gigantesque de

données qui est transportée par un tel câble pourrait bien être acheminée entre le lieu de son interception et celui de son exploitation sans mettre en place un autre câble à fibres optiques. L'utilisation d'un sous-marin équipé des dispositifs techniques d'exploitation ne peut être envisagée, en raison des dépenses, que dans des cas extrêmement rares. Par exemple, en cas de guerre, le but étant d'intercepter les communications militaires et stratégiques de l'ennemi. S'agissant de la surveillance quotidienne des télécommunications internationales, l'utilisation d'un sous-marin est, de l'avis de votre rapporteur, exclue. Dans les câbles à fibres optiques de la dernière génération, l'amplificateur intermédiaire est un laser à l'erbium, et ce type d'amplificateurs ne permet plus un branchement électromagnétique aux fins de l'interception. Pour de tels câbles à fibres optiques, l'interception n'est possible qu'aux extrémités de la liaison.

Dans la pratique, cela signifie, pour le réseau d'interception des **pays ECHELON**, que ces pays ne pourraient, sans s'exposer à des dépenses déraisonnables, procéder à des interceptions qu'aux extrémités des câbles sous-marins, se trouvant sur leur territoire. En résumé, ils ne peuvent intercepter que les communications tributaires du câble aboutissant chez eux ou partant de chez eux! Ce qui signifie qu'**en Europe**, l'accès à la communication par câble à l'entrée et à la sortie du territoire n'est possible que sur **le territoire du Royaume-Uni!** Car, jusqu'ici, les communications intérieures continuent, la plupart du temps, à être acheminées par le réseau câblé intérieur; la privatisation des télécommunications peut générer des exceptions, mais celles-ci sont partielles et non prévisibles!

Tel est à tout le moins le cas pour le téléphone et le téléscripteur. Pour les communications internet via le câble, la situation est différente. Sans trop s'étendre, il est possible de formuler les observations de nature restrictive suivantes:

- dans le réseau internet, les communications s'effectuent par paquets de données, des paquets adressés à un destinataire pouvant suivre différents itinéraires dans le réseau;

- au début d'internet, des créneaux non saturés du réseau scientifique public furent utilisés pour la transmission du courrier électronique. Le cheminement d'un message était dès lors tout à fait imprévisible, chaque paquet suivant un itinéraire chaotique qui ne pouvait être deviné. À l'époque, la principale liaison internationale était la "dorsale scientifique" entre l'Europe et l'Amérique;

- la commercialisation d'internet et l'apparition de fournisseurs d'internet entraîna également une commercialisation du réseau. Les fournisseurs internet exploitaient ou louaient leurs propres réseaux. Aussi s'efforcèrent-ils de plus en plus souvent de confiner les communications à l'intérieur du réseau leur appartenant, en sorte d'éviter de devoir payer des redevances d'utilisation à d'autres opérateurs du réseau. Dès lors, l'itinéraire d'un paquet de données dans le réseau est aujourd'hui déterminé non seulement par le degré de saturation du réseau, mais aussi par des considérations financières;

- un courrier électronique qui est envoyé par un client d'un fournisseur à un client d'un autre fournisseur reste en règle générale dans le réseau de l'entreprise, même si l'itinéraire qu'il suit alors n'est pas le plus rapide. Les ordinateurs qui sont disposés aux nœuds du réseau et qui décident du transport des paquets de données (les "routeurs") effectuent le transfert vers d'autres réseaux à certains points de connexion (les "commutateurs");

- à l'époque de la dorsale scientifique, les "commutateurs" de la communication internet mondiale étaient situés aux États-Unis. Aussi, les services de renseignement pouvaient-ils alors y mettre la main sur une partie essentielle des communications internet européennes. Aujourd'hui, les communications internet intraeuropéennes ne transitent plus que dans une mesure très limitée par les États-Unis;

- une petite partie des communications intraeuropéennes sont acheminées via un commutateur à Londres, auquel le GCHQ britannique (Centre national de communications) a accès. La plus grande partie des communications ne sortent pas du continent. C'est ainsi, par exemple, que plus de 95 % des communications internet allemandes sont traitées par un commutateur situé à Francfort.

Dans la pratique, cela signifie que les États ECHELON ne peuvent avoir accès qu'à une **partie très limitée** des communications internet tributaires du câble.

3.3.1.2. Communications hertziennes[9]

La possibilité d'intercepter des communications hertziennes dépend de la portée des ondes électromagnétiques utilisées. Si les ondes radio émises suivent la courbe de la surface terrestre (les **ondes de sol**), leur portée est limitée et dépend de la nature du sol, des constructions et de la végétation. Si les ondes radio sont envoyées vers l'espace (les **ondes d'espace ou indirectes**), elles peuvent franchir des distances considérables après réflexion sur les couches de l'ionosphère. Des réflexions successives augmentent notablement la portée.

La portée dépend de la longueur d'onde:

- les ondes myriamétriques et les ondes longues (3 kHz – 300 kHz) ne se propagent que via l'onde de sol, dès lors que l'onde d'espace n'est pas reflétée. Leur portée est limitée;

- les ondes moyennes (300 kHz – 3MHz) se propagent via l'onde de sol et, la nuit, également via l'onde d'espace. Elles ont une portée moyenne;

- les ondes courtes (3MHz – 30 MHz) se propagent principalement via l'onde d'espace et permettent, par réflexions successives, une réception **circumterrestre;**

- les ondes ultracourtes (30 MHz – 300 MHz) se propagent uniquement via l'onde de sol, dès lors que l'onde d'espace n'est pas reflétée. Elles se propagent plutôt en ligne droite, comme la lumière, leur portée dépendant ainsi, compte tenu de la courbure de la terre, de la hauteur des antennes de l'émetteur et du récepteur. Selon la puissance, leur portée peut atteindre quelque 100 km (pour les téléphones portables, 30 km environ);

- les ondes décimétriques et centimétriques (30 MHz – 30 GHz) se propagent davantage encore que les ondes ultracourtes de façon quasi-optique. Elles peuvent facilement être réunies en faisceaux, ce qui permet des transmissions ciblées à faible puissance (faisceaux hertziens terrestres). Elles ne peuvent être captées que par une antenne très proche, parallèlement, du faisceau hertzien ou située dans l'axe de celui-ci ou dans son prolongement.

Les ondes longues et moyennes ne sont utilisées que pour les émetteurs radio, les radiophares, etc. Les communications radio militaires et civiles s'effectuent par ondes courtes, et surtout par

[9] U. Freyer, Nachrichtenübertragungstechnik, Hanser Verlag, 2000.

ondes ultracourtes et ondes décimétriques/centimétriques.

Il ressort des observations qui précèdent qu'un système d'interception des communications fonctionnant à l'échelle mondiale ne peut avoir accès qu'aux émissions en ondes courtes. Pour tous les autres types d'émissions hertziennes, la station d'interception doit être située à 100 km ou moins (par exemple sur un bateau, dans une ambassade).

Dans la pratique, cela signifie que les pays ECHELON ne peuvent avoir accès qu'à une partie très limitée des communications hertziennes.

3.3.1.3.Communications via des satellites de télécommunication géostationnaires[10]

Comme il a déjà été dit, les ondes décimétriques et centimétriques peuvent être facilement réunies en faisceaux hertziens. Si un faisceau hertzien est dirigé vers un satellite de communication stationnaire sur orbite haute, satellite qui reçoit, transforme et renvoie les signaux hertziens vers la terre, il est possible de franchir de grandes distances sans utiliser le câble. En réalité, la portée d'une telle liaison n'est limitée que par le fait que le satellite ne peut recevoir des signaux venant de toute la terre ni envoyer des signaux vers toute la terre. Aussi faut-il plusieurs satellites pour obtenir une couverture planétaire. (Pour plus de détails, se référer au chapitre 4.) Si les pays ECHELON ont mis en place des stations d'interception dans les régions requises de la terre, ils peuvent en principe intercepter l'ensemble des communications – téléphone, fax et données – effectuées via de tels satellites.

3.3.1.4. Possibilités d'interception par avion et bateau

L'on sait, depuis longtemps, que des avions spéciaux du type AWACS sont utilisés pour repérer dans le monde entier d'autres avions. Le radar de ces appareils est équipé d'un système d'identification d'objectifs donnés, qui peut repérer des rayonnements électroniques, les classifier et les corréler avec des contacts radar. Il n'existe pas une capacité SIGINT distincte[11]. En revanche, l'avion-espion EP-3 des forces navales américaines, qui vole à faible vitesse, dispose de possibilités d'interception dans la bande des micro-ondes, des ondes ultracourtes et des ondes courtes. Les signaux sont exploités directement à bord; l'appareil sert uniquement à des fins militaires[12].

De plus, des navires de surface et, à proximité des terres des sous-marins sont utilisés pour intercepter les communications radio militaires[13].

3.3.1.5. Possibilités d'interception par satellite-espion

Lorsqu'elles ne sont pas réunies en faisceau par des antennes appropriées, les ondes radio se propagent dans toutes les directions, y compris vers l'espace. Les satellites SIGINT sur orbite basse ne peuvent garder le contact avec l'émetteur recherché que pendant quelques minutes. Dans les zones fortement peuplées et très industrialisées, l'interception est rendue plus difficile par la densité importante d'émetteurs de même fréquence, à un tel point qu'il n'est pratiquement

[10] Hans Dodel, Satellitenkommunikation, Hüthig Verlag, 1999.
[11] Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense, en date du 14.2.2001.
[12] Süddeutsche Zeitung, n° 80 du 5.4.2001, p. 6.
[13] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York, 1989, pp.188 et 190.

pas possible de filtrer les signaux[14]. Ces satellites ne se prêtent pas à une surveillance en continu des communications radio civiles.

Parallèlement, il existe des satellites SIGINT américains dits quasistationnaires sur orbite haute (42 000 km)[15]. Contrairement aux satellites de communication géostationnaires, ces satellites présentent une inclinaison de 3 à 10°, un apogée de 39 000 à 42 000 km et un périgée de 30 000 à 33 000 km. Les satellites ne sont donc pas immobiles sur leur orbite; ils se déplacent selon une orbite elliptique complexe. Aussi peuvent-ils, au cours d'une journée, couvrir une région plus grande et permettent-ils de repérer des sources radio. Il semble bien dès lors, et compte tenu également des autres caractéristiques du domaine public, que l'utilisation de ces satellites est purement militaire.

Les signaux reçus sont retransmis vers une station terrestre par une puissante liaison descendante en faisceaux de 24 GHz.

3.3.2. Possibilités d'exploitation automatique des communications interceptées: utilisation de filtres

Lorsque les communications extérieures sont l'objet de l'interception, celle-ci ne vise pas un raccordement téléphonique donné. Le but consiste plutôt à intercepter l'ensemble ou une partie des communications effectuées via les satellites surveillés ou le câble surveillé et à les filtrer au moyen d'ordinateurs en utilisation des notions clés. Et cela parce que l'exploitation de l'ensemble des communications interceptées est tout à fait impossible.

Le filtrage des communications effectuées par des raccordements donnés est simple. En utilisant des notions clés, il est également possible de saisir de façon spécifique les téléfax et les courriers électroniques. Il est même possible de repérer une voix donnée, si le système a été formé pour reconnaître celle-ci[16]. Par contre, la reconnaissance automatique de mots prononcés par une voix quelconque n'est aucunement, selon les informations en possession de votre rapporteur, possible actuellement. De plus les possibilités de filtrage sont encore limitées par d'autres facteurs: la capacité finale de l'ordinateur, le problème des langues et, surtout, le nombre limité des experts capables de lire et d'exploiter les informations filtrées.
Dans le contexte de l'appréciation des possibilités des systèmes de filtrage, il faut également tenir compte du fait que l'ensemble des possibilités techniques d'un tel système d'interception fonctionnant selon le "principe de l'aspirateur" sont ventilées selon différents thèmes. Une partie des mots clés concerne la sécurité militaire, une deuxième le trafic de drogue et d'autres formes de criminalité internationale, une troisième des notions relatives au commerce des biens à double usage et une quatrième le respect d'embargos. Une autre partie des notions clés a également trait à l'économie. Il en résulte que les capacités du système s'éparpillent entre plusieurs secteurs. Une concentration des mots clés sur le seul secteur intéressant du point de vue économique serait contraire aux priorités que les dirigeants politiques imposent à ces services; une telle réorientation n'a jamais eu lieu, même après la fin de la guerre froide[17].

3.3.3. Exemple du service de renseignements allemand

La deuxième section du service fédéral de renseignement allemand se procure des informations par l'interception des communications étrangères. Cette activité a fait l'objet d'un examen par la

[14] Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense, en date du 14.2.2001.
[15] Major Andronov, Zarubezhnoye voyennoye obozreniye, n° 12, 1993, pp. 37 à 43.
[16] Communication faite en privée au rapporteur, source protégée.
[17] Communication faite en privée au rapporteur, source protégée.

Cour constitutionnelle allemande. Les détails qui ont été rendus publics à cette occasion[18] donnent – conjointement avec les déclarations faites par le coordinateur des services secrets au sein de la chancellerie fédérale, Ernst Uhrlau, devant la commission ECHELON, le 21 novembre 2000 – une idée des possibilités des services de renseignement en matière d'interception des communications par satellite.

Il se peut que, çà et là, d'autres services de renseignement aient davantage de possibilités importantes, dans la mesure où l'accès aux communications tributaires du câble leur est permis ou si plus de personnes se consacrent à l'exploitation des informations. Si les communications tributaires du câble sont également interceptées, la probabilité statistique de réussite est notablement augmentée, ce qui n'est pas le cas nécessairement du nombre de communications exploitables. En fait, le cas du BND constitue, pour votre rapporteur, un exemple frappant des possibilités et stratégies des services de renseignement étrangers dans le domaine de l'interception des communications extérieures, même s'ils n'en font pas publiquement état.

Par la voie d'un contrôle **stratégique** des télécommunications, le service de renseignement fédéral s'efforce d'obtenir à l'étranger des informations concernant l'étranger. À cet effet, les communications satellitaires sont interceptées en se fondant sur une série de notions cibles (qui, en Allemagne, doivent être autorisées préalablement par la commission G10[19]). Quantitativement, le schéma se présente comme suit (état 2000): sur les quelque 10 millions de communications internationales/jour effectuées au départ et à destination de l'Allemagne, 800 000 environ le sont par satellite. À peine 10% d'entre elles (75 000) sont filtrées par un appareil de recherche. Cette situation s'explique, de l'avis de votre rapporteur, non par des raisons légales (en théorie, la totalité aurait été permise, à tout le moins avant le procès devant la Cour constitutionnelle), mais bien par des raisons techniques dues à certaines contraintes, comme la capacité d'exploitation.

De même, le nombre des notions de recherche pouvant être utilisées est limité tant par la technique que par l'autorisation préalable requise. Dans la motivation de son arrêt, la Cour constitutionnelle fait état, parallèlement aux notions de recherche purement formelles (interception d'étrangers ou d'entreprises étrangères à l'étranger), de 2 000 notions de recherche dans le domaine de la prolifération, de 1 000 dans le domaine du commerce des armes, de 500 dans le domaine du terrorisme et de 400 dans le domaine du trafic de drogue. S'agissant du terrorisme et du trafic de drogue, la procédure ne semble toutefois pas avoir été une réussite particulière.

L'appareil de recherche étudie les notions de recherche autorisées transmises par téléfax et par télex. Une reconnaissance automatique de mots n'est actuellement pas possible dans les communications vocales. Si les notions de recherche ne sont pas découvertes, les communications finissent automatiquement, de par la technique appliquée, dans la poubelle; elles ne peuvent pas être exploitées, parce qu'il n'existe aucune base juridique le permettant. Quotidiennement, quelque 5 communications d'utilisateurs des télécommunications relèvent de la protection de la constitution allemande. L'interception stratégique du service fédéral de renseignement vise à trouver des éléments pouvant servir de base pour une autre interception. Son objectif ne consiste pas à instaurer une surveillance absolue des communications extérieures. Selon les informations dont il dispose, votre rapporteur estime qu'il en est également ainsi pour

[18] BverfG, 1 BvR 2226/94 du 14.7.1999, paragraphe 1.
[19] Gesetz zur Beschränkung des Brief-,Post- und Fernmeldegeheimnisses (Gesetz zur Artikel 10 GG) du 13.8.1968.

l'activité SIGINT d'autres services de renseignement étranger.

4. Technique des communications satellitaires

4.1. Importance des satellites de télécommunication

Les satellites de communication forment aujourd'hui un élément indispensable du réseau mondial des télécommunications et de la diffusion de programmes de radio et de télévision, ainsi que de services multimédias. Néanmoins, la part des communications par satellite dans les communications internationales a fortement diminué ces dernières années en Europe centrale. Dans bien des régions, elle est même aujourd'hui inférieure à 10%[20]. Cette situation s'explique par les avantages que présente le câble à fibres optiques, qui peut acheminer un nombre bien plus important de communications, tout en garantissant une qualité élevée.

Désormais, les communications sont numérisées y compris dans le secteur vocal. La capacité des liaisons satellitaires numériques par transpondeur de satellite est limitée à **1890** canaux vocaux RNIS (64 kbits/sec). En revanche, une seule fibre optique peut aujourd'hui déjà offrir **241920** canaux vocaux à la même norme. Le rapport est ainsi de **1 à 128**!

De plus, la qualité des liaisons par satellite est moindre que celle des liaisons par câble marin à fibres optiques. Les pertes de qualité dues à la longueur du temps de parcours des signaux – plusieurs centaines de millisecondes – sont à peine perceptibles dans une transmission vocale normale, ce qui n'empêche qu'il est possible de les entendre. Pour les communications de données et de téléfax, qui s'effectuent par l'intermédiaire d'une procédure complexe de mise en liaison, le câble présente des avantages évidents en termes de sécurité de liaison. Force est toutefois de constater, parallèlement, que 15% de la population mondiale seulement est connectée au réseau mondial de câbles[21].

Aussi, les systèmes satellitaires demeureront-ils cependant plus avantageux que le câble pour certaines applications. Citons quelques exemples civils:

- acheminement national, régional et international de communications téléphoniques et de données dans des régions où le volume des communications est restreint, c'est-à-dire là où la réalisation d'une liaison par câble ne serait pas rentable compte tenu du taux d'utilisation;

- communication limitée dans le temps pour des interventions en cas de catastrophes, des manifestations, des chantiers importants, etc.;

- missions des Nations unies dans des régions où les infrastructures de communication sont peu développées;

- communication économique flexible/mobile avec des petits émetteurs (VSAT, cf. infra).

Cette gamme d'utilisation des satellites dans les communications trouve son origine dans les caractéristiques suivantes: les émissions d'un seul satellite géostationnaire peuvent couvrir près de 50% de la surface terrestre; des terrains impraticables peuvent également être franchis. Ainsi, 100% des utilisateurs, qu'ils soient terrestres, marins ou aériens, peuvent être desservis. Les

[20] Cf. Exposé des motifs de la modification de la loi G10 en Allemagne.
[21] Page d'accueil de Deutsche Telekom: www.detesat.com/deutsch/.

satellites sont opérationnels en quelques mois, et ce indépendamment de l'infrastructure locale. Ils sont plus sûrs que le câble et peuvent être mis hors service facilement.

Les caractéristiques suivantes des communications satellitaires appellent des commentaires négatifs: les temps de parcours relativement longs des signaux, la dégradation par éparpillement, la durée de vie – de 12 à 15 ans – plus courte que le câble, la plus grande vulnérabilité, ainsi que les possibilités plus importantes d'interception.

4.2. Fonctionnement d'une liaison satellitaire

Comme il a été dit précédemment (cf. chapitre 3), les micro-ondes peuvent facilement être réunies en faisceaux. Il est dès lors possible de remplacer le câble par des faisceaux hertziens. Si les antennes d'émission et de réception ne se trouvent pas sur un même plan – ce qui est le cas sur terre, notre planète affectant la forme d'une sphère –, l'antenne de réception "disparaît" par suite de la courbure de la surface, à partir d'une certaine distance, sous l'horizon. Alors, les deux antennes ne se "voient" plus. Ce serait également le cas, par exemple, pour un faisceau hertzien intercontinental entre l'Europe et les États-Unis. Pour pouvoir établir une liaison, les antennes devraient se trouver au sommet de mâts hauts de 1,8 km. Pour cette seule raison, un tel faisceau hertzien intercontinental ne peut être réalisé. D'autant plus que le signal est amorti par l'atmosphère et la vapeur d'eau sur l'ensemble du parcours. Toutefois, s'il est possible de disposer, à grande altitude, dans l'espace et sur une "position fixe", une sorte de miroir qui capte le faisceau hertzien, alors, de grandes distances peuvent être franchies en dépit de la courbure de la terre, la comparaison pouvant être faite avec un miroir routier qui permet de voir ce qu'il y a après un virage. Le principe décrit ci-dessus est mis en œuvre dans la pratique en utilisant des satellites dits géostationnaires.

4.2.1. Satellites géostationnaires

Si un satellite est placé sur orbite circulaire parallèle à l'équateur et fait un tour de la terre en 24 heures, alors il suit exactement la rotation terrestre. De la surface de la terre, il apparaît dès lors immobile à 36 000 km de distance. Il a une position **géostationnaire**. La plupart des satellites de télécommunications et de télévision appartiennent à ce type de satellites.

4.2.2. Cheminement d'une liaison satellitaire de télécommunication

La transmission des signaux via satellite s'effectue comme suit:

Le signal acheminé par une liaison est envoyé par une station terrestre équipée d'une antenne parabolique via un faisceau hertzien ascendant, appelé **uplink**, vers un satellite. Le satellite reçoit le signal, l'amplifie et le renvoie via un faisceau hertzien descendant, appelé **downlink**, vers une autre station terrestre. Là, le signal est réintroduit dans un réseau câblé.

Dans le cas de la communication mobile, le signal est transmis directement de l'unité de communication mobile au satellite d'où il peut être réinjecté, via une station terrestre, dans un réseau ou directement retransmis à une autre unité mobile.

4.2.3. Principaux systèmes de communication satellitaires existants

Les communications provenant de **réseaux de câbles accessibles au public** (qui ne sont pas nécessairement publics) sont, le cas échéant, acheminées via des systèmes satellitaires de dimensions différentes entre des stations terrestres fixes, pour être ensuite réinjectées dans les

réseaux de câbles. Une distinction est faite entre les systèmes satellitaires

- mondiaux (p. ex. INTELSAT),
- régionaux (continentaux) (p. ex. EUTELSAT), et
- nationaux (p. ex. ITALSAT).

La plupart de ces satellites se trouvent sur orbite géostationnaire. Dans le monde, 120 sociétés privées exploitent quelque mille satellites placés sur de telles orbites[22].

Parallèlement, il existe, pour le grand Nord, des satellites sur orbite spéciale très excentrique (orbites russes Molnyia), qui sont visibles pour l'utilisateur du grand Nord pendant la moitié de leur période orbitale. Deux satellites de ce genre permettent ainsi une couverture régionale, qui ne peut être obtenue à partir d'une position géostationnaire au-dessus de l'équateur.

De plus, le réseau INMARSAT – conçu au départ pour une utilisation à des fins maritimes - qui couvre le monde entier représente un **système de communication mobile**, permettant d'établir des liaisons satellitaires partout dans le monde. Il fait également appel à des satellites géostationnaires.

Le système de commmunication par portables IRIDIUM fonctionnant grâce à plusieurs satellites sur orbites basses différées a été mis hors service récemment, pour des raisons économiques, son taux d'utilisation étant insuffisant.

En outre, il existe un marché en rapide développement pour les communications VSAT (terminal équipé d'une très petite antenne). Il s'agit en l'occurrence de microstations dont l'antenne à un diamètre compris entre 0,9 et 3,7 m, qui sont exploitées par des entreprises pour leurs propres besoins (par exemple, des vidéoconférences) ou par des fournisseurs de services mobiles pour une demande temporaire de liaison (par exemple, des réunions). En 1996, 200 000 microstations étaient exploitées dans le monde entier. Le groupe Volkswagen exploite 3 000 unités VSAT, Renault 4 000, General Motors 100 000, et le plus grand groupe pétrolier européen 12 000. Les communications se font en clair, à moins que le client ne les crypte lui-même[23].

4.2.3.1. Systèmes de satellites fonctionnant à l'échelle mondiale

Ces systèmes de satellites couvrent l'ensemble de la planète grâce au positionnement de plusieurs satellites dans les zones atlantique, indienne et pacifique.

[22] G. Thaller, Satelliten im Erdorbit, Franzisverlag, Munich, 1999.
[23] H. Dodel, déclaration faite en privé.

INTELSAT[24]

INTELSAT (Organisation internationale des télécommunications par satellites), qui a été créée en 1964, est une autorité dont la structure organisationnelle est similaire à celle des Nations unies, et dont l'activité consiste à assurer des communications internationales. Les membres de cette organisation étaient les administrations nationales des postes publiques. À l'heure actuelle, 144 gouvernements sont membres d'INTELSAT. L'année 2001 verra la privatisation d'INTELSAT.

INTELSAT dispose d'une flotte de 19 satellites géostationnaires, qui mettent en contact plus de 200 pays et dont les services sont loués à ses membres, lesquels disposent de leurs propres stations au sol. Grâce à IBS (Service commercial d'INTELSAT), des tierces parties (p. ex., des sociétés de téléphone, de grandes entreprises, des groupes internationaux) peuvent également utiliser les satellites depuis 1984. INTELSAT propose des services planétaires dans différents domaines, comme les communications, la télévision, etc. Les télécommunications s'effectuent sur bandes C et Ku (cf. infra).

Les satellites d'INTELSAT sont les principaux satellites utilisés pour les communications internationales. Ils assurent l'essentiel des communications internationales satellitaires.

Ces satellites couvrent les zones atlantique, indienne et pacifique (cf. tableau, chapitre 5, point 5.3).

Au-dessus de l'Atlantique, il y a dix satellites positionnés entre les 304°Est et 359°Est; au-dessus de l'océan Indien, six satellites entre les 62°Est et 110,5°Est; au-dessus du Pacifique, trois satellites entre les 174°Est et 180°Est. L'existence de plusieurs satellites au-dessus de l'Atlantique permet de faire face aux besoins importants de communications dans cette zone.

INTERSPUTNIK[25]

En 1971, l'organisation internationale de communications satellitaires INTERSPUTNIK a été créée par neuf pays; il s'agissait d'une agence de l'ex-Union soviétique, dont la mission était similaire à celle d'INTELSAT. Aujourd'hui, INTERSPUTNIK est une organisation intergouvernementale, dont peut être membre le gouvernement de n'importe quel pays. Elle compte désormais 24 États membres (notamment l'Allemagne) et quelque 40 utilisateurs (entre autres, la France et le Royaume-Uni), qui sont représentés par leurs administrations postales ou par leurs organisations des télécommunications. Son siège est à Moscou.

Les télécommunications sont acheminées sur les bandes C et Ku (cf. infra).

Différents satellites (Gorizont, Express, Express A de la Fédération de Russie, et LMI-1 de l'entreprise commune Lockhead-Martin) couvrent également l'ensemble de la planète: un satellite orbite au-dessus de la zone atlantique et un deuxième est prévu; dans la zone de l'océan Indien, il y a trois satellites, et dans la zone pacifique, deux (cf. tableau, chapitre 5, point 5.3).

INMARSAT

Depuis 1979, INMARSAT (Organisation internationale des télécommunications maritimes par satellites) assure dans le monde entier des communications **mobiles** en mer, dans l'air et sur terre,

[24] Page d'accueil d'INTELSAT– http://www.intelsat.com.
[25] Page d'accueil d'INTERSPUTNIK: http://www.intersputnik.com.

ainsi qu'un service d'appels de détresse. INMARSAT a été mis en place en tant qu'organisation interétatique à l'initiative de l'Organisation maritime internationale. INMARSAT, aujourd'hui privatisée, a son siège à Londres.

Le système INMARSAT repose sur neuf satellites placés sur orbite géostationnaire. Quatre des satellites – qui appartiennent à la génération INMARSAT-III – couvrent l'ensemble de la planète jusqu'aux régions polaires les plus extrêmes. Chacun d'eux couvre environ un tiers de la surface terrestre. De par leur position au-dessus des quatre régions océaniques (Atlantique occidental et oriental, Pacifique, océan Indien), ils permettent une couverture planétaire. De plus, chaque satellite INMARSAT dispose également d'un certain nombre de faisceaux étroits, ce qui permet de concentrer l'énergie sur des zones où les besoins de communications sont importants.

Les télécommunications sont acheminées sur les bandes L et Ku (cf. infra, point 4.2.4).

4.2.3.2. Systèmes de satellites régionaux

Les zones d'empreinte des faisceaux des systèmes satellitaires régionaux couvrent différentes régions et différents continents. Les communications ainsi acheminées ne peuvent donc être reçues que dans ces régions.

EUTELSAT[26]

EUTELSAT a été créée en 1977 par dix-sept administrations postales européennes aux fins de couvrir les besoins spécifiques de l'Europe dans le domaine des communications par satellite et de soutenir l'industrie aérospatiale européenne. EUTELSAT, qui compte quelque quarante États membres, a son siège à Paris. L'organisation doit être privatisée en 2001.

EUTELSAT dispose de dix-huit satellites géostationnaires, qui couvrent l'Europe, l'Afrique et une grande partie de l'Asie, et qui assurent une liaison avec l'Amérique. Les satellites sont situés entre 12,5°Ouest et 48°Est. EUTELSAT offre essentiellement des services télévisuels (850 canaux numériques et analogiques) et radiophoniques (520 canaux), tout en assurant également des services de communications, avant tout en Europe (y compris en Russie): par exemple, pour des vidéoconférences, des réseaux privés de grandes entreprises (entre autres, General Motors et Fiat), des agences de presse (Reuters, AFP), des fournisseurs de services financiers et des services mobiles de transmission de données.

Les télécommunications sont acheminées sur la bande Ku.

ARABSAT[27]

ARABSAT est le pendant d'EUTELSAT dans la région arabe. L'organisation, qui a été créée en 1976, a pour membres 21 pays arabes. Les satellites d'ARABSAT sont utilisés tant pour la transmission télévisuelle que pour les communications.

Les télécommunications sont acheminées essentiellement dans la bande C.

[26] Page d'accueil d'EUTELSAT: http://www.com.
[27] Page d'accueil d'ARABSAT: http://www.arabsat.

PALAPA[28]

Le système indonésien PALAPA, qui est exploité depuis 1995, est le pendant sud-asiatique d'EUTELSAT. Son faisceau d'empreinte couvre la Malaisie, la Chine, le Japon, l'Inde, le Pakistan et d'autres pays de la région.

Les télécommunications sont acheminées sur les bandes C et Ku.

4.2.3.3. Systèmes de satellites nationaux[29]

De nombreux pays utilisent, pour couvrir leurs besoins nationaux, leurs propres systèmes de satellites, dont les zones d'empreinte sont limitées.

Le satellite français de télécommunications **TELECOM** sert notamment à relier les départements français d'Afrique et d'Amérique du Sud avec la métropole. Les télécommunications sont acheminées sur les bandes C et Ku.

ITALSAT dispose de satellites de télécommunications, dont les zones d'empreinte limitées, mais limitrophes, couvrent l'ensemble de la botte italienne. Aussi une réception n'est-elle possible qu'en Italie. Les télécommunications sont acheminées sur la bande Ku.

AMOS est un satellite israélien utilisé essentiellement pour des communications à poste fixe, dont la zone d'empreinte couvre le Moyen-Orient. Les télécommunications sont acheminées sur la bande Ku.

Les satellites espagnols de **HISPASAT** couvrent l'Espagne et le Portugal (traces Ku) et servent à transmettre des programmes de télévision vers l'Amérique du Nord et l'Amérique du Sud.

4.2.4. Attribution de fréquences

La répartition des fréquences est de la compétence de l'Union internationale des télécommunications. Pour assurer un certain ordre, le monde a été divisé pour les communications hertziennes en trois régions:

1. Europe, Afrique, ex-Union soviétique, Mongolie,

2. Amérique du Nord et Amérique du Sud, Groenland y compris,

3. Asie, exception faite des pays de la région 1, Australie et Pacifique Sud.

Cette répartition traditionnelle a été conservée pour les communications par satellites; elle est à l'origine d'une concentration de satellites dans certaines zones géostationnaires. Les principales bandes de fréquence pour les communications par satellites sont les suivantes:

- la bande L (0,4 – 1,6 GHz) pour les communications mobiles par satellites, par exemple via INMARSAT,

- la bande C (3,6 - 6,6 GHz) pour les stations hertziennes terrestres, par exemple via INTELSAT,

[28] H.Dodel, Satellitenkommunikation, Hüthigverlag, 1999.
[29] H.Dodel et recherches Internet.

- la bande Ku (10 - 20GHz) pour les stations hertziennes terrestres, par exemple INTELSAT-Ku-Spot et EUTELSAT,

- la bande Ka (20 - 46 GHz) pour les stations hertziennes terrestres, par exemple via les satellites nationaux comme ITALSAT,

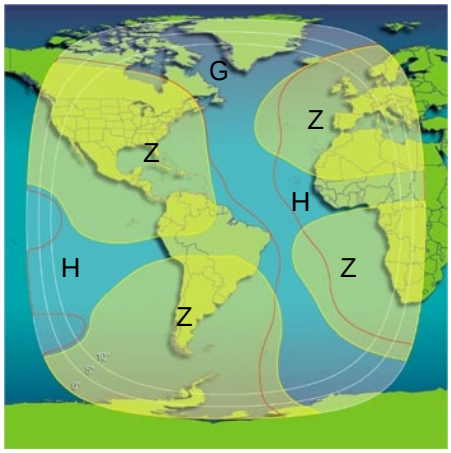
- la bande V (46 – 56 GHz) pour les microstations hertziennes (VSAT).

4.2.5. Zones couvertes par les satellites (empreintes au sol)

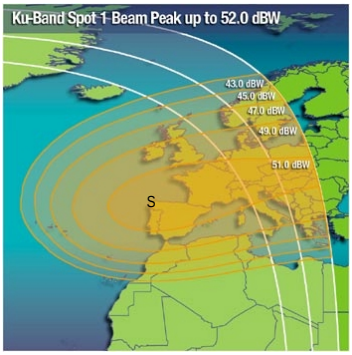
Par zone d'empreinte, on entend la région de la terre qui est couverte par une antenne de satellite. Cette zone peut représenter jusqu'à 50% de la surface terrestre ou, lorsque le signal est concentré, des points régionaux plus petits.

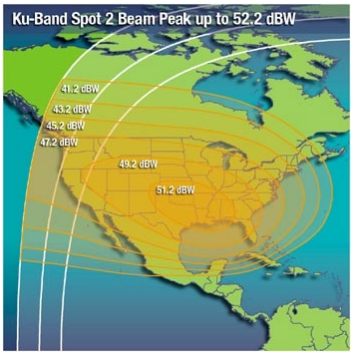
Plus la fréquence du signal émis est élevée, plus il est possible de le concentrer, et plus la zone d'empreinte peut être réduite. La concentration du signal satellitaire émis sur des zones d'empreinte plus petites permet d'augmenter l'énergie du signal. Ainsi, plus la zone d'empreinte est petite, plus le signal peut être fort, et, partant, plus l'antenne de réception peut être réduite.

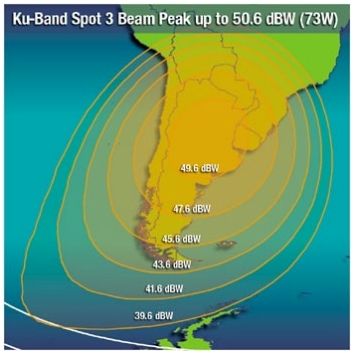
En résumé, la situation se présente précisément comme suit pour les satellites d'INTELSAT:



Les zones d'empreinte des satellites d'INTELSAT se répartissent entre différents faisceaux:
Le faisceau à couverture mondiale (G) de tout satellite couvre environ un tiers de la surface terrestre.
Les faisceaux à semi-couverture (H) couvrent une surface légèrement inférieure à la moitié de celle du faisceau à couverture mondiale Les faisceaux zonaux (Z) représentent des zones de réception dans certaines parties du monde; ils sont plus petits que les faisceaux à semi-couverture. Il y a enfin ce qu'il est convenu d'appeler les pinceaux, c'est-à-dire des zones d'empreinte précises et réduites(cf. infra).







Les fréquences de la bande C concernent les faisceaux à couverture mondiale, les faisceaux à semi-couverture ainsi que les faisceaux zonaux. Les fréquences de la bande Ku sont utilisées dans les faisceaux étroits.

4.2.6. Dimensions des antennes requises pour une station terrienne

Les antennes de réception terrestres sont des antennes paraboliques. Le miroir parabolique reflète toutes les ondes captées et les concentre en un point focal. C'est à cet endroit précis que se trouve le système de réception proprement dit. Plus l'énergie du signal au point de réception est grande, plus le diamètre de l'antenne parabolique peut être réduit.

Ce qui est déterminant pour le but poursuivi dans le contexte de l'enquête réalisée pour le présent rapport, c'est qu'une partie des communications intercontinentales sont acheminées via la bande C dans les faisceaux à couverture mondiale des satellites d'INTELSAT et d'autres satellites (par exemple, INTERSPUTNIK), et que pour leur réception des panneaux satellitaires d'un diamètre de l'ordre de 30 m sont parfois nécessaires (cf. chapitre 5). Des antennes de 30 m étaient également nécessaires pour les premières stations de réception des satellites de communications, dès lors que la première génération d'INTELSAT n'utilisait que des faisceaux à couverture mondiale et que la transmission des signaux était encore bien moins perfectionnée qu'aujourd'hui. Ces panneaux d'un diamètre parfois supérieur à 30 m sont encore utilisés aujourd'hui dans les stations en question, même si, techniquement, ils ne sont plus nécessaires.

Les antennes actuellement nécessaires pour les communications INTELSAT dans la bande C ont un diamètre compris entre 13 et 18 m. Dans des cas particuliers (par exemple, INTELSAT 511), une antenne plus grande est indispensable pour le faisceau à couverture mondiale. Pour les satellites INTELSAT les plus récents, des antennes d'un diamètre ne dépassant pas 5 m suffisent, y compris pour les faisceaux zonaux de la bande C.

Pour la réception des communications sur la bande C d'INTERSPUTNIK, il faut des antennes dont le diamètre varie de 2 à 25 m.

Pour les traces Ku des satellites d'INTELSAT ainsi que pour d'autres satellites (bande Ku d'EUTELSAT, bande Ku AMOS, etc.), le diamètre des antennes nécessaires est compris entre 2 et 10 m.

Pour les microstations, qui fonctionnent dans la bande V, et dont les signaux sont plus concentrés encore que dans la bande Ku, compte tenu de la fréquence élevée, un diamètre d'antenne compris entre 0,9 et 3,7 m est suffisant (p.ex., VSAT d'EUTELSAT ou INMARSAT).

5. Preuves par indices de l'existence d'au moins un système d'interception mondial

5.1. Pourquoi une preuve par indices?

Naturellement, les services secrets ne font pas publiquement état de leurs activités. Aussi ne faut-il pas, en tout état de cause, espérer trouver une déclaration officielle dans laquelle les services de renseignement étranger des pays ECHELON reconnaîtraient coopérer à l'exploitation d'un système d'interception mondial. Dès lor, la preuve doit être établie en réunissant un nombre maximal d'indices, pour constituer une preuve convaincante.

La chaîne des indices qui formeraient une telle preuve se compose de trois éléments:

- la preuve que les services de renseignement étranger des pays ECHELON interceptent des communications privées et commerciales;

- la preuve de la découverte des différentes stations d'interception terrestres – indispensables compte tenu du fonctionnement du système de communication civil par satellites – gérées par les pays ECHELON;

- la preuve qu'il existe entre ces pays une coopération des services de renseignement allant au-delà de ce qui est courant. Que cette coopération aille jusqu'à l'acceptation par les partenaires de contrats d'interception et à la communication directe par ceux-ci du matériel brut intercepté, sans aucune forme d'exploitation propre, voilà qui n'a aucune espèce d'importance pour la preuve de l'existence d'une coopération. Cela ne joue un rôle que pour la question de savoir quelles sont les hiérarchies dans le contexte de cette coopération d'interception.

5.1.1. Preuve de l'activité d'interception des services de renseignements étrangers

Dans les démocraties, à tout le moins, les services de renseignement exercent leurs activités sur la base de lois, qui énoncent leurs objectifs et/ou leurs pouvoirs. Aussi est-il simple de prouver qu'il existe dans nombre de ces pays des services de renseignement étranger, qui interceptent les communications civiles. Tel est également le cas des cinq pays ECHELON mentionnés, qui disposent de tels services. Pour chacun de ces pays, il ne faut pas apporter une preuve supplémentaire spécifique de l'interception des communications à destination ou en provenance de leur territoire. Sur leur territoire, ils peuvent également capter, dans le cas de communications par satellite, une partie des messages dont les destinataires se trouvent à l'étranger. Dans aucun des cinq pays ECHELON, nulle disposition légale n'empêche les services concernés d'agir ainsi. La logique interne de la méthode du contrôle stratégique des télécommunications extérieures et le but de ce contrôle, du moins celui qui en partie connu, obligent à considérer que lesdits services agissent bien ainsi.[30]

[30] Votre rapporteur dispose d'informations le prouvant. La source est protégée.

5.1.2. Preuve de l'existence de stations dans les zones géographiques requises

La seule limite à laquelle se heurte la tentative d'exercer une surveillance sur les communications effectuées par satellite procède de la technique même de ce moyen de communication. Il n'existe aucun endroit à partir duquel il serait possible de capter **toutes les** communications par satellite dans le monde entier (cf. chapitre 4, point 4.2.5).

Un système d'interception fonctionnant au niveau mondial pourrait être mis en place pour autant que les trois conditions suivantes existent:

- l'exploitant a une partie de son territoire dans toutes les régions du monde requises;

- l'exploitant a, dans une certaine mesure, une partie de son territoire dans toutes les régions du monde requises et, en plus, un droit d'hospitalité dans les parties du monde qui lui font défaut, et il peut y exploiter des stations ou utiliser celles de son hôte;

- l'exploitant est une association d'États dans le domaine du renseignement et utilise le système dans les régions du monde nécessaires à cet effet.

Aucun des pays ECHELON ne serait en mesure d'exploiter seul un système mondial. À tout le moins officiellement, les États-Unis n'ont aucune colonie. De même, le Canada, l'Australie et la Nouvelle-Zélande n'ont aucune partie de leur territoire située à l'extérieur de leurs frontières au sens propre. Le Royaume-Uni ne pourrait, lui non plus, exploiter seul un système d'interception mondial (cf. chapitre 6).

5.1.3. Preuve d'une association étroite entre les services de renseignements

Il n'est pas possible de dire, par contre, si et dans quelle mesure les pays ECHELON collaborent dans le secteur des services de renseignement. D'ordinaire, une collaboration entre ces services est d'ordre bilatéral et prend la forme d'un échange du matériel exploité. Une association multilatérale est en soi déjà quelque chose de très exceptionnelle; s'il faut encore y ajouter un échange régulier de matériel brut, alors nous sommes en présence d'un phénomène entièrement nouveau. L'existence d'une association de ce type ne peut être établie que sur la base d'indices.

5.2. Comment reconnaît-on une station d'interception des communications par satellite?

5.2.1. Critère 1: accès de l'installation

Les installations de la poste, de la radiotélévision ou des instituts de recherche disposant de grandes antennes sont accessibles aux visiteurs, au moins sur rendez-vous. Les stations d'interception ne le sont pas, par contre. La plupart du temps, elles sont gérées officiellement par des militaires, qui prennent également en charge l'aspect technique de l'interception. Ainsi, dans le cas de la NSA, par exemple, c'est le Naval Security Group (NAVSECGRU) ou l'Air Intelligence Agency des forces aériennes américaines (AIA) qui assure le fonctionnement des stations. Dans les stations britanniques, c'est la Royal Airforce qui gère les installations pour le compte du service de renseignement britannique (GCHQ). Ces dispositions garantissent un contrôle militaire strict de l'installation, tout en permettant de camoufler les activités.

5.2.2. Critère 2: type d'antenne

Dans les installations conformes au critère 1, il existe différents types d'antennes, pouvant se distinguer en fonction de leur structure caractéristique. Leur forme donne des indications quant au but poursuivi par l'installation d'interception. Ainsi, des rangées d'antennes verticales formant un cercle de grand diamètre (antennes Wullenweber) sont utilisées pour déterminer l'orientation de signaux hertziens. De même, une succession circulaire d'antennes rhomboïdales (antennes dites en râteau) sont utilisées dans le même but. Des antennes de réception multidirectionnelles ou antennes directionnelles, comparables à des antennes de télévision classiques gigantesques, servent pour intercepter des signaux hertziens non dirigés. **Pour la réception de signaux satellitaires, on utilise en revanche exclusivement des antennes paraboliques.** Lorsque les antennes paraboliques sont situées à découvert, il est possible de calculer, en connaissant leur situation, leur angle d'inclinaison (élévation) et leur orientation (azimut) le satellite dont les émissions sont interceptées. Il serait possible de le faire, par exemple, à Morwenstow (Royaume-Uni) ou à Yakima (États-Unis) et à Sugar Grove (États-Unis). La plupart du temps, les antennes paraboliques sont cependant dissimulées sous des enveloppes sphériques blanches, appelées radômes. Ces enveloppes servent non seulement à protéger les antennes mais aussi à cacher leur orientation.

Si des antennes paraboliques ou des radômes se trouvent sur le site d'une station d'interception, alors, on peut être sûr que des signaux provenant de satellites y sont captés. Ce qui ne nous dit toujours pas de quel genre de signaux il s'agit en l'occurrence.

5.2.3. Critère 3: dimension de l'antenne

Dans une installation conforme au critère 1, les antennes de réception des satellites peuvent être utilisées dans les buts suivants:

- stations de réception des communications militaires,
- stations de réception des satellites-espions (photos, radar)
- stations de réception des satellites militaires SIGINT
- stations de réception servant à l'interception des satellites de communications civils.

Il n'est pas possible de déduire la mission que remplissent les antennes/radômes à partir de leur aspect extérieur. Toutefois, il existe des dimensions minimales, fonction de la technique, pour les antennes destinées à recevoir le faisceau à couverture mondiale dans la bande C des communications internationales civiles par satellites. Pour la première génération de ces satellites, des antennes d'un diamètre de l'ordre de 25 à 30 m étaient nécessaires; aujourd'hui, un diamètre compris entre 15 et 18 m est suffisant. Le filtrage automatique des signaux captés par ordinateur requiert une qualité optimale du signal; aussi, lorsque le renseignement est l'objectif, opte-t-on pour une antenne de la dimension maximale. Comme les antennes sont montées sur des supports, le diamètre des radômes est encore supérieur à celui des antennes.

5.2.4. Conclusions

À ce que sait votre rapporteur, il n'existe aucune application militaire pour des antennes de cette dimension. Si leur présence est donc constatée sur un site conforme au critère 1, force est de constater que des communications civiles par satellite y sont interceptées.

5.3. Données, pouvant être obtenues par chacun, concernant les stations d'interception connues

5.3.1. Méthode

Afin de déterminer quelles stations répondent aux critères énoncés au point 5.2 et font partie du système d'interception mondial et de préciser de quelles missions elles sont chargées, la documentation afférente, parfois contradictoire (Hager[31], Richelson[32], Campbell[33]), les documents déclassés[34], la page d'accueil de la Federation of American Scientists[35] ainsi que les pages d'accueil de NSA, AIA, etc. et d'autres publications sur internet ont été consultés. En outre, les zones de couverture des satellites de communication ont été rassemblées, les dimensions des antennes nécessaires calculées et reportées sur des planisphères, de même que les stations possibles.

5.3.2. Analyse approfondie

L'analyse tient compte des principes ci-après, qui sont liés à la physique de la communication par satellite (voir également chapitre 4):

– Une antenne ne peut capter que ce qui se trouve dans la zone de couverture où elle est située. Pour pouvoir recevoir des communications relevant principalement des bandes C et Ku, une antenne doit se trouver à l'intérieur de la zone de couverture couvrant les bandes C et Ku.
– Il faut une antenne pour chaque faisceau à couverture mondiale, même si les faisceaux de deux satellites se recoupent.
– Si un satellite présente plus de zones de couverture que le faisceau mondial (c'est le cas de la génération de satellites actuelle), une seule antenne ne permet pas de capter toutes les communications transitant par ces satellites étant donné qu'une seule antenne ne peut se situer dans toutes les zones de couverture des satellites. Pour capter le faisceau à semi-couverture et le faisceau mondial d'un satellite, il faut donc deux antennes dans deux régions différentes (voir schéma des zones de couverture au chapitre 4). Si d'autres faisceaux s'ajoutent à cela (zonaux et pinceaux), des antennes supplémentaires sont nécessaires. Les différents faisceaux d'un même satellite qui se recoupent peuvent toutefois être captés par une seule antenne, car il est techniquement possible de séparer différentes bandes de fréquence à la réception.

---

[31] Hager, Nicky: EXPOSING THE GLOBAL SURVEILLANCE SYSTEM http://www.ncoic.com/echelon1.htm
Hager, Nicky: Secret Power. New Zealands´s Role in the international Spy Network, New Zealand 1996
[32] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson,T.Jeffrey, The U.S. Intelligence Community, Westview Press 1999
[33] Campbell, Duncan, Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, présenté à la commission Echelon du Parlement européen le 22 janvier 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html
[34] Richelson, Jeffrey: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[35] Federation of American Scientists

Pour le reste, les conditions énoncées au point 5.2. sont d'application: les installations ne sont pas accessibles étant donné qu'elles sont exploitées par les militaires[36]; la réception de signaux satellite suppose des antennes paraboliques; la taille des antennes destinées à capter la bande C du faisceau mondial pour la première génération INTELSAT est supérieure à 25 mètres, pour les autres générations, supérieure à 15-18 mètres.

5.3.2.1. Le parallélisme entre le développement des INTELSAT et la construction de stations

Tout système d'écoute global doit croître au rythme du progrès des communications. Le début des communications par satellite doit donc donner lieu à l'apparition des premières stations, et la mise en service de nouvelles générations de satellites à la construction de nouvelles stations et de nouvelles antennes satellitaires opérationnelles. Le nombre des stations et des antennes satellitaires doit augmenter chaque fois que l'interception des communications l'exige.

Par conséquent, à l'inverse, lorsque l'on crée de nouvelles zones de couverture et que l'on construit de nouvelles stations et de nouvelles antennes satellitaires, cela n'est pas par hasard: on peut voir là l'indice de l'existence d'une station d'écoute de communications.

Étant donné que les satellites INTELSAT étaient les premiers satellites de communication et que, de plus, ils couvraient la planète tout entière, il est logique que la mise en place et l'agrandissement de stations suivent le développement des générations d'INTELSAT.

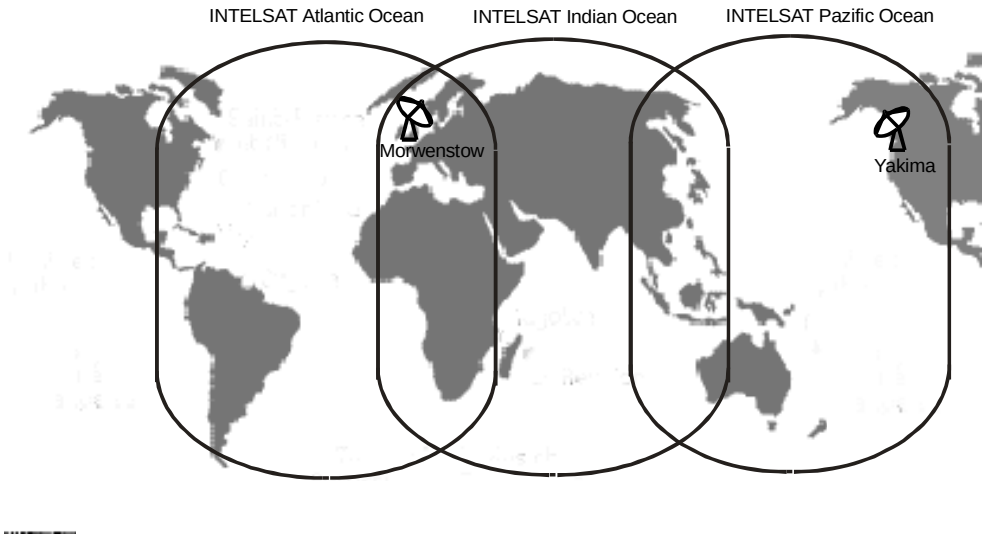
La première génération

C'est dès 1965 que le premier satellite INTELSAT (Early Bird) fut mis en orbite géostationnaire. Il avait une capacité de transmission encore faible et ne couvrait que l'hémisphère nord.

Avec les générations INTELSAT II et III, mises en service respectivement en 1967 et en 1968, on obtint, pour la première fois, une couverture globale. Les g*lobal beams* des satellites couvraient les zones atlantique, pacifique et indienne. Il n'y avait pas encore de zones de couverture plus petites. Pour capter la totalité des communications, il fallait donc trois satellites. Comme deux des g*lobal beams* se chevauchaient au-dessus de l'espace européen, il était possible, dans cette zone, grâce à une station munie de deux antennes satellitaires orientées différemment, de saisir les zones de couverture globales des deux satellites.

[36] Abréviations utilisées: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group

Première génération de satellites INTELSAT à couverture globale

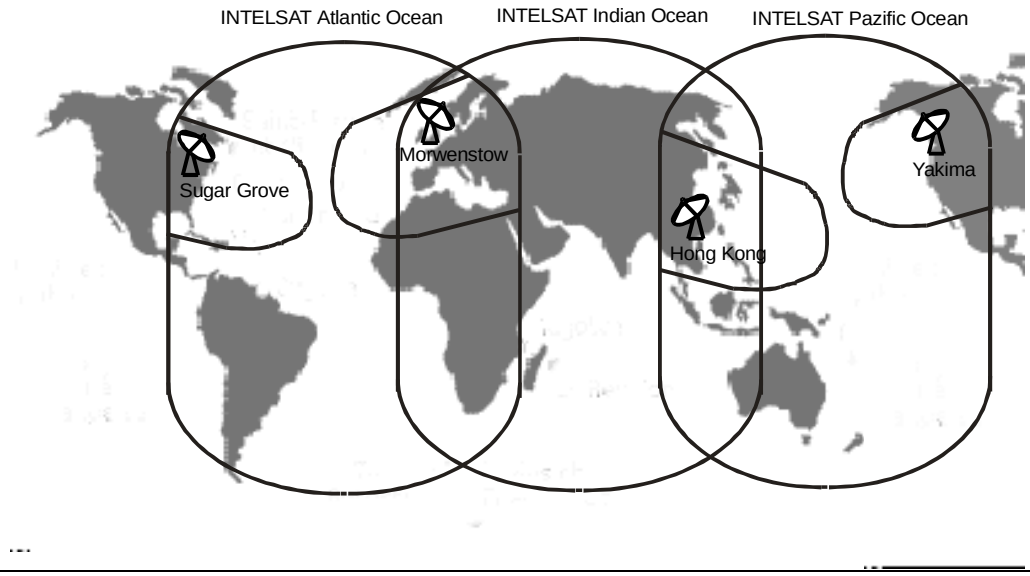


En 1970, **Yakima** fut créée dans le nord-ouest des États-Unis; en 1972/1973, **Morwenstow** fut créée dans le sud de l'Angleterre. Yakima disposait alors d'une grande antenne (orientée vers le Pacifique); Morwenstow avait deux grandes antennes (l'une orientée vers l'Atlantique, l'autre vers l'océan Indien). La localisation des deux stations permettait de capter la totalité des communications. En 1974, on construisit encore, à Menwith Hill, la première grande antenne satellitaire.

La deuxième génération globale

Les satellites INTELSAT de la deuxième génération (IV et IVA) furent développés dans les années 70 et mis en orbite géostationnaire (1971 et 1975). Les nouveaux satellites, qui assuraient aussi une couverture globale et disposaient de beaucoup plus de canaux radio (4000-6000), avaient aussi, outre les g*lobal beams*, des z*one beams* dans l'hémisphère nord (voir chapitre 4). Un z*one beam* couvrait l'est des États-Unis, un autre l'ouest des États-Unis, un autre encore l'Europe occidentale et un dernier l'Asie de l'est. Dès lors, deux stations munies de trois antennes satellitaires ne permettaient plus de capter la totalité des communications. La station de Yakima couvrait le z*one beam* de "Ouest des États-Unis"; Morwenstow couvrait le z*one beam* "Europe". Pour couvrir les deux autres z*one beams*, il fallait disposer d'une station à l'est des États-Unis et d'une autre dans la région est-asiatique.

Deuxième génération de satellites INTELSAT à couverture globale



À la fin des années 70, **Sugar Grove** fut construite dans l'est des États-Unis (la station existait déjà pour écouter les communications russes); elle entra en service en 1980. Toujours dans la fin des années 70, une station fut mise en place à **Hong-Kong**. Dès lors, dans les années 80, les quatre stations – Yakima, Morwenstow, Sugar Grove et Hong-Kong – permettaient l'écoute globale des communications INTELSAT.

Les satelliltes INTELSAT ultérieurs, avec z*one beams* et s*pot beams* en plus des g*lobal beam* et des *hemi beams*, nécessitèrent la mise en place de nouvelles stations dans différentes parties du monde. Arrivés à ce point, il est très difficile d'établir un lien entre la création de nouvelles stations et/ou l'installation de nouvelles antennes satellitaires.

Comme, de plus, on a beaucoup de mal à obtenir des informations concernant les stations, il est impossible de savoir précisément quels satellites, avec quels *beams*, sont captés par quelle station. Toutefois, on peut déterminer dans quels *beams* se trouvent des stations connues.

5.3.2.2. La couverture globale par stations qui écoutent manifestement des satellites de communication

À l'heure actuelle, les communications globales par satellite sont assurées par des satellites INTELSAT, INMARSAT et INTERSPUTNIK. Comme dans le cas des premières générations de satellites, la répartition en trois zones de couverture (zones indienne, pacifique et atlantique) est maintenue. Dans chacune des zones de couverture, on trouve des stations qui répondent aux critères caractéristiques des stations d'écoute.

Satellites en orbite au-dessus de l'océan Indien

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT zone indienne	Geraldton, Australie Pine Gap, Australie Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australie Pine Gap, Australie Misawa, Japon

Satellites en orbite au-dessus du Pacifique

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT zone pacifique	Waihopai, Nouvelle-Zélande Geraldton, Australie Pine Gap, Australie Misawa, Japon Yakima, États-Unis: uniquement Intelsat et Inmarsat

Satellites en orbite au-dessus de l'Atlantique

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT zone atlantique	Sugar Grove, États-Unis Buckley Field, États-Unis Sabana Seca, Puerto Rico Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni
INTELSAT 707 (359°)	Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni

On voit donc qu'une écoute globale des communications est possible.
En outre, il existe encore d'autres stations qui, si elles ne répondent certes pas au critère de dimension d'antennes, peuvent cependant faire partie du système d'écoute global. Ces stations permettraient, par exemple, d'intercepter les z*ones beams* ou s*pot beams* de satellites dont les g*lobal beams* sont écoutés par d'autres stations ou pour les g*lobal beams* desquels il n'est pas nécessaire de disposer de grandes antennes satelllitaires.

5.3.2.3. Les stations: détails

Pour la description détaillée des stations, on distingue entre, d'une part, stations qui écoutent manifestement des satellites de communication (critères de la section 5.2) et, d'autre part, stations dont la mission ne peut être prouvée sur la base des critères susmentionnés.

5.3.2.3.1. Stations destinées à l'écoute de satellites de communication

Les critères décrits à la section 5.2, qui peuvent être considérés comme indices de l'existence d'une station d'écoute de satellites de communication, sont aussi valables pour les stations suivantes:

Yakima, États-Unis (120°O, 46°N)

La station a été créée en 1970, en même temps que la première génération de satellites. Depuis 1995, la Air Intelligence Agency (AIA) est sur place, avec le 544th Intelligence Group (Detachment 4). Le Naval Security Group (NAVSECGRU) y est également stationné. La station compte six antennes satellitaires, dont les sources ne permettent pas de connaître la dimension. Selon Hager, ce sont des antennes satellitaires de grande dimension et elles sont orientées sur des satellites Intelsat en orbite au-dessus du Pacifique (deux antennes satelliltaires) et sur des satellites Intelsat en orbite au-dessus de l'Atlantique; des antennes sont orientées sur les satellites Inmarsat 2.

Le fait que Yakima a été créée en même temps que la première génération de satellites Intelsat, d'une part, et la description générale des missions du 544th Intelligence Group, d'autre part, donnent à penser que Yakima joue un rôle dans la surveillance globale des communications. Autre indice: Yakima est proche d'une station de réception de satelllites, située à 100 miles au nord.

Sugar Grove, États-Unis (80°O, 39°N)

Sugar Grove a été créée en même temps qu'était mise en service la deuxième génération de satellites Intelsat, à la fin des années 70. Y sont stationnés le NAVSECGRU ainsi que l'AIA, avec le 544th Intelligence Group (Detachment 3). Selon plusieurs auteurs, la station compte dix antennes satellitaires, dont trois ont plus de 18 mètres (18,2 mètres, 32,3 mètres et 46 mètres) et conviennent donc clairement pour écouter des satellites de communication. À la station, une des missions du Detachment 3 du 544th IG est de fournir un "intelligence support" pour la collecte, par les stations de la Navy, d'informations provenant de satellites de communication[37].

De plus, Sugar Grove est située à proximité (60 miles) de la station de réception de satellites Etam.

Sabana Seca, Puerto Rico (66°O, 18°N)

En 1952, le NAVSECGRU fut stationné à Sabana Seca. Depuis 1995, s'y trouve aussi la AIA, avec le 544th IG (Detachment 2). La station compte au moins une antenne satellitaire d'un diamètre de 32 mètres et quatre autres antennes satellitaires de petite dimension.

Officiellement, les missions de la station sont: traitement des communications par satellite ("performing satellite communication processing"), "cryptologic and communications service" et appui à des missions de la Navy et du DoD (notamment, collecte d'informations COMSAT (d'après le 544th IG)). À l'avenir, Sabana Seca doit devenir la première station d'analyse et de traitement de communications par satellite.

Morwenstow, Royaume-Uni (4°O, 51°N)

Tout comme Yakima, Morwenstow a été créée en même temps que la première génération de satelllites Intelsat, au début des années 70. Morwenstow est desservie par le service de renseignements britannique (GCHQ). Morwenstow compte environ 30 antennes satellitaires, dont deux d'un diamètre de 30 mètres; on ne dispose pas de données concernant la dimension des autres antennes.

[37] „It provides enhhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations.“ aus der Homepage der (44th Intelligence Group http://www.aia.af.mil

Par les sources officielles, on ne sait rien de la mission de la station. Mais la dimension et le nombre de ses antennes satellitaires ainsi que le fait qu'elle soit implantée à seulement 110 km de la station télécom de Goonhilly ne permettent aucun doute: il s'agit d'une station d'écoute de satellites de communication.

Menwith Hill, Royaume-Uni (2°O, 53°N)

Menwith Hill a été créée en 1956. En 1974, la station comptait déjà 8 antennes satellitaires. Depuis, on y trouve quelque 30 antennes satellitaires, dont plusieurs d'un diamètre supérieur à 20 mètres. A Menwith Hill, Britanniques et Américains coopèrent. Pour les Américains, y sont stationnés le NAVSECGRU, la AIA (451st IOS) ainsi que l'INSCOM, qui a le commandement de la station. Le site de Menwith Hill appartient au ministère britannique de la Défense et est loué au gouvernement américain. Officiellement, la mission de Menwith Hill est: "to provide rapid radio relay and to conduct communications research". Selon Richelson et la Fédération des scientifiques américains, Menwith Hill est à la fois une station terrestre pour satellites d'espionnage et une station terrestre pour satellites de communications russes.

Geraldton, Australie (114°O, 28°S)

La station existe depuis le début des années 90. Elle est dirigée par les services secrets australiens (DSD); des Britanniques, précédemment stationnés à Hong Kong (voir plus haut), font à présent partie du personnel de la station. Selon Hager, six antennes satellitaires, dont au moins une d'un diamètre de quelque 20 mètres (évaluation), sont orientées vers des satellites en orbite au-dessus de l'océan Indien et vers des satellites en orbite au-dessus du Pacifique. Selon des experts entendus sous serment au Parlement australien, Geraldton écoute des satellites de communication[38].

Pine Gap, Australie (133°O, 23°S)

La station de Pine Gap a été créée en 1966. Elle est dirigée par les services secrets australiens (DSD); à peu près la moitié des quelque 900 personnes qui y sont stationnées sont des Américains de la CIA et du NAVSECGRU[39].

Pine Gap compte 18 antennes satellitaires, dont une d'un diamètre d'environ 30 mètres et une d'un diamètre d'environ 20 mètres. Selon des sources officielles et différents auteurs, cette station est, depuis le début, une station terrestre pour satellites SIGINT. La station contrôle et commande plusieurs satellites d'espionnage, dont elle capte, traite et analyse les signaux. Toutefois, la présence des grandes antennes satellitaires donne à penser que la station écoute aussi des satellites de communication, car les satellites SIGINT ne nécessitent pas des antennes satellitaires de grande dimension. Jusqu'en 1980, les Australiens étaient exclus du département d'analyse des signaux. Depuis, ils ont libre accès à toutes les parties de la station, à l'exception de la salle de cryptographie nationale des Américains.

Misawa, Japon (141°O, 40°N)

La station de Misawa existe depuis 1948. Y sont stationnés des Japonais et des Américains. Pour les États-Unis, il y a le NAVSECGRU, l'INSCOM ainsi que certains groupes de la AIA (544th IG, 301st IS). Officiellement, Misawa est un "Cryptology Operations Center". Selon Richelson, Misawa permet d'écouter les satellites russes Molnya ainsi que d'autres satellites de communication russes.

[38] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

[39] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

Waihopai, Nouvelle-Zélande (173°O, 41°S)
Waihopai existe depuis 1989. Depuis, on y trouve une grande antenne d'un diamètre de 18 mètres; par la suite, on a ajouté une deuxième antenne, plus petite. Selon Hager, la grande antenne est orientée sur des Intelsat 701 en orbite au-dessus du Pacifique.

Buckley Field, États-Unis, Denver Colorado (104°O, 40°N)
La station a été créée en 1972. Y sont stationnés le 544th IG (Det. 45). La station compte environ cinq antennes satellitaires, dont quatre d'un diamètre d'environ 20 mètres. Officiellement, la station a pour mission de collecter, d'exploiter et d'analyser des données obtenues grâce à des satellites SIGINT concernant les phénomènes nucléaires. Mais la dimension des antennes satellitaires donne à penser que la station joue un rôle dans l'interception de communications civiles.

Hong Kong (22°N, 114°O)
Créée à la fin des années 70, en même temps que la deuxième génération d'Intelsat, la station était équipée de grandes antennes satellitaires. On ne dispose pas de données concernant les dimensions précises. En 1994, on a entamé le démantèlement de la station de Hong Kong. Les antennes ont été transférées en Australie. On ne sait pas quelle station a repris les missions d'Hong Kong: Geraldton, Pine Gap ou Misawa, au Japon. Ces missions pourraient avoir été réparties sur différentes stations.

5.3.2.3.2. Autres stations

S'agissant des stations ci-dessous, les critères susmentionnés ne permettent pas d'en déterminer clairement la fonction:

Leitrim, Canada (75°O, 45°N)
Leitrim fait partie d'un programme d'échanges entre unités militaires canadiennes et américaines. Selon la Navy, quelque 30 personnes y sont stationnées. En 1985, on y installa la première de quatre antennes satellitaires, dont les deux plus grandes ont un diamètre d'environ 12 mètres seulement (évaluation). Officiellement, la mission de la station est le "cryptologic rating" et l'écoute de communications diplomatiques.

Bad Aibling, Allemagne (12°O, 47°N)
La station, implantée à proximité de Bad Aibling et où travaillent quelque 750 Américains, a été reprise en 1952 par l'armée américaine (de 1972 à 1994, elle dépendait du Department of Defence). Sont stationnés à Bad Aibling le NAVSECGRU, l'INSCOM (66th IG, 718 IG) ainsi que divers groupes de l'AIA (402nd IG, 26th IOG). On trouve là 14 antennes satellitaires, dont aucune de plus de 18 mètres. Officiellement, Bad Aibling accomplit les missions suivantes: "rapid radio relay and secure commo, support to DoD and Unified Commands, medium and longhand commo HF& satellite, communication physics research, test and evaluate commo equipment". Selon Richelson, Bad Aibling est une station terrestre pour satellites SIGINT et satellites de communication russes.

Ayios Nikolaos, Chypre (32°O, 35°N)
Ayios Nikolaos (Chypre) est une station britannique. Elle compte neuf antennes satellitaires, de grandeur inconnue. Ses missions sont réparties entre deux unités: "Signals Regiment Radio et Signals Unit (RAF)".

Sa proximité par rapport aux États arabes et le fait qu'elle est la seule station à être située à l'intérieur de plusieurs zones de couverture (notamment des *spot beams*) de la région donnent à penser que la station de Ayios Nikolaos joue un rôle important en matière d'obtention de renseignements.

Shoal Bay, Australie (134°O, 13°S)
Shoal Bay est une station desservie uniquement par le service australien de renseignements. La station compterait dix antennes satellitaires, dont les dimensions ne sont pas précisées. D'après des photographies, les cinq plus grandes ont un diamètre de 8 mètres maximum, et la sixième que l'on peut voir a un diamètre encore inférieur. Selon Richelson, les antennes sont orientées vers les satellites PALAPA indonésiens. La station ferait-elle partie du système global d'écoute des communications civiles? On l'ignore.

Guam, Pacifique (144°O, 13°S)
Guam existe depuis 1898. Elle abrite aujourd'hui une Naval Computer and Telecommunication Station, où sont stationnés le 544th IG de la AIA ainsi que des soldats de la Navy. La station compte au moins deux antennes satellitaires, de dimension inconnue. Aussi la fonction de Guam demeure-t-elle peu claire.

Kunia, Hawaï (158°O, 21°N)
Depuis 1993, cette station est un Regional Security Operation Center (RSOC), desservi par le NAVSECGRU et l'AIA. Elle a notamment pour missions la mise à disposition d'informations et de communications, ainsi que le soutien cryptologique. La fonction de Kunia demeure peu claire.

Medina Annex, États-Unis, Texas (98°O, 29°N)
Tout comme Kunia, Medina – créée en 1993 – est un Regional Security Operation Center, qui est desservi par le NAVSECGRU et des unités de l'AIA. Ses missions concernent les Caraïbes.

Fort Gordon (81°O, 31°N)
Fort Gordon est aussi un Regional Security Operation Center. Il est desservi par l'INSCOM et l'AIA (702nd IG, 721st IB, 202nd IB, 31st IS). On n'est pas sûr de ses missions.

Fort Mead, États-Unis (76°O, 39°N)
Fort Mead est le quartier général de la NSA.

5.3.3. Résultats: résumé

Des données réunies en ce qui concerne les stations et les satellites, et des préalables exposés plus haut, on peut tirer les conclusions suivantes:

1. Dans chaque zone de couverture, il existe, pour au moins quelques-uns des g*lobal beams*, des stations d'écoute munies chacune d'au moins une antenne d'un diamètre supérieur à 18 mètres et desservies par des Américains ou des Britanniques et/ou où des Américains ou des Britanniques exercent des activités de renseignement. C'est là un indice fort de l'existence d'un système d'écoute global.

2. Le développement des communications par INTELSAT et l'apparition simultanée de stations d'écoute correspondantes attestent l'orientation globale du système.

3. À partir des points 1 et 2 ci-dessus, il est possible d'identifier certaines stations comme stations qui écoutent les communications internationales par satellite.

4. Les données figurant dans les documents déclassifiés et les données fournies par les opérateurs (AIA, NSA, Navy, etc.) peuvent être considérées comme attestant l'existence des stations qui y sont mentionnées.

5. Certaines stations se trouvent simultanément dans des *beams* et/ou *spots* de plusieurs satelllites, de sorte qu'une grande partie des communications peut être interceptée.

6. Il existe quelques autres stations qui ne sont pas munies de grandes antennes, mais qui peuvent cependant faire partie du système, car elles sont capables de capter des communications en provenance des *beams* et *spots*. Là, il faut renoncer à l'indice de la dimension des antennes et recourir à d'autres indices.

7. Il est démontré que certaines des stations mentionnées se trouvent à proximité immédiate de stations terrestres régulières de satellites de communication.

5.4. L'accord UKUSA

On appelle accord UKUSA un accord SIGINT signé en 1948 par le Royaume-Uni, les États-Unis, l'Australie, le Canada et la Nouvelle-Zélande.

5.4.1. Genèse de l'accord UKUSA[40]

L'accord UKUSA est un prolongement de la coopération très étroite qui a uni les États-Unis et la Grande-Bretagne pendant la deuxième guerre mondiale et qui s'était esquissée dès la première guerre mondiale.

L'intiative visant à la création d'une allliance SIGINT fut prise par les Américains, en août 1940, lors d'une rencontre entre Américains et Britanniques, à Londres[41]. En février 1941, les crypto-analystes américains envoyèrent en Grande-Bretagne une machine à décoder (PURPLE). La coopération en matière de crypto-analyse débuta au printemps 1941[42]. La coopération entre services de renseignements fut renforcée par l'engagement commun des flottes dans l'Atlantique nord, à l'été 1941. En juin 1941, les Britanniques réussirent à casser ENIGMA, le code de la

[40] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 -109

[41] ibidem, p. 99: „At a metteing in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,´ and said that ´the time had come or a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol.I, pp.312-13)

[42] Ibidem, p. 100: „ In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration"

marine allemande.

L'entrée en guerre de l'Amérique renforça encore la coopération SIGINT. En 1942, des cryptologues américains de la "naval SIGINT agency" commencèrent à travailler au Royaume-Uni[43]. La communication entre les "U-Boot Tracking-Rooms" de Londres, de Washington, puis, à partir de 1943, de Ottawa (Canada) devint à ce point étroite que, selon les participants, elles travaillaient comme une organisation unique[44].

Le printemps 1943 vit la signature de l'accord BRUSA-SIGINT ainsi qu'un échange de personnel. Le contenu de l'accord, qui concerne notamment le partage du travail, est résumé dans les trois premiers paragraphes: échange de toute information provenant de la découverte, de l'identification et de l'écoute de signaux, ainsi que des algorythmes des codes et clés de cryptage. Les Américains étaient compétents pour le Japon; les Britanniques pour l'Allemagne et l'Italie[45].

Après la guerre, c'est surtout la Grande-Bretagne qui préconisa le maintien d'une alliance SIGINT. Les bases en furent convenues lors d'une tournée mondiale effectuée, au printemps 1945, par des agents de renseignement britanniques (parmi lesquels Sir Harry Hinsley, dont les livres sont à la base de l'article cité). Un des objectifs était d'envoyer du personnel SIGINT d'Europe dans le Pacifique, dans le cadre de la guerre contre le Japon. Dans ce contexte, il fut convenu avec l'Australie de mettre des ressources et du personnel (britannique) à la disposition des services australiens. Le voyage de retour, via la Nouvelle-Zélande et le Canada, conduisait aux États-Unis.

En septembre 1945, Truman signa un mémorandum top secret qui constituait la clef de voûte d'une alliance SIGINT en temps de paix[46]. Puis Britanniques et Américains ouvrirent des négociations en vue de la conclusion d'un accord. De plus, une délégation britannique prit contact avec les Canadiens et les Australiens, pour discuter d'une participation éventuelle. En février et mars 1946, une conférence SIGINT anglo-américaine se tint dans le plus grand secret, pour discuter des détails. Les Britanniques étaient mandatés par les Canadiens et les Australiens. La conférence produisit un accord de quelque 25 pages, toujours classifié, qui arrêtait les détails d'un accord SIGINT entre les États-Unis et le Commonwealth britannique. D'autres négociations eurent lieu au cours des deux années suivantes, de sorte que le texte final de l'accord dit UKUSA put être signé en juin 1948[47].

5.4.2. Éléments attestant l'existence de l'accord

À ce jour, les États signataires n'ont jamais reconnu officiellement l'existence de l'accord UKUSA. Mais plusieurs éléments attestent clairement son existence.

---

[43] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol II, p.56)
[44] Ibidem, p. 101 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol. II, p 48)
[45] Ibidem, p.101-2: Interivews mit Sir F.H. Hinsley, „Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW
[46] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: „The Secretary of War and the Secretary of the Navy are hereby authorised ti direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Oerations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States." (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))
[47] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing

5.4.2.1 Liste des acronymes utilisés par la Navý

Selon la marine américaine[48], UKUSA veut dire "United Kingdom, USA" et désigne "un accord SIGINT entre cinq nations".

5.4.2.2 Déclaration du directeur du DSD

Lors d'une interview, le directeur du service de renseignements australien (DSD) a confirmé l'existence de cet accord: selon lui, les services secrets australiens coopèrent avec d'autres services de renseignements d'outre-mer dans le cadre de l'accord UKUSA[49].

5.4.2.3 Rapport du Canadian Parliamentary Security and Intelligence Committee

Ce rapport indique que le Canada coopère, en matière de renseignements, avec certains de ses alliés les plus anciens et les plus proches. Il nomme ces alliés: les États-Unis (NSA), le Royaume-Uni (GCHQ), l'Australie (DSD) et la Nouvelle-Zélande (GCSB). Il ne donne pas la dénomination de l'accord.

5.4.2.4 Déclaration de M. Louis Torella, ancien directeur adjoint de la NSA

Dans une interview donnée, en novembre 1987 et avril 1992, à Christopher Andrew, professeur à l'Université de Cambridge, M. Louis Torella, qui était présent lors de la signature, confirme l'existence de l'accord[50].

5.4.2.5 Lettre de M. Joe Hooper, ancien directeur du GCHQ

Dans une lettre au Marshall S. Carter, ancien directeur de la NSA, M. Joe Hooper, ancien directeur du GCHQ, confirme l'existence de l'accord UKUSA.

5.4.2.6 Interlocuteurs du rapporteur

Le rapporteur a discuté de l'accord UKUSA avec plusieurs personnes qui, de par leurs fonctions, doivent connaître cet accord et son contenu. Dans tous les cas, le style des propos tenus a confirmé indirectement l'existence de cet accord.

5.5. Exploitation des documents américains ayant cessé d'être classés confidentiels

5.5.1. Nature des documents

Dans le cadre du "Freedom of Information Acts" de 1966 (5 U.S.C. § 552) et du règlement du ministère de la défense (DoD FOIA règlement 5400.7-R de 1997), des documents classés

[48] „Terms/Abbreviations/Acronyms“ veröffentlicht durch das US Nave and Marine Corps Intelligence Training Centre (NMITC) bei http://www.cnet.navy.mil/nmitc/training/u.html
[49] Martin Brady, Direktor des DSD, Canberra 16. März 2000
[50] Andrew, Christopher „The growth of the Australian Intelligence Community and the Anglo-American Connection“, pp. 223-4

précédemment secrets ont cessé de l'être et sont ainsi devenus accessibles à tous.

Le public peut avoir accès aux documents par l'intermédiaire de la National Security Archive créée en 1985 (George Washington University, Washington D.C.). Jeffrey Richelson, ancien membre de la National Security Archive, a communiqué par internet 16 documents, qui donnent une idée de la genèse, du développement, de la gestion et du mandat de la NSA (National Security Agency)[51]. De plus, deux des documents citent le nom d'ECHELON. Ces documents sont sans cesse mentionnés par différents auteurs ayant écrit à propos d'ECHELON, qui les considèrent comme la preuve de l'existence du système d'espionnage mondial ECHELON. En outre, certains des documents mis à disposition par Richelson, confirment l'existence du NRO (National Reconnaissance Office) et constatent que sa mission consiste à gérer et à exploiter les satellites SIGINT[52].

5.5.2. Contenu des documents

Dans ces documents, on peut trouver des descriptions ou mentions fragmentaires des thèmes suivants:

5.5.2.1. Mission et conception de la NSA (documents 1, 4, 10, 11 et 16)

Dans la directive 9 du National Security Council Intelligence (NSCID 9) du 10 mars 1950, la notion de communication extérieure est définie au sens du COMINT; c'est ainsi qu'il faut entendre par **communication extérieure toute communication gouvernementale au sens large (pas uniquement militaire), ainsi que toute autre communication, pouvant contenir des informations d'intérêt militaire, politique, scientifique ou économique**.

La directive (NSCID 9 rév. du 29.12.1952) stipule que le FBI est seul responsable pour la sécurité intérieure.

La directive du ministère de la défense du 23 décembre 1991 (DoD) concernant la NSA et le Central Security Service (CSS) définit comme suit ce concept pour la NSA:

– la NSA est un service distinct au sein du ministère de la défense, qui est placé sous la direction du ministère de la défense;

– la NSA assure, d'une part, la mission SIGINT des États-Unis et met, d'autre part, à la disposition de tous les ministères et services des systèmes de communication sûrs;

– l'activité SIGINT de la NSA ne s'étend pas à la production et à la diffusion d'informations déjà traitées. Cette tâche est du ressort d'autres ministères et services.

Par ailleurs, la directive DoD de 1991 présente, dans les grandes lignes, la structure de la NSA et du CSS.

Dans une déclaration qu'il a faite le 12 avril 2000 devant la commission d'enquête permanente "Renseignement" de la chambre des représentants, Hayden, directeur de la NSA, décrit comme suit les missions de la NSA:

– la surveillance électronique sert à rassembler des communications extérieures à

[51] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html.
[52] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html.

l'intention des militaires et responsables politiques (décideurs politiques);

– la NSA fournit aux consommateurs gouvernementaux américains des renseignements sur le terrorisme international, la drogue, la prolifération des armements;

– la NSA n'a pas pour mission de collecter toutes les communications électroniques;

– la NSA ne peut transmettre des informations qu'à des destinataires autorisés par le gouvernement; elle ne peut en transmettre directement aux entreprises américaines.

Dans un mémorandum du vice-amiral des forces navales américaines, W.O. Studeman, établi au nom du gouvernement, en date du 8 avril 1992, il est fait état du caractère de plus en plus mondial (access) de la mission de la NSA, parallèlement au "Support of military operations".

5.5.2.2. Pouvoirs des services de renseignement (document 7)

Il ressort de la directive 18 de l'United States Signals Intelligence (USSID 18) que les signaux acheminés par câble comme les signaux hertziens sont interceptés.

5.5.2.3. Coopération avec d'autres services (documents 2 a et 2 b)

Au nombre des tâches incombant au Communications Intelligence Board américain, il y a notamment la surveillance de tous les "arrangements" avec les gouvernements étrangers dans le domaine COMINT. Le directeur de la NSA est entre autres responsable de tous les contacts avec les services COMINT étrangers.

5.5.2.4. Mention des unités actives sur les "sites ECHELON" (documents 9 et 12)

Dans les instructions C5450.48A du NAVSECGRU, le mandat, la fonction et l'objectif de la Naval Security Group Activity (NAVSECGRUACT), 544e Intelligence Group de Sugar Grove, Virginie occidentale, sont décrits. Il y est indiqué qu'une mission spécifique consiste à gérer et exploiter un site ECHELON; une autre mission citée est le traitement des informations provenant des services de renseignement.

Dans le document "History of the Air Intelligence Agency – 1 january to 31 December 1994" (RCS: HAF-HO (A&SA) 7101, volume 1), il est fait mention au point "Activation of Echelon Units" de l'Air Intelligence Agency (AIA), detachment 2 et 3:

Les documents ne disent nullement en quoi consiste un "site ECHELON", ce qui est fait sur un "site ECHELON", ni ce que recouvre l'appellation ECHELON. De même, les documents ne permettent pas de savoir en quoi consiste l'accord UKUSA.

5.5.2.5. Mention de stations (documents 6, 9 et 12)

– Sugar Grove (Virginie occidentale), dans les NAVSECGRU INSTRUCTIONS C5450.48A,

– Misawa Air Base (Japon), in History of the Air Intelligence Agency – January to

31 december 1994 (RCS: HAF-HO (A&SA)7101, volume 1),

– Porto Rico (Sabana Seca), ibidem,

– Guam, ibidem,

– Yakima (Washington), ibidem,

– Fort Meade (Maryland); un rapport COMINT de la NSA émanant de Fort George G. Meade (Maryland), en date du 31 août 1972, prouve l'existence d'activités COMINT en cet endroit.

5.5.2.6. Protection de la vie privée des citoyens américains (documents 7, 7a à f, 11 et 16)

Les NAVSECGRU INTRUCTIONS C5450.48A arrêtent qu'il faut protéger la vie privée des citoyens.

Différents documents expliquent que la vie privée des citoyens américains doit être protégée, indiquant comment le faire (Baker, General Counsel, NSA, lettre du 9 septembre 1992, United States Signals Intelligence Directive (USSID) 18, 20 octobre 1980, et différents suppléments[53].

5.5.2.7. Définitions (documents 4, 5 a et 7)

La directive du ministère de la défense du 23 décembre 1991 donne des définitions précises de SIGINT, COMINT, ELINT et TELINT, tout comme la directive n° 6 du National Security Council Intelligence du 17 février 1972.

Selon ces définitions, il faut entendre par COMINT la collecte et le traitement des communications extérieures (acheminées par des moyens électromagnétiques), ainsi que l'interception et le traitement des communications écrites non cryptées, de la presse et de la propagande, à moins qu'elle ne soit cryptée.

5.5.3. Résumé

1. Voici 50 ans déjà, les informations jugées intéressantes concernaient les domaines non seulement de la politique et de la sécurité mais aussi de la science et de l'économie.

2. Les documents prouvent que la NSA collabore avec d'autres services dans le domaine COMINT.

3. Les documents qui fournissent des renseignements sur l'organisation de la NSA, les missions de celle-ci et ses liens avec le ministère de la défense n'apportent pas véritablement de renseignements supplémentaires par rapport aux sources publiquement accessibles de la page d'accueil de la NSA.

[53] Dissemination of U.S. Government Organizations and Officials, Memorandum du 5 février 1993; Reporting Guidance on References to the First Lady, 8 juillet 1993; Reporting Guidance on Former President Carter's Involvement in the Bosnian Peace Process, 15 décembre 1994; Understanding USSID 18, 30 septembre 1997; USSID 18 Guide, 14 février 1998;
NSA/US IDENTITIES IN SIGINT, mars 1994; Statement for the record of NSA Director Lt Gen. Michael V. Hayden, USAF, 12 avril 2000).

4. Les communications par câble peuvent être interceptées.

5. Le 544e Intelligence groupe et les Detachments 2 et 3 de l'Air Intelligence Agency participent à la collecte des informations du renseignement.

6. Le nom d'"ECHELON" apparaît dans différents contextes.

7. S'agissant des stations SIGINT, les noms suivants sont cités: Sugar Grove (Virginie occidentale), Misawa Air Base (Japon), Porto Rico (Sabana Seca), Guam, Yakima (État de Washington).

8. Les documents indiquent comment la vie privée des citoyens américains doit être protégée.

S'ils n'apportent aucune preuve concrète, les documents n'en fournissent pas moins de véritables indices, qui conjointement avec d'autres, permettent de tirer des conclusions.

5.6. RENSEIGNEMENTS ÉMANANT D'AUTEURS SPÉCIALISÉS ET DE JOURNALISTES

5.6.1. Livre de Nicky Hager

Dans le livre de Nicky Hager "Secret Powers – New Zealand's role in the international spy network" paru en 1996, le système ECHELON est décrit pour la première fois dans le détail. Selon l'auteur, l'origine du système ECHELON remonte à 1947, année où, dans le prolongement de la coopération de l'époque de guerre, le Royaume-Uni et les États-Unis sont convenus de poursuivre à l'échelle mondiale pour ainsi dire les activités de "renseignement transmissions" (COMINT). Ces deux pays devaient collaborer pour mettre en place un système d'interception autant que possible mondial, étant entendu qu'ils se partageraient les équipements spécifiques nécessaires à cet effet, ainsi que les dépenses occasionnées, et qu'ils auraient l'un et l'autre accès aux résultats. Par la suite, le Canada, l'Australie et la Nouvelle-Zélande ont adhéré au pacte UKUSA.

Selon Hager, l'interception des communications satellitaires constitue l'élément central du système actuel. Dès les années 70, les communications acheminées par Intelsat – le premier système mondial de télécommunications par satellites[54] – furent interceptées par des stations au sol. Ces informations étaient alors étudiées aux moyens d'ordinateurs sur la base de mots-clés ou d'adresses préprogrammés en sorte de filtrer les informations importantes. Par la suite, la surveillance a été étendue à d'autres satellites, comme par exemple ceux d'Inmarsat[55], organisation dont les activités concernent principalement les communications maritimes.

Hager signale dans son livre que l'interception des communications satellitaires ne constitue

[54] Cf. à ce propos: http://www.intelsat.int/index.htm.
[55] Cf. à ce propos: http://www.inmarsat.org/index3.html.

qu'une composante – certes importante – du système d'interception géant. Parallèlement, il existerait de nombreuses autres installations de surveillance du faisceau hertzien et des câbles, à propos desquelles les documents sont toutefois moins nombreux et dont il est difficile de prouver l'existence, dès lors que contrairement aux stations au sol, elles peuvent pratiquement passer inaperçues. Echelon est ainsi devenu le synonyme d'un système d'interception mondial.

5.6.2. Déclarations de Duncan Campbell

Dans l'étude 2/5 de 1999 du STOA qui examine de façon approfondie les aspects techniques, dont il a été question précédemment, Duncan Campbell démontrait dans le détail – en expliquant comment – que chaque moyen utilisé aux fins de communication pouvait être intercepté. Dans une de ses dernières études, il constatait toutefois clairement qu'ECHELON avait lui aussi ses limites, et que l'idée selon laquelle une surveillance sans faille était possible s'était révélée infondée, soulignant qu'ECHELON et le système d'espionnage électronique dont il forme une partie ne sont pas en mesure d'assurer une telle surveillance, et qu'en outre, l'équipement qui permettrait de traiter et de reconnaître la nature de toute communication orale ou de tout appel téléphonique n'existait pas[56].

5.6.3. Déclarations de Jeff Richelson

Jeff Richelson, ancien membre des National Security Archives, a fourni par internet l'accès à seize documents précédemment secrets qui donnent un aperçu de la genèse, du développement, de la gestion et du mandat de la NSA (National Security Agency)[57].

Il est en outre l'auteur de différents ouvrages et articles sur les activités des services de renseignements des États-Unis. Dans son livre intitulé "The ties that binds"[58], publié en 1985, il décrit dans le détail la genèse de l'accord UKUSA et les activités menées dans ce contexte par les services secrets participants des États-Unis, du Royaume-Uni, du Canada, d'Australie et de Nouvelle-Zélande.

Dans son volumineux ouvrage intitulé "The U.S Intelligence Community"[59], de 1999, il donne un aperçu des activités des services secrets des États-Unis, des structures d'organisation des services, de leurs méthodes de collecte et d'analyse du renseignement. Au chapitre 8 de cet ouvrage, il fournit des détails sur les capacités SIGINT des services et décrit quelques stations au sol. Au chapitre 13, il évoque les relations des États-Unis avec d'autres services de renseignements, notamment l'accord UKUSA. Il cite le nom ECHELON en tant que nom de code d'un système d'échange informatisé.

Dans un article intitulé "Desperately seeking Signals"[60], publié en 2000, il présente brièvement l'accord UKUSA, cite des installations d'interception de communications par satellites et évoque les possibilités et les limites de l'interception de communications civiles.

5.6.4. Déclarations de James Bamford

[56] Duncan Campbell, Inside Echelon. The history, structure and function of the global surveillance system knows as Echelon, p. 1.
[57] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[58] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London
[59] Jeffrey T. Richelson 1999 (4th ed.): „The U.S. Intelligence Community“, Westview Press
[60] Jeffrey T. Richelson 2000: „Desperately seeking Signals“ The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No. 2, pp. 47-51

À insérer par la suite.

5.6.5. Déclarations de Bo Elkjaer et de Kenan Seeberg

Les deux journalistes danois Bo Elkjaer et Kenan Seeberg ont déclaré, le 22 janvier 2001 devant la commission, qu'ECHELON avait déjà atteint un stade très avancé dans les années 80, et que le Danemark collaborait avec les États-Unis depuis 1984.

5.7. Déclarations d'anciens collaborateurs des services de renseignements

5.7.1. Margaret Newsham (ex-collaboratrice de la NSA)

Margaret Newsham[61] a été employée, de 1974 à 1984, par Ford et Lockheed, et elle a travaillé pendant ce temps, selon ses propres dires, pour la NSA. Elle a été formée pour son travail au quartier général de la NSA à Fort George Meade (Maryland, États-Unis), et a travaillé en 1977 et 1978 à Menwith Hill, la station terrestre américaine en territoire britannique. Là, elle a eu l'occasion d'écouter une conversation du sénateur américain Strohm Thurmond au sénat. Dès 1978, ECHELON pouvait intercepter les télécommunications d'une personne donnée effectuées par satellite.

S'agissant de son propre rôle au sein de la NSA, elle aurait eu la responsabilité d'élaborer des systèmes et programmes, de les configurer et de les rendre opérationnels sur de grands ordinateurs. Les logiciels s'appelaient SILKWORTH et SIRE, ECHELON étant le nom du réseau.

5.7.2. Wayne Madsen (ancien collaborateur de la NSA)

Wayne Madsen[62], ancien collaborateur de la NSA, confirme également l'existence d'ECHELON. Selon lui, la collecte des données économique se voit reconnaître un caractère véritablement prioritaire et son objet consiste à procurer des avangages aux entreprises américaines. Il craint en particulier qu'ECHELON ait pu espionner des ONG comme Amnesty International ou Greenpeace. Il déclare également que la NSA a dû admettre qu'elle disposait de plus de mille pages d'informations sur la princesse Diana, dont la campagne contre les mines terrestres dérangeait la politique américaine.

[61] Cf. pour ce qui suit Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.
[62] http://cryptome.org/echelon-60min.htm.

5.7.3. Mike Frost (ancien collaborateur des services secrets canadiens)

Mike Frost a travaillé pendant plus de vingt ans dans le service secret canadien CSE[63]. La station d'interception d'Ottawa ne serait qu'un élément d'un réseau mondial de stations d'espionnage[64]. Dans une interview accordée à la CBS, il a déclaré que partout dans le monde, chaque jour, les communications téléphoniques, les courriers électroniques et les fax étaient surveillés par ECHELON, qui était un réseau de surveillance secret du gouvernement[65]. Il en allait également ainsi pour les communications civiles. À titre d'exemple, il cite dans une interview accordée à une radio australienne, un cas dans lequel le CSE avait effectivement enregistré le nom et le numéro de téléphone d'une femme dans une base de données concernant des terroristes éventuels, cette femme ayant employé une notion ambigüe dans une conversation téléphonique innocente avec un ami. En filtrant les communications, l'ordinateur avait rencontré le mot-clé et retransmis la communication, le responsable de l'analyse qui ne savait pas réellement que penser, ayant ainsi enregistré ses données personnelles[66].

Les services de renseignement des pays ECHELON s'aideraient également mutuellement, en ce sens qu'un service espionnerait pour le compte d'un autre, en sorte que rien ne pourrait être reproché au service de renseignement local du moins. Ainsi, le GCHQ britannique aurait demandé au CSE canadien d'espionner pour son compte deux ministres anglais, le premier ministre, Mme Thatcher, voulant savoir si ceux-ci se rangeaient à ses côtés[67].

5.7.4. Fred Stock (ancien collaborateur du service secret canadien)

Selon ses propres dires, Fred Stock a été exclu du service secret canadien CSE en 1993, parce qu'il avait protesté contre la nouvelle orientation du service qui mettait davantage l'accent sur des informations économiques et des objectifs civils. Les communications interceptées auraient fourni des informations sur des opérations commerciales avec d'autres pays, notamment les négociations sur l'ALENA, l'achat de céréales par la Chine, et les ventes d'armes françaises. Selon Stock, le service se serait également procuré de façon habituelle des informations sur des actions environnementales menées par des navires de Greenpeace en haute mer[68].

5.8. Informations de sources gouvernementales

5.8.1. Déclarations américaines

James Woolsey, ancien directeur de la CIA, a déclaré à l'occasion d'une conférence de presse[69], donnée à la demande du ministère américain des affaires étrangères, que les États-Unis se livraient à des activités d'espionnage en Europe continentale. Le renseignement économique

[63] Interview de NBC "60 Minutes" du 27.2.2000; http://cryptome.org/echelon-60min.htm.
[64] Communication Security Establishment, service dépendant du ministère canadien de la défense, qui est chargé de l'activité Sigint.
[65] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special.
[66] Interview de NBC "60 Minutes" du 27.2.2000; http://cryptome.org/echelon-60min.htm.
[67] Interview de la chaîne australienne Channel 9 du 23.3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm.
[68] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html.
[69] Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm.

proviendrait toutefois à hauteur de 95 % de l'exploitation des sources d'information publiques, les secrets volés ne représentant que 5 %. Les données économiques d'autres pays sont espionnées dans des cas en rapport avec le respect de sanctions et les biens à double usage, ainsi que les tentatives de corruption lors de la passation de marchés. Ces informations ne sont toutefois pas communiquées aux entreprises américaines. Woolsey a souligné que même lorsque l'activité d'espionnage des données économiques permet de découvrir des informations dont l'utilisation présenterait un intérêt économique, il faudrait beaucoup de temps à un analyste pour exploiter la quantité importante de données existant dans ce domaine et qu'il serait irrationnel de perdre son temps à espionner des partenaires commerciaux amis. De plus, il a fait observer que même si cela était fait, il serait difficile, compte tenu des interdépendances internationales, de savoir quelle entreprise doit être réputée américaine et se voir confier ainsi les informations obtenues.

Dans un article paru ultérieurement dans the Wall Street Journal Europe[70], Woolsey a répété que les États-Unis espionnaient l'Europe, mais qu'ils ne le faisaient qu'aux fins de détecter des cas de corruption. Dans cet article, il a également affirmé que les États-Unis utilisaient des ordinateurs pour rechercher des données sur la base de mots-clés.

5.8.2. Déclarations anglaises

Il ressort de différentes questions posées au sein de la chambre des Communes[71], que la station de la RAF de Menwith Hill dépend du ministère anglais de la défense, ce qui n'empêche qu'elle est mise à la disposition du ministère américain de la défense, et en particulier de la NSA[72], un membre du personnel de celle-ci étant le chef de la station[73], en tant qu'installation de communication[74]. Au milieu de l'année 2000, Menwith Hill occupait 415 militaires américains, 5 militaires britanniques, 989 civils américains et 392 civils britanniques, compte non tenu des collaborateurs du GCHQ[75]. La présence des troupes américaines est régie par le traité de l'Atlantique nord et par des accords administratifs spéciaux et secrets[76], qui sont jugés conformes aux relations existant entre les gouvernements du Royaume-Uni et des États-Unis dans le contexte d'une défense commune[77]. La station fait partie intégrante du réseau mondial du ministère américain de la défense, qui défend les intérêts du Royaume-Uni, des États-Unis et de l'OTAN[78].

Le rapport annuel 1999/2000 souligne expressément l'importance que revêt l'étroite collaboration dans le cadre de l'accord UKUSA et la qualité des renseignements qu'elle permet d'obtenir. Il est en particulier dit que si les installations de la NSA devenaient inopérationnelles, le GCHQ pourrait, trois jours plus tard, servir non seulement ses clients britanniques mais aussi ses clients américains[79].

---

[70] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, p. 31.
[71] Commons Written Answers, House of Commons Hansard Debares.
[72] 12.7.1995.
[73] 25.10.1994.
[74] 3.12.1997.
[75] 12.5.2000.
[76] 12.7.1995.
[77] 8.3.1999 et 6.7.1999.
[78] 3.12.1997.
[79] Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, présenté au Parlement par le Premier

5.8.3. Déclarations australiennes[80]

Martin Brady, directeur de la DSD, service de renseignement australien[81], a confirmé dans une lettre adressée au programme "Sunday" de la chaîne australienne "Channel 9", que la DSD collaborait avec d'autres services de renseignement dans le cadre de l'UKUSA. Dans la même lettre, il a souligné que l'ensemble des installations de renseignement australiennes était géré par les services australiens seuls ou en commun avec les services américains. Dans les cas où ces installations sont utilisées en commun, le gouvernement australien a pleinement connaissance de toutes les activités, et le personnel australien est associé à tous les stades[82].

5.8.4. Déclarations néerlandaises

Le 19 janvier 2001, le ministre néerlandais de la défense a présenté au Parlement néerlandais un rapport sur les aspects techniques et juridiques de l'interception mondiale des systèmes de télécommunications modernes[83]. Le gouvernement néerlandais y défend l'idée que même s'il ne dispose pas lui-même d'éléments de preuve, il juge, compte tenu des informations disponibles auprès de tiers, très plausible l'existence du réseau ECHELON, mais qu'il est possible qu'existent également d'autres systèmes présentant les mêmes possibilités. Il arrive à la conclusion que l'interception à grande échelle des systèmes de télécommunications modernes n'est pas l'apanage des pays parties au système ECHELON et qu'elle est également pratiquée par les responsables d'autres pays.

5.8.5. Déclarations italiennes

Luigi Ramponi, ex-directeur du service de renseignement italien SISMI, ne laisse lui non plus, dans une interview accordée au journal "Il Mondo", subsister aucun doute quant à l'existence d'ECHELON[84]. Ramponi déclare expressément qu'en sa qualité de chef du SISMI, il était au courant de l'existence d'ECHELON. Depuis 1992, il connaissait l'existence d'une forte activité d'écoute des ondes de basse, moyenne et haute fréquences. Lorsqu'il est arrivé au SISMI en 1991, l'essentiel de travail était en rapport avec le Royaume-Uni et les États-Unis.

5.9. Rapports parlementaires

5.9.1. Rapports du comité permanent R de contrôle belge

---

ministre en novembre 2000.

[80] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp .

[81] Defence Signals Directorate, Service de renseignement australien gérant le MRE (SIGINT).

[82] Lettre de Martin Brady, directeur de la DSD, du 16 mars 1999 à Ross Coulthart, Sunday Program; cf. à ce propos également: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.

[83] Lettre à l'attention de la chambre des députés concernant l'interception à grande échelle des systèmes de télécommunications modernes en date du 19.1.2001.

[84] Francesco Sorti, Dossier. exclusivo. caso Echelon. parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998.

Le comité permanent R de contrôle belge a déjà rendu deux rapports sur le dossier Échelon.

Le troisième chapitre du "Rapport d'activités 1999" est entièrement consacré aux réactions des services belges de renseignement à l'existence éventuelle d'un système Échelon de surveillance des communications. Les auteurs de l'analyse, qui occupe une bonne quinzaine de pages, parviennent à la conclusion que les deux services belges de renseignement, à savoir la Sûreté de l'État et le Service Général du Renseignement (SGR), n'ont obtenu des informations sur ce système qu'au moyen de documents publics.

Le "Rapport complémentaire d'activités 1999" traite du système Échelon d'une manière beaucoup plus approfondie en se prononçant sur les études du STOA. Une partie de ses développements consiste dans l'exposé des conditions techniques et juridiques de l'interception des télécommunications. Il ressort de ses conclusions que le système Échelon existe réellement et permet de capter toutes les informations transmises par satellite (1% environ du nombre total des communications téléphoniques internationales), dès lors qu'est mise en œuvre une recherche par mots clés, et que ses capacités de décryptage sont infiniment supérieures à ce que les Américains veulent bien admettre. Il est permis de mettre en doute les déclarations selon lesquelles aucune activité d'espionnage industriel n'est conduite dans les installations de Menwith Hill. Les auteurs du rapport soulignent expressément l'impossibilité d'établir avec certitude ce que le système Échelon fait ou ne fait pas.

5.9.2. Rapport de la commission de la défense nationale de l'Assemblée nationale française

En France, la commission de la défense nationale a soumis à l'Assemblée nationale un rapport sur les systèmes d'écoute[1].

Après avoir traité en détail les différents aspects de la question, le rapporteur, Arthur Paecht, parvient à la conclusion qu'il existe bien un système d'interception nommé Échelon et qu'il s'agit du seul système multinational connu. Les capacités d'un tel système sont réelles, mais ont atteint leurs limites, non seulement parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications, mais aussi parce que certaines cibles ont appris à se protéger des interceptions.

Le système Échelon a "divergé" par rapport à ses objectifs initiaux, qui étaient liés au contexte de la guerre froide. Aussi n'est-il pas impossible que des informations recueillies soient utilisées à des fins politiques et économiques contre certains membres de l'OTAN.

Échelon peut constituer un danger pour les libertés fondamentales. À ce titre, son existence pose de nombreux problèmes qui appellent des réponses appropriées. Il serait vain d'imaginer que les pays membres du réseau vont cesser leurs activités. Plusieurs indices incitent à croire qu'un

[1] Rapport d'information, déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, n° 2623 - Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

nouveau système s'est constitué pour dépasser les limites d'Échelon grâce à de nouveaux moyens et sans doute de nouveaux partenariats.

6. Peut-il exister d'autres systèmes d'interception mondiaux?

6.1. Conditions nécessaires pour un tel système

6.1.1. Conditions technico-géographiques

Pour pouvoir intercepter des communications internationales acheminées par les satellites de la première génération, des stations de réception sont indispensables dans la zone atlantique, dans la zone de l'océan Indien et dans la zone de l'océan Pacifique. Pour la génération plus récente de satellites, permettant une émission par sous-région, il faut encore respecter d'autres conditions quant à la position géographique des stations d'interception si l'objectif consiste à capter l'ensemble des communications transmises par satellite.

Un autre système d'interception fonctionnant à l'échelle mondiale doit installer ses stations ailleurs que dans les territoires relevant des pays ECHELON.

6.1.2. Conditions politico-économiques

La mise en place d'un tel système d'interception fonctionnant à l'échelle mondiale doit cependant également présenter un intérêt économique et politique pour le ou les exploitants. Le ou les bénéficiaires d'un tel système doivent avoir des intérêts économiques et militaires ou d'autres intérêts en termes de sécurité, ou à tout le moins croire qu'ils font partie des puissances mondiales. Dès lors, le cercle des pays concernés se limite, pour l'essentiel, à la Chine et aux pays du G8, sans les États-Unis et le Royaume-Uni.

6.2. France

Dans les trois zones précitées, la France possède des territoires, départements et collectivités locales qui lui sont propres.

Dans l'Atlantique, il y a, à l'est du Canada, Saint-Pierre-et-Miquelon (65° O / 47° N), au nord-est de l'Amérique du Sud, la Guadeloupe (61° O / 16° N) et la Martinique (60° O / 14° N) ainsi qu'au large de la côte nord-est de l'Amérique du Sud, la Guyane française (52° O / 5° N).

Dans la zone de l'océan Indien, il y a, à l'est de l'Afrique australe, Mayotte (45° E / 12° S) et La Réunion (55° E / 20° S), ainsi que tout au sud, les terres Australes et Antarctiques francaises. Dans la zone du Pacifique, on trouve la Nouvelle-Calédonie (165° E / 20° S), Wallis et Futuna (176° O / 12° S), ainsi que la Polynésie française (150° O / 16° S).

S'agissant de l'existence éventuelle de stations du service de renseignement français – la DGSE (Direction générale de la sécurité extérieure) – dans ces régions d'outre-mer, les renseignements sont peu nombreux. Selon certains journalistes français[85], il existe des stations à Kourou (Guyane française), ainsi qu'à Mayotte. Aucune donnée précise n'est disponible en ce qui concerne la grandeur de ces stations ainsi que le nombre ou les dimensions des antennes satellitaires. En France, d'autres stations existeraient à Domme (près de Bordeaux) et aux Alluetts-le-Roi (près de Paris). Jauvert estime à 30 au total le nombre des panneaux satellitaires. L'écrivain Schmidt-Enboom[86] affirme qu'une station serait également en service en Nouvelle-Calédonie.

En théorie, la France pourrait également exploiter un système d'interception fonctionnant à l'échelle mondiale. Votre rapporteur ne dispose toutefois pas de suffisamment d'informations de sources publiques pour pouvoir l'affirmer sérieusement.

6.3. Russie

Le FAPSI (Direction des transmissions présidentielles) – service de renseignement russe responsable pour la sécurité des communications et le SIGINT – exploiterait, conjointement avec le GROU (Service de renseignement de l'armée), des stations au sol en Lettonie, au Vietnam et à Cuba.

Dans la zone de l'Atlantique, il y a, selon les indications de la Federation of American Scientists, la station cubaine de Lourdes (82° O / 23° N), qui est exploitée en commun avec le service de renseignement cubain. Pour la zone de l'océan Indien, il y a des stations en Russie, à propos desquelles on ne dispose d'aucune information précise, ainsi qu'une station à Skrunda (Lettonie). Dans la zone du Pacifique, il y aurait une station dans la baie de Cam Ranh (République socialiste du Vietnam). On ne sait rien de précis sur ces stations ni sur le nombre et les dimensions des antennes.

Ces stations et celles qui existent en Russie même permettent en théorie une couverture mondiale. En l'occurrence, les informations disponibles sont également insuffisantes pour pouvoir affirmer sérieusement quelque chose.

[85] Jean Guisnel, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage, comment la France écoute le monde, Le nouvel Observateur, 5.4.2001, N° 1900, pp. 14 et ss.
[86] E.Schmidt-Eenboom, dans: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg, 1999, p.180.

6.4. Autres pays du G8 et Chine

Les autres pays du G8 et la Chine n'ont aucun territoire propre ou véritable allié dans les régions du monde nécessaires pour exploiter un système d'interception mondial.

7. Compatibilité d'un système d'interception des communications du type "ECHELON" avec le droit de l'Union européenne

7.1. Commentaires sur la question

Selon son mandat, la commission est notamment expressément chargée de vérifier la compatibilité d'un système d'interception des communications du type ECHELON avec le droit communautaire[87]. Elle doit en particulier s'assurer qu'un tel système est compatible avec les deux directives relatives à la protection des données (95/46/CE et 97/66/CE, ainsi qu'avec l'article 286 du traité CE et l'article 8, paragraphe 2, du traité sur l'Union européenne.

Il semble nécessaire d'envisager cette question sous deux angles différents. Une première approche procède de la preuve par indices du chapitre 5, dont il ressort que le système baptisé ECHELON a été conçu comme un système d'interception des communications, qui par la collecte et l'exploitation des données communiquées, doit fournir aux services secrets américain, canadien, australien, néo-zélandais et britannique des informations sur des faits à l'étranger. En l'occurrence, il s'agit donc d'un instrument d'espionnage classique des services de renseignement extérieur[88]. Aussi faut-il, dans un premier temps, examiner la question de la compatibilité d'un tel système de renseignement avec le droit de l'Union.

Par ailleurs, dans le rapport qu'il a présenté au STOA, Campbell formule une accusation, à savoir que ce système serait utilisé aux fins de l'espionnage industriel, ce qui serait à l'origine de préjudices graves pour l'économie des pays européens. De plus, selon certaines déclarations faites par l'ancien directeur de la CIA, R. James Woosley, les États-Unis espionneraient des entreprises européennes, et ce uniquement toutefois pour rétablir un marché équitable, dès lors qu'autrement les contrats ne sont obtenus que grâce à la corruption[89]. S'il est exact que les systèmes sont utilisés aux fins de l'espionnage industriel, alors la question de la compatibilité avec le droit communautaire se pose de nouveau. Ce deuxième aspect doit donc être étudié séparément.

7.2.Compatibilité d'un système de renseignement avec le droit de l'Union européenne

7.2.1. Compatibilité avec le droit communautaire

En principe, les activités et mesures concernant la sûreté de l'État ou les poursuites pénales ne relèvent pas du champ d'application du traité CE. Dans la mesure où conformément au principe de la compétence restreinte, la Communauté européenne ne peut agir que là où elle est formellement habilitée à le faire, elle a exclu ces différents domaines du champ d'application des directives relatives à la protection des données, fondées sur le traité CE et, en particulier, son article 95 (ex-article 100A). La directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[87] Cf. à ce propos chapitre 1, point 1.3.
[88] Cf. à ce propos chapitre 2.
[89] Cf. à ce propos chapitre 5, points 5.6 et 5.8.

et à la libre circulation de ces données[90] et la directive 97/66/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[91] ne s'appliquent pas "en tout état de cause aux traitements[92]/activités [93] concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsque ces traitements sont des questions de sûreté de l'État/lorsqu'il s'agit d'activités liées à la sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal/ou aux activités de l'État dans les domaines relevant du droit pénal". La proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dont le Parlement est actuellement saisi, fait également sien ce libellé. Aussi, la participation d'un État membre à un système d'interception aux fins de la sûreté de l'État n'est-elle pas incompatible avec les directives relatives à la protection des données.

Il ne saurait pas davantage être question d'une violation de l'article 286 du traité CE, qui étend le champ d'application des directives relatives à la protection des données au traitement des données par les organes et institutions communautaires. Il en va de même pour le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[94]. Ce règlement ne s'applique également que là où ces organes et institutions agissent dans le cadre du traité CE[95]. Pour éviter tout malentendu, il convient de souligner expressément ici qu'une participation des organes et institutions communautaires à un système d'interception n'a jamais été évoquée, et que votre rapporteur ne dispose d'aucun élément lui permettant de croire à une telle participation.

7.2.2. Compatibilité avec d'autres dispositions législatives de l'Union européenne

Pour les domaines ressortissant aux titres V (politique étrangère et de sécurité commune) et VI (coopération policière et judiciaire en matière pénale), il n'existe aucune disposition concernant la protection des données qui soit comparable avec les directives communautaires. Le Parlement européen a souligné à plusieurs reprises déjà qu'il était impérieux d'agir dans ce domaine[96].

Dans ces domaines, la protection des droits et libertés fondamentaux des personnes est garantie par les articles 6 et 7, et en particulier par l'article 6, paragraphe 2, du traité sur l'Union européenne, par lequel l'Union s'engage à respecter "les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés

[90] JO L 281 du 23.11.1995, p. 31.
[91] JO L 24 du 30.1.1998, p. 1.
[92] Directive 95/46/CE, art. 3, par. 2.
[93] Directive 97/66/CE, art. premier, par. 3.
[94] Règlement (CE) n° 45/2001, JO L 8 du 12.1.2001, p. 1.
[95] Art. 3, par. 1; cf. également le considérant 15: "lorsque ce traitement est effectué par les institutions et organes communautaires pour l'exercice d'activités situées hors du champ d'appplication du présent règlement, en particulier celles prévues aux titres 5 et 6 du traité sur l'Union européenne, la protection des libertés et droits fondamentaux des personnes est assurée dans le respect de l'article 6 du traité sur l'Union européenne. (…)".
[96] Cf. par exemple le paragraphe 25 de la résolution sur le projet de plan d'action du Conseil et de la Commission concernant les modalités optimales de mise en œuvre des dispositions du traité d'Amsterdam relatives à l'établissement d'un espace de liberté, de sécurité et de justice (13844/98 – C4-0692/98 – 98/0923(CNS)), JO C 219 du 30.7.1999, pp. 61 et ss.

fondamentales (…) et tels qu'ils résultent des traditions constitutionnelles communes aux États membres". Ainsi, si les États membres sont tenus de respecter les droits fondamentaux et en particulier la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (cf. à ce propos infra chapitre 8), l'Union est elle aussi tenue de respecter les droits fondamentaux dans l'exercice de ses compétences législatives et administratives. Dès lors qu'il n'existe toutefois pas jusqu'ici, dans l'Union européenne, une réglementation concernant la légalité de la surveillance des télécommunications aux fins de la protection de la sûreté de l'État et du renseignement[97], la question de la violation de l'article 6, paragraphe 2, du traité sur l'Union européenne ne se pose pas directement.

7.3. Problème de la compatibilité en cas d'utilisation du système aux fins de l'espionnage économique

Si un État membre prêtait assistance à un système d'interception, destiné entre autres à également espionner les entreprises, en permettant d'utiliser à cet effet ses propres services de renseignement ou en mettant son territoire à la disposition de services de renseignement étrangers, alors, il pourrait très bien y avoir violation du droit communautaire. En effet, aux termes de l'article 10 du traité CE, les États membres ont un devoir de loyauté générale et doivent en particulier s'abstenir "de toutes mesures susceptibles de mettre en péril la réalisation des buts du (…) traité." Même dans le cas où l'interception de télécommunications ne se ferait pas au profit de l'économie nationale (ce qui au demeurant aurait un effet comparable à celui d'une aide d'État et serait dès lors incompatible avec l'article 87 du traité CE), mais bien au profit de pays tiers, une telle activité serait fondamentalement contraire au principe du marché commun à la base du traité CE, dans la mesure où elle équivaudrait à une distorsion de concurrence.

De l'avis de votre rapporteur, une telle attitude représenterait en outre une violation de la directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[98] dès lors que la question de l'applicabilité des directives doit être résolue sur la base de considérations fonctionnelles et non organisationnelles. Et ce non seulement en raison du libellé des dispositions relatives au champ d'application mais aussi de l'esprit de la loi. Si des services de renseignement utilisent leurs capacités aux fins de l'espionnage économique, leur activité n'est pas en rapport avec la sûreté de l'État ou des poursuites pénales, mais elle vise d'autres objectifs et entre dès lors pleinement dans le champ d'application de la directive. Aux termes de l'article 5 de celle-ci, les États membres sont tenus de garantir la confidentialité des communications, et en particulier d'interdire "à toute autre personne que les utilisateurs (…) d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance (…)". Aux termes de l'article 14, des exceptions ne sont possibles que dans le cas où elles sont nécessaires "pour sauvegarder la sûreté de l'État, la défense (…) et la poursuite d'infractions pénales (…)".

---

[97] En matière de surveillance des télécommunications, il n'existe actuellement dans l'Union européenne que deux actes, aucun d'eux n'ayant trait à la question de la légalité:
– la résolution du Conseil, du 17 janvier 1995, relative à l'interception légale des télécommunications (JO C 329 du 4.11.1996), dont l'annexe constitue un condensé des besoins des autorités compétentes pour la réalisation technique des mesures d'interception légale dans les systèmes modernes de télécommunications, et
– l'acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (JO C 197 du 12.7.2000, p. 1, art. 17 et ss.), qui arrête les conditions dans lesquelles l'entraide judiciaire en matière pénale doit être possible pour ce qui est de l'interception des télécommunications. Il n'en résulte aucune atteinte pour les droits de ceux dont les communications sont interceptées, l'État où ceux-ci se trouvent ayant alors toujours la possibilité de refuser l'entraide judiciaire, lorsque le droit national s'y oppose.

[98] Directive 97/66/CE, JO L 24 du 30.1.1998, p. 1.

L'espionnage économique n'étant pas un motif légitime d'exception, il y aurait alors violation du droit communautaire.

7.4. Conclusions

En résumé, il est possible de dire que dans la situation juridique actuelle, un système de renseignement du type ECHELON ne saurait être contraire au droit de l'Union, dès lors qu'il ne présente aucun rapport avec des éléments du droit de l'Union justifiant son incompatibilité. Il en va toutefois uniquement ainsi tant que le système est utilisé exclusivement aux fins de garantir la sûreté de l'État. S'il est par contre détourné de ses objectifs pour espionner des entreprises étrangères, il y a bien infraction au droit communautaire. Et si un État membre participait à une activité de ce type, il violerait le droit communautaire.

8. La surveillance des communications par les services de renseignements est-elle compatible avec le droit fondamental au respect de la vie privée

8.1. La surveillance des communications, atteinte au droit fondamental au respect de la vie privée

Toute écoute de communication, à commencer par l'interception de données par des services de renseignements à cette fin[99], représente une atteinte profonde à la vie privée de la personne. L'écoute illimitée par la puissance publique n'est admissible que dans un "État policier". Dans les États membres de l'UE, qui sont des démocraties évoluées, la nécessité pour les organes de l'État, c'est–à–dire aussi pour les services de renseignements, de respecter la vie privée est incontestée et généralement inscrite dans les différentes constitutions nationales. La vie privée bénéficie donc d'une protection particulière et des possibilités d'intervention ne sont accordées qu'après évaluation des biens protégés par des dispositions légales et dans le respect du principe de proportionnalité.

Dans les pays qui font partie d'ECHELON aussi, on est conscient du problème. Les dispositions de protection prévues visent toutefois le respect de la vie privée des ressortissants nationaux, de sorte que le citoyen européen est généralement exclu du bénéfice de celles–ci. Aux États–Unis, dans les dispositions qui définissent les conditions de la surveillance électronique, aux intérêts de l'État en ce qui concerne le bon fonctionnement des services de renseignements ne fait pas pendant le souci d'une protection générale efficace des droits fondamentaux, mais la nécessaire protection de la vie privée des "citoyens américains".[100]

8.2. La protection de la vie privée garantie par les conventions internationales

Le respect de la vie privée en tant que droit fondamental est inscrit dans de nombreuses conventions de droit international public[101]. Au plan mondial, la convention internationale relative aux droits civils et politiques[102], conclue en 1966 dans le cadre de l'ONU, garantit en son article 17 la protection de la vie privée. Tous les pays qui font partie d'ECHELON ont souscrit aux décisions de la commission des droits de l'homme instituée conformément à l'article 41 et qui examine les violations de la convention, et ce dès lors qu'il y a plainte d'autres pays. Le

---

99 Tribunal constitutionnel fédéral, 1 BvR 2226/94 du 14.7.1999, n° 187 "Eingriff ist [...] schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet."

100 Cf. rapport au Congrès des États–Unis de fin février 2000 "Legal Standards for the Intelligence Community in conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, der auf den Foreign Intelligence Surveillance Act (FISA), abgedruckt in Titel 50 Kapitel 36 U.S.C. § 1801 ff und dieExec. Order No. 12333, 3 C.F.R. 200 (1982), abgedruckt in Titel 50, Kapitel 15 U.S.C. § 401 ff verweist, http://www4.law.cornell.edu/uscode/50/index.html.

101 Art. 12 Déclaration universelle des droits de l'homme; Art 17, Convention des Nations unies relative aux droits civils et politiques; Art. 7, Charte de l'UE, Art. 8, convention européenne des droits de l'homme, recommandation du Conseil de l'OCDE über Leitlinien für die Sicherheit von Informationssystemen, angenommen am 26./27.11.1993 C(92) 188/Final; Art 7 Europaratskonvention über den Schutz von Personen betreffend die automatische Verarbeitung personenbezogener Daten; vgl dazu die von STOA in Auftrag gegebene Studie Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), october 1999, 2.

102 International Covenant on Civil and Political Rights, adoptée par l'AG des Nations unies le 16. 12. 1966.

protocole additionnel[103], qui étend la compétence de la commission aux recours individuels, n'a cependant pas été signé par les États–Unis, de sorte qu'il est impossible à une personne privée de s'adresser à la commission des droits de l'homme en cas de violation de la convention par les États-Unis.

Au niveau de l'UE, on s'est efforcé de mettre en place une protection européenne particulière des droits fondamentaux en élaborant une charte des droits fondamentaux de l'UE. L'article 7 de celle-ci, qui concerne le respect de la vie privée et familiale, régit même expressément le droit au respect des communications[104]. De plus, l'article 8 régit le droit fondamental à la protection des données à caractère personnel. Cette disposition protégerait la personne au cas où des données la concernant seraient traitées (par la voie informatique ou non), ce qui est généralement le cas en cas d'écoute et l'est toujours en cas d'interception par d'autres moyens.

A ce jour, la Charte n'a pas été incorporée au traité. Elle n'est contraignante que pour les trois institutions qui y ont souscrit dans la déclaration solennelle en marge du Conseil européen de Nice: Conseil, Commission et Parlement européen. À la connaissance du rapporteur, celles-ci ne sont pas engagées dans des activités de services secrets. Même si l'incorporation au traité donnait à la Charte tous ses effets, il faut tenir compte de son champ d'application limité. Aux termes de l'article 51, ces dispositions "s'adressent aux institutions et organes de l'Union ... ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union". La Charte s'appliquerait donc en plus de l'instrument représenté par l'interdiction d'aides publiques contraires à la concurrence (voir chapitre 7, point 7.3).

Le seul instrument efficace au plan international en matière de protection globale de la vie privée est constitué par la convention européenne relative aux droits de l'homme.

8.3. Les dispositions de la convention européenne des droits de l'homme

8.3.1. L'importance de la convention dans l'UE

La protection des droits fondamentaux assurée par la convention revêt une importance particulière dans la mesure où la convention a été ratifiée par tous les États membres de l'UE, de sorte qu'elle assure un niveau de protection uniforme en Europe. Les États partie à cette convention se sont engagés en droit international à garantir les droits reconnus par la convention et à se soumettre à la juridiction de la Cour européenne des droits de l'homme de Strasbourg. Celle-ci peut vérifier la conformité des réglementations nationales par rapport à la convention. En cas de violation des droits de l'homme, elle peut condamner les États signataires et les contraindre à payer des dédommagements. L'importance de la convention se trouve encore accrue du fait que la Cour de justice des Communautés européennes l'a consultée à plusieurs reprises dans le contexte de vérifications de dispositions législatives par rapport aux principes généraux du droit des États membres. Le traité d'Amsterdam (article 6, paragraphe 2, du traité UE) prévoit en outre l'obligation pour l'UE de respecter les droits fondamentaux tels qu'ils sont garantis par la convention.

---

[103] Opitional Protocol to the International Covenant on civil and Political Rights, adopté par l'AG des Nations unies le 16.12.1966.

[104] "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications".

8.3.2. Portée de la protection offerte par la convention

Les droits inscrits dans la convention sont des droits de l'homme universels qui ne sont donc pas liés à la nationalité. Ils doivent être reconnus à toutes les personnes soumises à la juridiction des États signataires. Cela signifie que les droits de l'homme doivent dans tous les cas êtres accordés sur l'ensemble du territoire national, des exceptions locales constituant une violation de la convention. De plus, ces droits s'appliquent aussi hors du territoire national des États signataires dès lors que la puissance publique s'y exerce. Les droits garantis par la convention vis–à–vis d'un État signataire sont donc reconnus aux personnes hors du territoire national dès lors qu'un État signataire porte atteinte à la vie privée hors du territoire national[105].

Ce dernier aspect est particulièrement important dans le contexte qui nous intéresse car le problème des droits fondamentaux dans le domaine de la surveillance des télécommunications présente la particularité que l'État qui est responsable de la surveillance, la personne surveillée et le processus d'interception lui–même ne sont pas présents en un même lieu. Cela s'applique notamment aux communications internationales mais aussi dans certains cas aux communications nationales lorsque le transport de l'information s'effectue via l'étranger. C'est même la règle en ce qui concerne l'action des services de renseignements à l'étranger. Par ailleurs, il ne peut être exclu que les informations obtenues grâce à la surveillance par un service de renseignements soient transmises à d'autres pays.

8.3.3. Surveillance des télécommunications au regard de l'article 8 de la convention

L'article 8, paragraphe 1, de la convention dispose que "toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance". Il n'est pas fait mention expressément de la protection des communications téléphoniques et des télécommunications, mais en vertu de la jurisprudence de la Cour des droits de l'homme, ces aspects sont également couverts par les notions de vie privée et de correspondance et bénéficient à ce titre de la protection de l'article 8 de la convention[106]. La protection des droits fondamentaux s'étend non seulement au contenu des communications, mais aussi à l'enregistrement de données extérieures. Cela signifie que même si un service de renseignements n'enregistre que des données telles que heure et durée des communications ou encore numéros composés, il s'agit là d'une atteinte à la vie privée[107].

Le droit qui est reconnu à l'article 8, paragraphe 2, de la convention n'est pas illimité. Des atteintes au droit fondamental au respect de la vie privée sont admissibles dès lors qu'elles disposent d'une base juridique dans le droit national[108]. Le droit doit être accessible à tous et

---

105 Voir EGMR Loizidou/Türkei, 23.3.1995, n° 62 avec d'autres éléments à l'appui "...the concept of 'jursidiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" mit Verweis auf EGMR, Drozd und Janousek, 26.6.1992, n° 91. Voir Jacobs, The European Convention on Human Rights (1996), 21 ff.

106 Voir Cour des droits de l'homme, Klass ua, 6.9.1978, n° 41.

107 Voir Cour des droits de l'homme, Malone, 2.8.1984, n° 83 et suivants; Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 656.

108 Selon la jurisprudence de la Cour des droits de l'homme (voir notamment Sunday Times, 26.4.1979, p. 46 ss, Silver ua, 25.3.1983, p.85 ss) la notion de "loi" visée à l'art. 8, par. 2 englobe non seulement les lois au sens formel, mais aussi les dispositions de catégories inférieures, c'est–à–dire aussi le droit non écrit. Cela suppose toutefois que le justiciable ait la possibilité de déterminer dans quelles circonstances une ingérence est possible. Voir Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ff, 495.

prévisible dans ses effets[109].

Les États membres ne disposent donc pas d'une liberté totale pour organiser ces ingérences. L'article 8 de la convention n'autorise celles-ci que pour réaliser les objectifs énumérés au paragraphe 2, à savoir notamment sécurité nationale, sûreté publique, prévention d'infractions pénales ainsi que bien–être économique du pays[110], ce qui ne justifie toutefois pas l'espionnage économique car seules les interventions nécessaires dans une société démocratique sont couvertes. Pour toute intervention, il faut recourir au moyen minimal permettant d'atteindre l'objectif et, en outre, prévoir des garanties suffisantes contre les abus.

8.3.4. Importance de l'article 8 de la convention sous l'angle des activités des services de renseignements

Du point de vue de l'organisation conforme aux droits fondamentaux des activités des services de renseignements, ces principes généraux signifient que s'il apparaît nécessaire, pour assurer la sécurité nationale, d'autoriser les services de renseignements à intercepter le contenu de télécommunications ou au moins des données relatives aux communications, cela doit être prévu par le droit national et les dispositions afférentes doivent être accessibles à tous. Les conséquences de ces dispositions doivent être prévisibles pour chacun, non toutefois sans tenir compte des exigences du secret. C'est ainsi que dans un arrêt relatif à la conformité avec l'article 8 de contrôles secrets visant des fonctionnaires dans des domaines touchant à la sécurité nationale, la Cour des droits de l'homme a constaté que l'aspect de prévisibilité dans ce cas particulier ne peut être identique à ce qu'il est dans d'autres domaines[111]. Elle a demandé dans ce cas aussi que les dispositions juridiques précisent dans quelles circonstances et conditions la puissance publique peut porter une atteinte secrète et, partant, potentiellement dangereuse, à la vie privée[112].

Une organisation conforme aux droits de l'homme des activités des services de renseignements suppose que l'on tienne compte de l'aspect suivant: si la sécurité nationale constitue une justification, celle–ci est toutefois soumise au principe de proportionnalité, conformément à l'article 8, paragraphe 2 de la convention. Même la sécurité nationale ne peut justifier des ingérences que dans le cas où celles–ci apparaissent nécessaires au sein d'une société démocratique. À cet égard, la Cour des droits de l'homme a indiqué que le souci de l'État de protéger la sécurité nationale doit être mis en balance avec les intérêts de la personne en ce qui concerne le respect de la vie privée[113]. Les ingérences ne sont certes pas limitées à ce qui est indispensable mais il ne suffit pas qu'elles soient opportunes ou souhaitables[114]. L'idée selon laquelle l'interception de toute télécommunication constituerait la meilleure protection contre la criminalité organisée serait contraire à l'article 8 de la convention même si cela était prévu par le droit national.

---

109 Silver ua, 25.3.1983, Z 87 f.

110 L'argument du bien–être économique a été admis par la Cour dans un cas où il s'agissait de la communication de données médicales importantes du point de vue de l'octroi de prestations publiques: M.S./Schweden, 27.8.1997, p.38; ainsi que dans un cas concernant l'expulsion des Pays–Bas d'une personne qui était dépendante de la sécurité sociale après que la justification de son permis de séjour fut devenu caduc. . Ciliz/Niederlande, 11.7.2000, p 65.

111 Cour européenne des droits de l'homme, Leander, 26.3.1987, p. 51.

112 Cour européenne des droits de l'homme, Malone, 2.8.1984, p. 67.

113 Cour européenne des droits de l'homme, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, p. 46 ss.

114 Cour européenne des droits de l'homme, Silver ua, 24.10.1983, Z 97.

Il faut en outre prévoir des possibilités de contrôle plus importantes eu égard au caractère particulier des activités des services de renseignements qui supposent le secret et, par voie de conséquence, une certaine mise en balance des intérêts. La Cour a souligné qu'un système de surveillance secret destiné à garantir la sécurité nationale porte en soi le risque de saper ou de détruire la démocratie sous prétexte de la défendre et qu'il faut par conséquent des garanties appropriées et efficaces contre de tels abus[115]. Les activités légitimes des services de renseignements ne sont conformes aux droits fondamentaux que si l'État signataire de la convention a prévu des systèmes de contrôle suffisants et d'autres garanties contre les abus. À cet égard, la Cour a fait observer, dans le contexte des activités des services de renseignements suédois, qu'elle accordait une importance particulière à la présence de députés au sein de l'organe de contrôle policier ainsi qu'à la surveillance exercée par le ministre de la justice, par le médiateur parlementaire et par la commission juridique du Parlement. Dans ces conditions, il apparaît critiquable que la France, la Grèce, l'Irlande, le Luxembourg et l'Espagne ne disposent pas de commissions parlementaires chargées de contrôler les services secrets[116], pas plus que de système de contrôle comparable au médiateur parlementaire des pays nordiques[117]. Le rapporteur se félicite par conséquent des efforts déployés par la commission de la défense de l'Assemblée nationale française pour instituer une commission de contrôle[118], d'autant que la France dispose de capacités de renseignements notables, tant du point de vue technique que du point de vue géographique.

8.4. Obligation de vigilance vis–à–vis des activités de services de renseignements étrangers

8.4.1. Caractère inadmissible d'une violation de l'article 8 de la convention liée à l'intervention de services de renseignements étrangers

Comme il a été exposé plus haut, les parties signataires doivent satisfaire à plusieurs conditions pour que les activités de leurs services de renseignements soient compatibles avec l'article 8 de la convention. Il est évident que les services de renseignements ne peuvent se soustraire à ces obligations en recourant aux services d'autres organismes de renseignements soumis à des dispositions moins rigoureuses. S'il en était autrement, le principe de légalité et ses deux composantes – possibilité d'accès et prévisibilité – se trouverait privé de ses effets cependant que la jurisprudence de le Cour serait vidée de sa substance.

Cela signifie d'une part que l'échange de données entre services de renseignements n'est admissible que dans une mesure limitée. Un service de renseignements ne peut solliciter d'un autre des données que si lesdites données peuvent être obtenues dans des conditions prévues par le droit national. Le rayon d'action défini par la loi ne peut être étendu à travers des accords avec d'autres services. De la même manière , un service de renseignements ne peut intervenir sur instructions d'un service de renseignements étranger qu'à condition d'avoir établi que lesdites activités sont conformes au droit national. Même si les informations sont destinées à un pays étranger, cela ne change rien au fait qu'une ingérence que le justiciable ne pouvait prévoir est contraire à ses droits fondamentaux.

---

115 Cour européenne des droits de l'homme, Leander, 26.3.1987, p. 60.

116 Le rapporteur sait que ni le Luxembourg ni l'Irlande ne disposent ni de services de renseignements à l'étranger ni de SIG-INT. La nécessité d'une instance de contrôle particulière ne concerne que les activités de renseignements à l'intérieur du pays.

117 Au sujet du contrôle des services de renseignements dans les États membres, voir chapitre 9.

118 Voir "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", et rapport afférent du député Arthur Paecht, N° 1951 Assemblée nationale, 11. législature, 23. november 1999.

Par ailleurs, les pays signataires de la convention ne peuvent autoriser des services de renseignements étrangers à intervenir sur leur territoire dès lors que l'on peut soupçonner que leurs activités ne sont pas conformes aux dispositions de la convention[119].

8.4.2. Conséquences sous l'angle des activités de services de renseignements extra–européens sur le territoire de pays signataires de la convention

8.4.2.1. Jurisprudence de la Cour européenne des droits de l'homme

En ratifiant la convention, les signataires se sont engagés à soumettre l'exercice de leur souveraineté à une vérification du respect des droits fondamentaux. Ils ne peuvent se soustraire à cette obligation en renonçant à leur souveraineté. Ils conservent la responsabilité de leur territoire ainsi que leurs obligations vis–à–vis du justiciable européen dès lors que l'exercice de la puissance publique est assuré par le service de renseignements d'un autre pays. La jurisprudence de la Cour confirme de manière constante que les pays signataires sont tenus de prendre des mesures positives pour protéger la vie privée afin que les personnes privées (!) ne violent pas l'article 8 de la convention, et ce y compris au plan horizontal où la personne ne se trouve pas face à la puissance publique mais à une autre personne[120]. Si un pays autorise un service de renseignements étranger à intervenir sur son territoire, la protection nécessaire est d'autant plus grande que c'est dans ce cas une autre autorité qui exerce sa puissance. Il semble tout simplement logique de considérer que l'État doit veiller à la conformité des activités de services de renseignements avec les droits de l'homme sur son territoire.

8.4.2.2. Conséquences en ce qui concerne les stations

En Allemagne, les États–Unis d'Amérique disposent à Bad Aibling d'un territoire propre qu'ils utilisent exclusivement pour la réception d'émissions de satellites. À Menwith Hill, au Royaume-Uni, ils partagent un terrain dans le même but. Si un service de renseignements américain interceptait dans ces stations des communications non militaires de personnes privées ou d'entreprises en provenance d'un pays signataire de la convention, cela donnerait lieu à des obligations de contrôle. Dans la pratique, cela signifie que l'Allemagne et le Royaume–Uni, signataires de la convention, sont tenus de s'assurer que les activités des services de renseignements américains sont conformes aux droits fondamentaux. Cela s'impose d'autant plus que des représentants des ONG et de la presse ont déjà fait part à plusieurs reprises de leur inquiétude face aux agissements de la NSA.

8.4.2.3. Conséquences en ce qui concerne les écoutes pratiquées sur instructions de l'étranger

À Morwenstow, au Royaume–Uni, le GCHQ pratique en coopération avec la NSA, sur instructions de cette dernière, l'interception de communications civiles qui sont transmises telles quelles aux États–Unis. Même si les activités sont effectuées pour compte de tiers, il y a obligation de vérifier qu'elles sont conformes aux droits fondamentaux.

---

[119] Voir Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit européen 2000, 187 ss.

[120] Cour européenne des droits de l'homme, Abdulaziz, Cabales et Balkandali, 28.5.1985, p. 67; X u Y/Niederlande, 26.3.1985, p. 23; Gaskin vs Vereinigtes Königreich 7.7.1989, Z 38; Powell et Rayner, 21.2.1990, p. 41.

8.4.2.4. Obligation de vigilance par rapport aux pays tiers

S'agissant de pays signataires de la convention, on peut dans une certaine mesure considérer de part et d'autre que l'autre pays respecte aussi la convention. Cela n'est toutefois valable que jusqu'à ce qu'il soit établi qu'un pays signataire de la convention viole celle–ci de manière systématique et répétée. Les États–Unis ne sont pas signataires de la convention et ils ne se soumettent pas à un dispositif de contrôle comparable. Les activités de leurs services de renseignements sont très précisément réglementées, du moins par rapport aux citoyens des États–Unis, c'est–à–dire à des personnes qui se trouvent en séjour légal aux États–Unis. Les activités de la NSA à l'étranger font l'objet d'autres dispositions dont un grand nombre sont apparemment secrètes et donc inaccessibles. Préoccupant est en outre le fait que les services de renseignements américains sont soumis au contrôle des commissions de la Chambre des députés et du sénat, mais que les commissions parlementaires ne s'intéressent que très peu aux activités de la NSA à l'étranger.

Il apparaît donc opportun de lancer un appel à l'Allemagne et au Royaume–Uni pour qu'ils tiennent dûment compte des obligations qui découlent de la convention et qu'ils subordonnent l'autorisation d'activités de services de renseignements de la NSA sur leur territoire au respect de la convention dans ce contexte. À cet égard, trois aspects importants sont à prendre ne considération:

1) La convention prévoit que les atteintes à la vie privée ne sont possibles que sur la base de dispositions accessibles à tous et dont les conséquences sont prévisibles pour chacun. Il n'est satisfait à cette condition que si les États–Unis informent la population européenne sur les modalités de l'information. Aussi longtemps que la convention ne sera pas respectée, il faudra adapter les dispositions aux garanties offertes en Europe.

2) La convention prévoit que les interventions ne peuvent être disproportionnées et qu'il faut recourir aux moyens minimaux. Pour le citoyen européen, une intervention européenne est à considérer comme moins grave qu'une intervention américaine car dans le premier cas seulement il peut se tourner vers les voies de recours nationales[121]. Les interventions doivent donc dans la mesure du possible être effectuées par les Allemands ou par les Anglais, ce qui s'assortit logiquement dans les deux cas d'une possibilité de recours. Les Américains ont tenté à plusieurs reprises de justifier les écoutes en accusant les Européens de corruption[122]. Il a été rappelé aux Américains que tous les pays de l'UE disposent de systèmes pénaux en état de fonctionnement. En cas de suspicion, les États–Unis doivent s'en remettre au système pénal du pays d'accueil. S'il n'y a pas de suspicion, la surveillance est à considérer comme disproportionnée et donc contraire aux droits de l'homme, ce qui la rend inadmissible. La compatibilité avec la convention n'existe que si les États–Unis se limitent à des mesures de surveillance utiles à leur sécurité nationale, c'est–à–dire dépourvues de finalité pénale.

3) Comme il a déjà été indiqué, la jurisprudence de la Cour exige, pour qu'il y ait conformité aux droits fondamentaux, que des systèmes de contrôle et des garanties suffisantes contre les abus soient prévus. Cela signifie que la surveillance américaine des télécommunications sur le territoire européen n'est conforme aux droits de l'homme que si les États–Unis prévoient des contrôles efficaces dans les cas où ils interceptent des communications pour assurer leur sécurité nationale ou que les activités menées par la NSA sur le territoire européen soient soumises au

---

121 Cela assure aussi la conformité à l'article 13 de la convention des droits de l'homme qui reconnaît à la personne lésée le droit de s'adresser aux instances nationales.

122 Woolsey (ancien directeur de la CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31.

contrôle du pays d'accueil (c'est-à-dire de l'Allemagne ou du Royaume-Uni).

C'est seulement à condition que ces trois exigences soient respectées qu'il sera possible de garantir que les écoutes de télécommunications pratiquées par les États-Unis sont conformes à la convention et que le niveau de protection garanti de manière uniforme en Europe par celle-ci est sauvegardé.

9. Les citoyens de l'UE sont–ils suffisamment protégés face aux activités des services de renseignements?

9.1. Protection face aux activités des services de renseignements: rôle des parlements nationaux

Étant donné que les activités des services de renseignements pourraient à l'avenir constituer un aspect de la PESC, mais qu'il n'y a pour l'heure aucune disposition communautaire en la matière[123], l'organisation de la protection face aux activités des services de renseignements ne relève que des systèmes juridiques nationaux.

Dans ce contexte, les parlements nationaux jouent un double rôle: en tant que législateur, ils déterminent les effectifs et les pouvoirs des services de renseignements ainsi que l'organisation du contrôle de leurs activités. Comme il a été exposé au chapitre précédent, les parlements, lorsqu'ils abordent le problème de l'admissibilité de la surveillance des télécommunications, doivent s'en tenir aux limites fixées par l'article 8 de la convention: les dispositions doivent être nécessaires et proportionnelles et leurs conséquences doivent être prévisibles pour chacun. De plus, les pouvoirs des autorités de surveillance doivent être soumis à des mécanismes de contrôle appropriés et efficaces.

Par ailleurs, les parlements nationaux jouent dans la plupart des pays un rôle actif de contrôle. Le contrôle de l'exécutif (et donc des services de renseignements) est la deuxième fonction classique du parlement, à côté de la législation. Cela s'organise de diverses manières dans les États membres de l'UE, généralement des organes parlementaires coexistent avec des organes non parlementaires.

9.2. Pouvoirs des autorités nationales en matière de mesures de surveillance

La puissance publique peut prendre des mesures de surveillance dans un contexte pénal, pour préserver l'ordre ou pour assurer la sécurité de l'État (vis-à-vis de l'étranger)[124].

Dans le contexte pénal, le secret des communications peut être brisé dans tous les États membres dès lors qu'un soupçon fondé pèse sur l'auteur présumé d'une infraction pénale (lequel doit être dûment qualifié). Eu égard à la gravité de l'intervention, l'autorisation d'un magistrat est généralement requise[125]. La durée de la surveillance fait l'objet d'indications précises de même que le contrôle de celle–ci et la radiation des données.

Pour préserver la sécurité intérieure et l'ordre public, les possibilités d'interception sont étendues au-delà des recherches individuelles en cas de soupçon précis. Afin de dépister précocement les mouvements extrémistes ou subversifs, le terrorisme ou la criminalité organisée, le législateur autorise la collecte d'informations concernant certaines personnes ou groupements. La collecte desdites informations et leur analyse sont effectuées par des services de renseignements intérieurs.

---

123 Voir chapitre 7.

124 Ces objectifs sont reconnus comme justification d'atteinte à la vie privée par l'article 8, paragraphe 2, de la convention des droits de l'homme. Voir 8.3.2. ci–dessus.

125 À la différence du droit britannique qui confie la décision d'autorisation au Secretary of State (Regulation of Investigatory Powers Act 2000, Section 5 (1) und (3) (b).

Enfin, la sécurité de l'État représente un aspect important des activités de surveillance. Le traitement, l'analyse et la présentation des informations via l'étranger incombent généralement à un service de renseignements à l'étranger[126]. Généralement, ce ne sont pas des individus précis qui sont les cibles de la surveillance mais plutôt des régions ou fréquences. En fonction des moyens dont dispose le service de renseignements, ainsi que de ses pouvoirs, l'éventail est vaste, qui va du renseignement radio à caractère militaire (ondes courtes) à la surveillance de tous les types de communications avec l'étranger. Dans nombre d'États membres, la surveillance des télécommunications à des fins de renseignements est interdite[127]. Dans d'autres, elle peut, dans certains cas, sous réserve de l'approbation d'une commission indépendante[128], être autorisée par un ministre[129] et ce sans restriction aucune pour de nombreux moyens de communication[130]. Les pouvoirs relativement importants de nombreux services de renseignements à l'étranger s'expliquent par le fait qu'ils assurent la surveillance des communications avec l'étranger, qui ne concernent qu'un faible pourcentage des justiciables, de sorte que ces activités suscitent peu d'intérêt.

9.3. Les contrôle des services de renseignements

Un contrôle efficace et global est d'autant plus important que, d'une part, les services de renseignements travaillent dans le secret, que leurs activités concernent le long terme, que les personnes concernées ignorent pendant longtemps ou (en fonction de la situation juridique) ne savent absolument rien de la surveillance effectuée et que, d'autre part, les activités de surveillance concernent dans bien des cas des groupes assez importants aux contours mal définis, de sorte que l'État peut obtenir à très bref délai un volume important de données à caractère personnel.

Tous les organes de contrôle – quelle que soit leur structure – sont évidemment confrontés au problème que, en raison du caractère particulier des services secrets, il est généralement très difficile de déterminer si toutes les informations ont été fournies ou si une partie de celles-ci ont été retenues. La réglementation doit donc se faire avec beaucoup de soin. En principe, on peut considérer que l'efficacité des contrôles et, partant, la garantie de la légalité des interventions, sont assurées dès lors que la possibilité d'ordonner une surveillance est l'apanage du niveau administratif le plus élevé, que sa réalisation nécessite l'autorisation préalable d'un magistrat et qu'un organe indépendant contrôle la réalisation des opérations. De plus, il est souhaitable, pour des raisons touchant à la démocratie et à l'état de droit, que les activités des services de renseignements dans leur ensemble soient conformes au principe de séparation des pouvoirs de contrôle d'un organe parlementaire.

Tel est le cas, dans une large mesure, en Allemagne. Dans ce pays, c'est le ministre fédéral compétent qui ordonne les activités de surveillance des télécommunications. Sauf en cas

---

126 Voir chapitre 2.

127 Autriche et Belgique.

128 En Allemagne, Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Gemäß § 9 ist die Kommission (außer bei Gefahr im Verzug) vor dem Vollzug zu benachrichtigen.

129 Au Royaume–Uni (Regulation of Investigatory Powers Act, Section 1) et en France (Art. 3 une 4 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

130 En France (Art. 20 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

d'urgence, une commission indépendante, non liée par un mandat (G 10-Kommission[131]) doit en être informée et c'est elle qui statue sur la nécessité et sur la recevabilité de l'intervention. Dans les cas où le service de renseignements à l'étranger est autorisé à pratiquer une surveillance de télécommunications en recourant au filtrage par clés de recherche, la commission statue également sur la recevabilité desdites clés. C'est à cette commission qu'incombe en outre le contrôle de la notification, prévue par la loi, à l'intéressé, ainsi que de la destruction des données recueillies par le BND.

Il existe en outre un organe de contrôle parlementaire (PKGr)[132] composé de neuf députés du Bundestag et qui est chargé de surveiller les activités des trois services de renseignements allemands. Cet organe a le droit de consulter les dossiers, d'entendre les agents des services de renseignements et de se rendre auprès de ces services ainsi que de se faire informer, ce qui ne peut être refusé que pour des raisons impératives d'accès à l'information ou pour des raisons de protection des droits de tiers ou lorsque la substance même de la responsabilité propre de l'exécutif est en jeu. Les travaux de cet organe sont secrets et ses membres sont tenus au devoir de réserve, même après avoir quitté l'organe en question. À mi–législature et à la fin de la législature, cet organe rend compte de ses activités de contrôle au Bundestag.

Ce contrôle presque sans faille des services de renseignements constitue cependant une exception parmi les États membres.

En France[133], seules les activités de surveillance nécessitant une table d'écoute requièrent l'autorisation du Premier ministre. Seules ces activités sont soumises à la surveillance d'une commission ad hoc (commission nationale de contrôle des interceptions de sécurité), qui se compose d'un député et d'un sénateur. L'autorisation d'une écoute demandée par un ministre ou par son délégué est soumise au président de la commission qui, en cas de doute quant à la légalité de l'opération, peut saisir la commission, qui émet des recommandations et, en cas de suspicion de violation de la loi susceptible de poursuites pénales, informe le ministère public. Les opérations d'écoute à des fins de défense des intérêts nationaux qui comportent l'interception de communications par radio ainsi que de communications par satellite ne sont soumises à aucune restriction et échappent donc au contrôle d'une commission.

Les activités des services de renseignements français ne sont par ailleurs pas soumises au contrôle d'une commission parlementaire spéciale, mais des travaux sont en cours à ce sujet. La commission de la défense de l'Assemblée nationale a adopté une proposition[134], mais il n'y a pas encore eu de débat en séance à ce sujet.

Au Royaume-Uni, toute surveillance pratiquée sur le sol britannique nécessite l'autorisation d'un ministre (Secretary of State). Le texte de la loi n'indique toutefois pas clairement si l'"interception" non ciblée de communications soumises à l'épreuve des mots–clés relève de la notion d'interception utilisée dans la "Regulation of Investigatory Powers Act 2000" (RIP) dès lors que l'analyse n'est pas effectuée sur le sol britannique mais communiquée telle quelle à l'étranger, sans évaluation. Le contrôle du respect des dispositions de la RIP 2000 est effectué

---

131 Voir: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, herausgegeben vom Deutschen Bundestag, Sekretariat des PKGr.

132 Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

133 Loi 91-646 du 10 uuillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications.

134 Voir "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", und den diesbezüglichen Bericht von Abgeordnetem Arthur Paecht, N° 1951 Assemblée nationale, 11, législature, 23. November 1999.

a posteriori par des "commissioners" (contrôleurs), des hauts magistrats en fonction ou retraités désignés par le Premier ministre. Le contrôleur chargé des écoutes (Interception Commissioner) contrôle l'octroi des autorisations d'écoute et suit l'examen des plaintes relatives aux écoutes. Le contrôleur responsable de l'Intelligence Service contrôle les autorisations concernant les activités des services de renseignements et de sécurité et suit les enquêtes relatives aux plaintes concernant ces services. L'Investigatory Powers Tribunal, présidé par un haut magistrat, examine toutes les plaintes relatives aux écoutes et aux activités des services.

Le contrôle parlementaire est assuré par l'Intelligence and Security Committee (ISC)[135], qui surveille les activités des trois services de renseignements civils (MI5, MI6 et GCHQ). Il est chargé notamment de contrôler les dépenses et la gestion ainsi que les activités du service de sécurité, du service de renseignements et du GCHQ. Cette commission se compose de neuf membres des deux Chambres mais ne peut compter aucun ministre en son sein. À la différence des commissions de contrôle d'autres pays, qui sont généralement élues ou désignées par le parlement ou par le président du parlement, celle-ci est nommée par le Premier ministre après consultation du chef de l'opposition.

Ces exemples montrent que les niveaux de protection sont très différents. S'agissant du contrôle parlementaire, le rapporteur tient à faire observer que l'existence de commissions chargées de surveiller les services de renseignements est très importante. Ces commissions présentent l'avantage de bénéficier de la confiance des services de renseignements parce que leurs membres sont tenus au secret et que leurs séances se déroulent à huis clos. De plus, ces commissions disposent de pouvoirs particuliers pour s'acquitter de leurs missions, ce qui est indispensable pour surveiller les activités menées dans le domaine secret.

Il convient de se féliciter de ce que la majorité des États membres de l'Union se sont dotés de commissions de contrôle parlementaires pour surveiller les services de renseignements. En Belgique[136], au Danemark[137], en Allemagne[138], en Italie[139], aux Pays–Bas[140] et au Portugal[141], il existe des commissions de contrôle parlementaires qui assurent à la fois le contrôle des services militaires et des services civils. Au Royaume–Uni[142], la commission de contrôle ne s'occupe que des services de renseignements civils (qui sont nettement plus importants), le service militaire étant contrôlé par la commission de la défense. En Autriche[143], les deux branches du service de

---

135 Intelligence services act 1994, Section 10.

136 Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.

137 Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

138 Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

139 Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

140 Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.

141 Conselho de Fiscalização dos Serviços de Informações (CFSI), Gesetz 30/84 vom 5. September 1984, geändert durch das Gesetz 4/95 vom 21. Februar 1995, das Gesetz 15/96 vom 30. April 1996 und das Gesetz 75-A/97 vom 22. Juli 1997.

142 Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

143 Ständigen Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der

renseignements sont contrôlées par deux commissions distinctes qui sont toutefois organisées de la même manière et qui bénéficient des mêmes droits. En Finlande[144] et en Suède[145] le contrôle parlementaire est assuré par un médiateur indépendant élu par le parlement. En France, en Grèce, en Irlande, au Luxembourg et en Espagne, il n'y a pas de commission parlementaire spécialisée. Le contrôle est assuré par les commissions dans le cadre des activités parlementaires général.

9.4. Analyse de la situation du citoyen européen

La situation du citoyen européen apparaît peu satisfaisante. L'ampleur des pouvoirs des services de renseignement en matière de surveillance des télécommunications présente des différences notables. La même remarque s'applique aux organes de contrôle. Tous les États membres qui possèdent un service de renseignements ne disposent pas d'organes de contrôle parlementaires indépendants dotés de pouvoirs de contrôle appropriés. On ne saurait parler d'un niveau de protection uniforme – tant s'en faut.

Du point de vue européen, cela est d'autant plus regrettable que cette situation n'affecte pas tellement les citoyens des États dont le comportement électoral peut influer sur le niveau de protection. Les effets défavorables concernent avant tout les ressortissants des autres États, puisque les activités des services de renseignements à l'étranger concernent par définition l'extérieur du pays. Le citoyen est relativement sans défense face aux systèmes étrangers. Le besoin de protection est donc plus grand encore dans ce domaine. Par ailleurs, il convient de ne pas perdre de vue qu'en raison du caractère particulier des services de renseignements, les citoyens de l'UE peuvent être concernés par les activités de plusieurs services de renseignements en même temps. Une protection uniforme conforme aux principes démocratiques serait souhaitable. Il conviendrait en outre d'examiner dans ce contexte si, en la matière, des dispositions communautaires relatives à la protection des données sont faisables.

Enfin, la question de la protection du citoyen européen se posera en des termes tout nouveaux lorsque, dans le cadre d'une politique de sécurité commune, la coopération entre services de renseignements des États membres deviendra réalité. Dans ce domaine, les institutions européennes seront appelées à adopter des dispositions de protection suffisantes. Il incombera au Parlement, champion du principe de l'État de droit, de faire en sorte qu'un contrôle approprié soit exercé par lui en tant qu'organe disposant d'une légitimité démocratique. Le Parlement devra en outre faire le nécessaire pour garantir le traitement confidentiel de données sensibles et autres documents secrets par une commission spéciale dont les membres seraient tenus au secret. Ce n'est que si ces conditions sont remplies qu'il sera réaliste de réclamer ces pouvoirs de contrôle en vue aussi d'assurer une bonne coopération entre les services de renseignements, coopération indispensable à une politique de sécurité commune digne de ce nom.

---

verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.

144 Ombudsmann, gesetzliche Grundlage für die Kontrolle für die Polizei (SUPO): Poliisilaki 493/1995 §33 und Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, für das Militär: Poliisilaki 493/1995 §33 und Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

145 Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Verordnung (1989:773) über die nationale Polizeibehörde).

10. Protection contre l'espionnage économique

10.1. Économie et espionnage

On observe dans les entreprises économiques trois types d'informations. Premièrement, les informations qui font délibérément l'objet d'une large diffusion. Il s'agit d'informations objectives concernant les produits de l'entreprise (caractéristiques des produits, prix, etc.) et d'informations publicitaires qui influent sur l'image de l'entreprise.

Deuxièmement, il est des informations qui ne sont ni protégées ni diffusées parce qu'elles n'ont rien à voir avec la position concurrentielle de l'entreprise, par exemple la date de l'excursion d'entreprise, les menus de la cantine et la marque des télécopieurs utilisés.

Enfin, il y a les informations qui sont mises à l'abri de l'accès de tiers. Ces informations sont protégées de la concurrence mais aussi, si l'entreprise entend ne pas respecter la loi, de l'État (fisc, embargos, etc.). Différents niveaux de protection sont prévus qui vont jusqu'au secret absolu, par exemple pour les résultats de la recherche avant une demande de brevet ou la production de biens d'armement[146].

Dans le cas qui nous occupe, l'espionnage consiste à se procurer des informations tenues secrètes par une entreprise. Si le responsable est une entreprise concurrente, on parle d'espionnage de concurrence (espionnage industriel). S'il s'agit d'un service de renseignements d'État, on parle d'espionnage économique.

10.1.1. Les objectifs de l'espionnage

Les données stratégiques qui présentent un intérêt pour l'espionnage à caractère économique peuvent être classées suivant les branches et les services d'entreprise.

10.1.1.1. Branches

Il est évident que les informations des secteurs suivants présentent un grand intérêt: biotechnologie, génie génétique, technique médicale, technique environnementale, ordinateurs, logiciels, optoélectronique, stockage de données, céramique, etc.. La liste n'est pas exhaustive et elle se modifie constamment au rythme de l'évolution technique. Dans ces secteurs, l'espionnage consiste principalement à subtiliser des résultats de recherche ou à s'approprier des techniques de production particulières.

10.1.1.2. Départements d'entreprise

Les objectifs de l'espionnage se situent logiquement dans les services de recherche et de développement, d'achat, du personnel, de production, de distribution, de vente, de commercialisation, de produits et financiers. L'importance et la valeur de ces informations sont souvent sous–estimées (voir point 10.1.4).

---

[146] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997.

10.1.2. Espionnage de concurrence

La position stratégique d'une entreprise sur le marché dépend de son statut dans les secteurs de la recherche et du développement, des procédés de fabrication, des lignes de produits, du financement, de la commercialisation, de la distribution, de l'achat et de la main–d'oeuvre[147]. Des informations concernant ces aspects présentent un grand intérêt pour tout concurrent parce qu'elles renseignent sur les projets et sur les points faibles d'une entreprise et permettent de prendre des contre–mesures stratégiques.

Une partie de ces informations sont accessibles au public. Il existe des entreprises de conseil très spécialisées qui, en toute légalité, effectuent des analyses de la concurrence, par exemple Roland & Berger en Allemagne. "Competitive Intelligence" est aujourd'hui un outil standard de gestion aux États–Unis[148]. À partir d'une multitude d'informations, il est possible de brosser le tableau clair d'une situation.

Le passage de la légalité à l'espionnage répréhensible dépend des moyens retenus pour se procurer les informations. On entre dans le domaine criminel dès lors que les moyens utilisés sont illicites. L'établissement d'analyses n'est pas répréhensible en soi. Les informations susceptibles d'intéresser un concurrent sont évidemment protégées et il n'est possible d'y accéder qu'en violant la loi. Les techniques utilisées ne se distinguent pas des méthodes d'espionnage évoquées au chapitre 2.

On ne dispose pas d'indications précises quant à l'ampleur de l'espionnage de concurrence. Comme pour l'espionnage classique, les chiffres occultes sont très élevés. Les deux parties concernées (auteur et victime) n'ont aucun intérêt à faire de la publicité. Pour les entreprises concernées, l'espionnage représente toujours une perte en terme d'image. Quant aux auteurs, ils n'ont aucun intérêt à ce que leurs activités soient mises au jour. Les cas qui sont soumis aux tribunaux sont donc très rares.

La presse fait pourtant sans cesse état de faits d'espionnage de concurrence. Le rapporteur a évoqué ce problème avec les responsables de la sécurité de grandes entreprises allemandes[149] et avec des dirigeants d'entreprises américaines et européennes. On peut dire en résumé que l'espionnage de concurrence, s'il est sans cesse constaté, n'influe pas sur la vie quotidienne des entreprises.

10.2. Les préjudices causés par l'espionnage

L'importance du chiffre occulte ne permet pas de chiffrer avec précision l'ampleur des dommages causés par l'espionnage de concurrence ou l'espionnage économique. À cela s'ajoute le fait que certains de ces chiffres sont volontairement gonflés. Les entreprises de sécurité et les services de contre–espionnage ont intérêt à situer l'ampleur du dommage dans la partie supérieure de l'échelle possible. Il n'empêche que les chiffres donnent une certaine idée.

Dès 1988, l'institut Max Planck évaluait le préjudice dû à l'espionnage économique en Allemagne à 8 milliards de marks au moins[150]. Le président de l'association des entreprises de conseil en sécurité d'Allemagne avance, en s'appuyant sur l'avis d'experts, un chiffre de 15 milliards de marks par an. Le président des syndicats de police européens, Herman Lutz,

147 M.F.Porter, competitive Strategy.
148 Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997.
149 Détails et noms confidentiels.
150 IMPULSE, 3/97, S.13 ff.

chiffre le préjudice à 20 milliards de dollars par an. Le FBI[151] évoque pour les années 1992-1993 un préjudice de 1,7 milliard de dollars subi par l'économie américaine à cause de l'espionnage de concurrence et économique. L'ancien président de la commission de contrôle des services secrets de la Chambre des représentants des États–Unis parle de 100 milliards de dollars de préjudice lié aux commandes perdues et aux frais de recherche et développement supplémentaires. Entre 1990 et 1996, le phénomène a été à l'origine de la perte de 6 millions d'emplois[152].

En fait, il n'est pas nécessaire de connaître le préjudice avec précision. L'État est tenu de lutter contre l'espionnage de concurrence et économique en faisant appel aux services de police et de contre–espionnage indépendamment du montant du préjudice économique. Les chiffres globaux du préjudice ne peuvent servir de base non plus pour déterminer les décisions des entreprises relatives à la protection de l'information et aux mesures de lutte contre l'espionnage. Il appartient à chaque entreprise de calculer le préjudice maximal admissible, d'évaluer les possibilités d'intrusion et de comparer ces chiffres au coût de la sécurité. Le problème ne réside pas dans l'absence de chiffres globaux mais plutôt dans le fait que les grandes entreprises n'effectuent guère d'analyses coût-avantages, de sorte qu'elles négligent la sécurité.

10.3. Qui espionne?

Selon une étude de la société Ernest Young LLP[153], les principaux commanditaires sont les concurrents (39%), les clients (19%), les fournisseurs (9%) et les services secrets (7%). L'espionnage est le fait des propres collaborateurs de l'entreprise, d'officines spécialisées dans l'espionnage, de professionnels rémunérés ou d'agents des services secrets[154].

10.3.1. Collaborateurs de l'entreprise (délit d'initié)

Les ouvrages analysés, les indications des experts devant la commission et les entretiens du rapporteur avec des chefs de la sécurité et des services de contre–espionnage vont tous dans le même sens: le risque le plus grand vient de collaborateurs déçus ou insatisfaits. Faisant partie du personnel de l'entreprise, ils ont un accès direct à l'information, se laissent acheter et pillent les secrets d'entreprise pour leurs commanditaires.

Le risque est grand aussi en cas de changement d'emploi. Actuellement, il n'est pas nécessaire de copier des montagnes de papier pour emporter des informations importantes. Celles–ci peuvent être enregistrées discrètement sur disquette et remises au nouvel employeur lors du changement d'emploi.

10.3.2. Officines spécialisées

Le nombre d'entreprises qui se sont spécialisées dans le pillage d'informations augmente sans cesse. Leurs agents sont en partie d'anciens collaborateurs de services de renseignements. Elles exercent souvent des activités de conseil en sécurité ou de recherche, fournissant des renseignements sur demande. Généralement, elles utilisent des méthodes légales, mais il en est qui recourent à des procédés illicites.

---

151 Congressional Statement, L.J.Freech, Director FBI, 9.5.1996.
152 Robert Lyle, Radio Liberty/Radio fre Europe, 10 février 1999.
153 Computerzeitung, 30.11.1995, S.2.
154 R.Hummelt, Spionage auf dem Datenhighway, München 1997, pp. 49 et suiv..

10.3.3. Hackers

Il s'agit de spécialistes de l'informatique qui, grâce à leurs connaissances, parviennent à accéder de l'extérieur aux réseaux informatiques. Initialement, il s'agissait de fous d'ordinateurs qui prenaient plaisir à venir à bout des mesures de sécurité des systèmes. Aujourd'hui, ils agissent sur commande, tant auprès des services que sur le marché.

10.3.4. Services de renseignements

La guerre froide ayant pris fin, les missions des services de renseignements ont évolué. La criminalité internationale organisée et l'économie constituent de nouveaux terrains d'activité (voir détails au chapitre 10, point 10.5).

10.4 Comment espionne–t–on?

D'après les informations fournies par les services de contre–espionnage et les responsables de la sécurité de grandes entreprises, l'espionnage économique a recours à toutes les méthodes et instruments du renseignement (voir point 2.4). Toutefois, les entreprises présentent des structures plus ouvertes que l'armée ou les services de renseignements ou encore les services gouvernementaux. Le domaine économique présente des risques supplémentaires:

- il est plus facile de trouver des collaborateurs parce que les possibilités offertes par la sécurité des entreprises ne sont pas comparables à celles des services de contre–espionnage;
- la mobilité de l'emploi fait que des informations importantes peuvent être emportées au moyen de l'ordinateur portable; le vol de tels appareils ou la copie discrète du disque dur après intrusion dans une chambre d'hôtel font partie des techniques habituelles de l'espionnage économique;
- l'intrusion dans les réseaux informatiques est plus facile que lorsqu'il s'agit d'organismes publics sensibles à la sécurité: les petites et moyennes entreprises ne sont pas sensibilisées aux problèmes de sécurité et prennent peu de précautions;
- les écoutes (voir point 3.2) sont elles aussi plus simples, pour les mêmes raisons.

L'analyse des informations recueillies fait ressortir que l'espionnage économique s'opère sur place ou sur le lieu de travail mobile parce que, à de rares exceptions près (voir point 10.6), les informations recherchées ne peuvent être obtenues en interceptant les communications internationales.

10.5. Espionnage économique d'État

10.5.1. Espionnage économique stratégique effectué par les services de renseignements

La fin de la guerre froide a libéré des capacités de renseignements qui se sont investies dans d'autres domaines. Les États–Unis ne cachent pas qu'une partie de leurs activités de renseignements concerne aussi l'économie. Cela englobe notamment le contrôle du respect des sanctions économiques, le contrôle du respect des conditions de livraison d'armes ou de biens à usage mixte, l'évolution des marchés des matières premières et celle des marchés financiers internationaux. D'après ce que le rapporteur a pu constater, les services américains ne sont pas les seuls à s'intéresser à ce domaine et cela ne fait pas l'objet d'une réprobation massive.

10.5.2. Les services de renseignements, agents de l'espionnage de concurrence

Ce qui suscite des critiques, c'est le fait que des services de renseignements soient mis à contribution pour procurer aux entreprises du pays des avantages dans la concurrence internationale. On distingue deux types de cas[155]:

10.5.2.1. Pays très avancés sur le plan technologique

Les pays très industrialisés peuvent profiter de l'espionnage industriel. En se renseignant sur l'état de développement d'un secteur, ils peuvent prendre des mesures (économie extérieure ou aide financière) qui améliorent la compétitivité de leur industrie ou leur permettent d'économiser des subventions. Un autre aspect important peut résider dans l'obtention de détails relatifs aux marchés à valeur élevée (voir point 10.6).

10.5.2.2. Pays moins avancés sur le plan technique

Certains de ces pays sont confrontés aux problèmes de l'acquisition de savoir–faire technique, à l'effet de combler le retard qu'accusent leurs industries, et ce sans avoir à supporter de frais de développement et de redevances de licences. Ils doivent en outre se procurer des informations sur les produits et les techniques de fabrication afin de mettre sur le marché mondial, dans des conditions concurrentielles, des copies fabriquées à peu de frais (salaires). Il est établi que les services russes se sont vu confier cette tâche. La loi n° 5 de la Fédération de Russie relative aux renseignements étrangers mentionne l'acquisition d'informations économiques et technico–économiques parmi les missions des services de renseignements.

D'autres États (notamment Iran, Irak, Syrie, Libye, Corée du nord, Inde et Pakistan) ont à se procurer des informations pour leurs programmes nationaux d'armement, principalement dans le secteur nucléaire et dans celui des armes chimiques et biologiques. Un autre volet des activités des services de ces pays réside dans la gestion d'entreprises de couverture leur permettant d'acheter, sans éveiller les soupçons, des biens à usage mixte.

[155] Indication confidentielle d'un service de contre–espionnage, source protégée.

10.6. ECHELON est-il adapté à l'espionnage industriel?

Le contrôle stratégique des télécommunications internationales ne permet d'obtenir des informations utiles dans le contexte de l'espionnage de concurrence que par hasard. De fait, les informations sensibles se trouvent principalement dans les entreprises mêmes, de sorte que l'espionnage de concurrence consiste à tenter de les obtenir par l'entremise de collaborateurs ou de personnes infiltrées ou encore en pénétrant dans les réseaux informatiques. C'est seulement lorsque des données sensibles parviennent à l'extérieur par câble ou par voie hertzienne (satellite) qu'un système de surveillance peut être utilisé pour l'espionnage de concurrence. Cela se pratique systématiquement dans trois cas:

- pour les entreprises qui travaillent dans trois régions–horaires: les résultats intérimaires d'Europe sont envoyés en Amérique puis en Asie;
- dans le cas de vidéoconférences d'entreprises multinationales qui se déroulent grâce à des satellites ou à des liaisons câblées;
- lorsque des marchés importants sont négociés sur place (construction d'usines, infrastructures de télécommunications, construction de systèmes de transport, etc.), endroit à partir duquel il faut en référer à la maison–mère.

Si dans ces cas les entreprises ne protègent par leurs communications, l'interception de ces dernières fournit des données précieuses du point de vue de l'espionnage de concurrence.

10.7. Cas divulgués

On compte quelques cas d'espionnage économique ou de concurrence qui ont été évoqués dans la presse ou dans la littérature spécialisée. Une partie de ces sources ont été compulsées. On trouvera un résumé dans le tableau ci-après. Sont indiqués les participants, la date des faits, ce qui s'est passé, quel était l'objectif visé et quelles ont été les conséquences.

Il est à noter qu'une même affaire fait parfois l'objet de comptes rendus très divergents. Citons à titre d'exemple le cas Enercon: selon les sources, l'"auteur" est la NSA ou le ministère américain de l'économie ou encore la concurrence photographique.

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
Air France	DGSE	jusqu'en1994	Conversations d'hommes d'affaires en déplacement	Des micro-punaises ont été découverts dans les cabines de première classe d'Air France. La compagnie a fait des excuses publiques.	Collecte d'informations.	Non précisé.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/
Airbus	NSA	1994	Informations relatives à un achat d'avions entre Airbus et la compagnie d'Arabie saoudite.	Interception de fax et de communications téléphoniques entre les partenaires.	Transmission des informations aux concurrents américains Boeing et McDonnell-Douglas.	Les Américains ont conclu un marché de 6 milliards de dollars.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Airbus	NSA	1994	Contrat de 6 milliards de dollars avec l'Arabie saoudite. Mise au jour d'une manœuvre de corruption du consortium européen Airbus.	Interception de fax et de communications téléphoniques entre le consortium Airbus et la compagnie le gouvernement d'Arabie saoudite par satellites de communication.	Mise au jour d'une manœuvre de corruption.	McDonnell-Douglas, le concurrent américain d'Airbus, a obtenu le marché.	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Distributeur	non précisé	Description du procédé de fabrication de la matière première d'une crème dermatologique de l'entreprise BASF (département cosmétique)	Non précisé	Non précisé	Aucune car affaire éventée.	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Oktober 1992
Ministère fédéral de l'économie	CIA	1997	Informations sur des produits de haute technologie au ministère fédéral de l'économie.	Intervention d'un agent.	Collecte d'informations.	L'agent a été démasqué et expulsé.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministère fédéral de l'économie	CIA	1997	Arrière-plan du processus Myconos de Berlin, crédits Hermès concernant les exportations vers l'Iran, structure d'entreprises allemandes fournissant des produits de haute technologie à l'Iran.	Un agent de la CIA se faisant passer pour un ambassadeur américain a mené des conversations amicales avec le chef pour la région arabe (principalement l'Iran) du service compétent du ministère fédéral de l'économie.	Collecte de renseignements.	Non précisé. Un fonctionnaire s'est adressé aux services de sécurité allemands, qui ont signalé aux Américains que l'opération de la CIA était inopportune. L'agent de la CIA a été rappelé.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
Dasa	Renseignements russes	1996 – 1999	Vente et transfert de documents relatifs aux technologies d'armement d'une entreprise munichoise (d'après SZ/30.5.2000: Dasa à Ottobrunn)	2 Allemands en mission.	Collecte de renseignements sur les systèmes d'armes (blindés et DCA).	SZ/30.5.2000: Trahison "pas très grave" du point de vue militaire. Cela s'applique également au préjudice économique, constate le tribunal.	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001 „Haftstrafe wegen Spionage für Russland“, SDZ / 30. Mai 2000

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
Embargo	BND	vers 1990	Reprise des exportations de technologies sous embargo à destination de la Libye (notamment Siemens).	Interception de télécommunications.	Mise au jour de transferts illégaux d'armes et de technologies.	Aucune conséquence particulière, les livraisons n'ont pas été interdites.	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 110
Enercon	Experts en énergie éolienne d'Oldenburg et collaboratrice de Kenetech	Non précisé.	Éolienne de la société Enercon	Non précisé.	Non précisé.	Non précisé.	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001
Enercon	NSA	Non précisé.	Éolienne pour la production d'électricité développée par l'ingénieur A. Wobben	Non précisé.	Communication d'éléments techniques de Wobben à une entreprise américaine.	L'entreprise américaine demande le brevet avant Wobben, qui est attaqué en justice par un cabinet d'avocats américain (infraction au droit des brevets).	„Aktenkrieger“, SZ, 29. März 2001
Enercon	Entreprise américaine Kenetech	1994	Détails importants d'une éolienne de haute technologie.	Photographies.	Demande de brevet couronnée de succès aux États-Unis.	Enercon GmbH a laissé tomber ses projets de conquête du marché américain.	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
Enercon	Ingénieur W. et entreprise américaine Kenetech	Mars 1994	Éolienne de type E-40 d'Enercon	L'ingénieur W. fournit des informations, une collaboratrice de Kenetech photographie l'installation et des détails.	Kenetech cherche des preuves pour une plainte pour infraction au droit des brevets contre Enercon. Enercon: collecte illicite d'informations touchant à des secrets d'entreprise. Un journaliste de la télévision aurait appris d'un ancien collaborateur de la NSA que ce qu'Enercon savait d'Echelon avait été communiqué par les Américains à Kenetech.	Non précisé.	„Klettern für die Konkurrenz“, SZ 13. Oktober 2000
Enercon	Kenetech Windpower	Avant 1996	Données relatives à une éolienne d'Enercon.	Des ingénieurs de Kenetech photographient le dispositif.	Reconstitution du système chez Kenetech.	Enercon obtient justice; action contre les espions; estimation de la perte: plusieurs centaines de millions de marks.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministre du commerce du	CIA	1996	Négociations relatives à des quotas d'importation de	Piratage du système informatique du ministère	L'américain M. Kantor approuverait l'offre la plus	Kantor accepte l'offre la plus basse.	„Wirtschaftsspionage: Was macht eigentlich die

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
Japon			voitures américaines sur le marché japonais.	japonais du commerce.	basse.		Konkurrenz?“ von Arno Schütze, 1/98
Automobiles japonaises	Gouverne m. américain	Non précisé.	Négociations concernant l'importation de véhicules de luxe japonais. Informations concernant les normes d'émission des voitures japonaises.	COMINT, sans précision.	Collecte de renseignements.	Non précisé.	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
López	NSA	Non précisé.	Vidéoconférence de VW et López	Interception à partir de Bad Aibling.	Transmission des informations à General Motors et à Opel.	L'interception aurait fourni au ministère public des indications très précises pour une enquête.	Bundeswehrhauptmann Erich Schmidt-Eenboom, zitiert in „Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López et 3 de ses collabora-teurs	1992 - 1993	Documents et données des secteurs de la recherche, de la planification, de la fabrication et des achats (documents relatifs à une usine en Espagne, informations relatives au coût de différents modèles, études de projets, stratégies d'achat et d'économies).	Collecte de matériel.	Utilisation par VW des documents de General Motors.	Règlement à l'amiable entre les groupes. López démissionne de ses fonctions de directeur de VW. VW se sépare en 1997 de 3 autres collaborateurs de l'équipe López, verse 100 millions de dollars à GM/Opel (prétendus frais d'avocat) et achète durant 7 ans des pièces de rechange pour un total de 1 milliard de dollars à GM/Opel.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
López	NSA	1993	Vidéoconférence entre López et le directeur de VW F. Piëch	Extrait de vidéoconférence et communication à GM.	Protection des secrets de l'entreprise américaine GM que López entendait communiquer à VW (tarifs, projets secrets relatifs à une nouvelle usine et à un nouveau véhicule).	López est démasqué, l'action en justice est suspendue en 1998 moyennant versement d'amendes. Rien au sujet de NSA.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000 „Abgehört“, Berliner Zeitung, 22. Januar 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28. Juli 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Alamos	Israel	1988	Deux collaborateurs du programme israélien de recherche nucléaire forcent l'ordinateur central du laboratoire nucléaire de Los	Piratage.	Collecte de renseignements sur de nouveaux détonateurs nucléaires américains.	Aucune conséquence particulière; les pirates s'enfuient en Israël; l'un d'entre eux est arrêté mais aucun lien avec les services secrets	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 137

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			Alamos.			israéliens n'est officiellement évoqué.	
Contrebande	BND	Années 70	Contrebande d'installations informatiques en RDA.	Non précisé.	Mise au jour de transferts de technologies à destination du bloc de l'Est.	Pas de conséquences particulières, les livraisons ne sont pas interdites.	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 113
TGV	DGSE	1993	Calcul des coûts de Siemens. Commande pour la livraison de trains à grande vitesse destinés à la Corée du Sud.	Non précisé.	Offre inférieure.	Le constructeur ICE perd le marché au profit d'Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Non précisé.	1993	Calcul des coûts d'AEG et de Siemens concernant un marché public en Corée du Sud concernant la fourniture de trains à grande vitesse.	Siemens dénonce une interception de ses communications téléphoniques et par fax dans son établissement de Séoul.	Avantage pour le concurrent anglo-français GEC-Alsthom.	GEC-Alsthom est retenu alors que l'offre allemande était plus favorable.	„Abgehört“, Berliner Zeitung, 22. Januar1996
Thomson-Alcatel et Raytheon	CIA/ NSA	1994	Passation d'un marché brésilien relatif à la surveillance par satellite de l'Amazone à la firme française Thomson-Alcatel (1,4 milliard de dollars).	Interception des communications du soumissionnaire retenu (Thomson-Alcatel).	Mise au jour d'une opération de corruption.	Clinton se plaint auprès du gouvernement brésilien; sous la pression du gouvernement des États-Unis, le marché est réattribué à l'entreprise américaine Raytheon.	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 91
Thomson-Alcatel et Raytheon	Ministère américain de l'économie	1994	Négociations relatives à un projet de surveillance par radar de la forêt tropicale brésilienne.	Non précisé.	Obtention du marché.	Les groupes français Thomson CSF et Alcatel perdent le marché au profit de l'entreprise américaine Raytheon.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Thomson-Alcatel et Raytheon	NSA Ministère du commerce	Minisitère du commerce	Négociations relatives à un projet (1,4 milliard de dollars) relatif à la surveillance de l'Amazone. Mise au jour d'une opération de corruption du groupe de sélection brésilien. Remarque de Campbell: Rayethon équipe une station d'interception à Sugar Grove.	Interception des négociations entre Thomson CSF et le Brésil et communication à Raytheon.	Mise au jour d'une affaire de corruption; obtention du marché.	Raytheon obtient le marché.	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Marché relatif à l'exploitation de gaz et de pétrole en mer du Nord.	Interception de fax du soumissionnaire retenu (Thyssen).	Mise au jour d'une affaire de corruption.	BP réclame des dommages-intérêts à Thyssen.	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 92
VW	Non précisé.	„années passées“	Non précisé.	Caméra infrarouge enterrée et transmettant ses images par voie hertzienne.	Collecte de renseignements sur les innovations.	VW annonce des pertes considérables.	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
VW	Non précisé.	1996	Circuit d'essais de VW.	Caméra cachée.	Informations concernant les nouveaux modèles de VW.	Non précisé.	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11. Juni 1998

10.8. Protection contre l'espionnage économique

10.8.1. Protection juridique

Les systèmes juridiques des pays industrialisés punissent le vol de secrets d'entreprise. Comme dans tous les autres domaines du droit pénal, les niveaux de protection nationaux sont différents. En règle générale, les sanctions sont nettement moins sévères que dans les cas d'espionnage en rapport avec la sécurité militaire. Dans nombre de cas, l'espionnage de concurrence n'est interdit que s'il concerne des entreprises du pays, pas s'il concerne des entreprises de l'étranger. Tel est également le cas aux États-Unis.

La législation afférente n'interdit essentiellement que l'espionnage entre entreprises. Il est douteux qu'elle restreigne aussi les activités des services de renseignements nationaux. En effet, les dispositions qui ont créé ceux-ci les autorisent à s'emparer des informations.

Un cas limite se présente lorsqu'un service de renseignements obtient par espionnage des informations qu'il met à la disposition de différentes entreprises. Normalement, ce cas n'est plus couvert par les dispositions qui donnent des pouvoirs spéciaux aux services de renseignements. Au sein de l'UE, il s'agirait là d'une infraction au traité CE (voir point ...).

Abstraction faite de cela, il serait très difficile à une entreprise, dans la pratique, de s'adresser aux tribunaux. L'interception ne laisse pas de trace, c'est-à-dire pas de preuve utilisable en justice.

10.8.2. Autres entraves à l'espionnage économique

Les différents pays acceptent le fait que les services de renseignements, dans la recherche d'informations stratégiques, exercent aussi leurs activités dans le domaine économique. Toutefois, il est largement porté atteinte à ce "gentleman's agreement" en cas d'espionnage de concurrence au profit des industries nationales. Si un pays est pris la main dans le sac, il se trouve confronté à de gros problèmes politiques. Cela s'applique aussi à une puissance mondiale telle que les États-Unis, qui verraient leurs prétentions au leadership politique mondial gravement compromises. Les puissances moyennes pourraient se permettre cela, mais pas une puissance mondiale.

À côté des problèmes politiques, se pose la question pratique de savoir à quelle entreprise communiquer les résultats de l'espionnage de concurrence. Dans le secteur de la construction aéronautique, la réponse est facile parce qu'il n'y a que deux grands fournisseurs au monde. Dans tous les autres cas, les fournisseurs sont nombreux et ils ne sont pas propriété de l'État, ce qui rend difficile d'en favoriser un. S'agissant de la communication d'informations relatives aux offres de concurrents dans le contexte de marchés publics internationaux, la communication à tous les concurrents du pays serait concevable. Tel est notamment le cas lorsqu'il existe une structure gouvernementale de soutien accessible à tous les concurrents du pays - ce qui est le cas aux États-Unis (Advocacy Center). En cas de vol de technologie débouchant sur une demande de brevet, l'égalité de traitement des entreprises devient

impossible.

Cela poserait un grave problème dans le système politique américain. Les hommes politiques américains sont largement tributaires, pour le financement de leurs campagnes électorales, des dons des entreprises de leur circonscription. Si un cas de favoritisme des services de renseignements à l'égard d'une entreprise était divulgué, il y aurait des remous considérables dans le système politique. Pour reprendre la formule de l'ancien directeur de la CIA Woolsey, lors d'un entretien avec les représentants de la commission: "In this case the hill (i.e. the US-Congress) would go mad!" ("Dans ce cas, le Congrès deviendrait enragé!"). À n'en pas douter!

10.9. Les États–Unis et l'espionnage économique

10.9.1. Position officielle des Américains sur l'espionnage économique

L'ancien directeur de la CIA Woolsey et le président de la commission de contrôle des services secrets de la Chambre des représentants, Porter Goss, ont pris position comme suit - en résumé - lors d'entretiens:

1. les États-Unis surveillent les communications internationales afin de se procurer des informations générales sur l'évolution économique, sur les livraisons de biens à usage mixte et sur le respect des embargos,
2. les États-Unis surveillent spécialement les communications d'entreprises dans le contexte de la passation de marchés afin d'empêcher les distorsions liées à la corruption au détriment des entreprises américaines.

La corruption est interdite aux entreprises américaines et les responsables du contrôle sont tenus de signaler les versements de pots de vin. Si la surveillance des communications permet de constater des affaires de corruption dans les marchés publics, l'ambassadeur des États-Unis intervient auprès du gouvernement du pays concerné. Les entreprises américaines concurrentes ne sont en revanche pas informées directement.

10.9.2. Rôle de l'Advocacy Center dans la promotion des exportations américaines

10.9.2.1. Missions de l'Advocacy Center

L'Advocacy Center, implanté au ministère américain du commerce, est l'élément clé de la stratégie d'exportations menée par Clinton et poursuivie par Bush. Créé en 1993, ce centre a aidé des centaines d'entreprises américaines à obtenir des marchés publics à l'étranger. Il rassemble les ressources gouvernementales américaines en matière d'expertise dans différents domaines, de l'attaché économique d'ambassade jusqu'à la Maison blanche.

10.9.2.2. Méthodes de travail

Le centre n'occupe qu'une petite équipe de 12 personnes (situation à la date du 6.2.2001). Il est l'interlocuteur central des entreprises et représente les différents services de l'administration américaine qui s'occupent de la promotion des exportations. Il intervient de manière non discriminatoire vis-à-vis des entreprises mais, en vertu de règles très claires, ne soutient que des projets conformes aux intérêts nationaux des États-Unis. Les produits fournis doivent, du point de vue de la valeur, provenir à 50 % au moins des États-Unis.

10.9.2.3. Questions sans réponse

Le gouvernement américain n'a pas autorisé les entretiens que les membres de la commission souhaitaient avoir avec le Centre. Deux questions qui suscitent des doutes n'ont donc pu être tirées au clair:

a) la commission dispose de documents qui semblent établir une participation de la CIA aux activités du Centre,

b) parmi les informations qu'il fournit sur Internet, le Centre indique qu'il rassemble les ressources de 19 "government agencies" des États-Unis. Par ailleurs, il n'est fait état que de 14 organismes. Pourquoi les noms de 5 de ceux-ci ne peuvent-ils être rendus publics?

10.10. Sécurité des réseaux informatiques

À compléter.

10.11. Sous–estimation des risques

Le rapporteur doit encore avoir des entretiens à ce sujet et analyser de la documentation écrite. Seront examinés les aspects suivants:

10.11.1. Grandes entreprises

10.11.2. Petites et moyennes entreprises

10.11.3. Institutions européennes

10.11.4. Établissements de recherche

11. Le cryptage en tant qu'instrument d'autoprotection

11.1. Objectif et mode de fonctionnement du cryptage

11.1.1. Objectif du cryptage

Toute transmission d'informations porte en elle le risque que ladite information tombe aux mains de personnes non autorisées. Si l'on veut éviter que des tiers ne prennent connaissance des informations, il faut les placer dans l'impossibilité de lire ou d'écouter le message, c'est-à-dire crypter celui-ci. Dans le domaine militaire et diplomatique, les techniques de cryptage ont toujours été employées[156].

Au cours des vingt dernières années, l'importance du cryptage a grandi parce qu'un pourcentage sans cesse croissant des communications prennent le chemin de l'étranger, où le pays d'origine ne peut plus protéger le secret de la correspondance ou des communications. De plus, les possibilités techniques accrues dont dispose un État d'écouter ou d'intercepter légalement les communications débouchent sur un besoin accru de protection des citoyens préoccupés. Enfin, le désir accru des délinquants d'accéder illégalement aux informations, voire de les falsifier, a été à l'origine de mesures de protection (par exemple dans le secteur bancaire).

L'invention des communications électriques et électroniques (télégraphe, téléphone, radio, télécopieur, Internet) a notablement simplifié la transmission de l'information et l'a considérablement accélérée. Le hic est que cela ne s'est pas assorti d'une protection technique contre les écoutes/interceptions et que n'importe qui peut, à condition de disposer de l'appareillage nécessaire, intercepter une communication s'il a accès aux vecteurs. Effectuées de manière professionnelle, les interceptions ne laissent pas ou guère de traces. Le cryptage a donc pris une importance nouvelle. Le secteur bancaire a été le premier à utiliser systématiquement le cryptage pour protéger les communications auxquelles a donné lieu l'apparition de la monnaie électronique. L'internationalisation croissante de l'économie s'est également accompagnée, du moins dans une certaine mesure, du cryptage des communications. Les communications via Internet, non protégées, ont fait grandir le besoin éprouvé par les particuliers de mettre leurs communications à l'abri des écoutes.

La question se pose donc, dans le contexte du présent rapport, de savoir s'il existe des méthodes de cryptage des communications intéressantes du point de vue du coût, autorisées par la loi, suffisamment sûres et simples à appliquer pour se mettre à l'abri des écoutes.

11.1.2 Mode de fonctionnement du cryptage

Le principe du cryptage consiste à traiter un texte en clair de telle manière qu'il n'ait plus de sens ou qu'il ait un sens différent. Les initiés peuvent toutefois le décrypter. Lors du cryptage, une séquence pertinente de lettres est modifiée, de telle manière qu'une personne non initiée ne peut plus la comprendre.

[156] On en trouve la preuve jusque dans l'Antiquité, par exemple à Sparte au V^{e} siècle après Jésus-Christ.

Cela s'effectue suivant une méthode déterminée (algorithme de cryptage) reposant sur la permutation de lettres (transposition) et/ou le remplacement de lettres par d'autres (substitution). La méthode de cryptage (algorithme) n'est plus tenue secrète à l'heure actuelle. Au contraire, il a été procédé récemment à un appel d'offres public à l'échelle mondiale au sujet de la nouvelle norme mondiale de cryptage à utiliser dans le domaine économique. La même remarque s'applique à la réalisation d'un algorithme de cryptage déterminé pour tel ou tel appareil – par exemple un télécopieur crypté.

Ce qui est secret, c'est ce que l'on appelle la clé. Un exemple emprunté à un domaine apparenté permettra d'expliquer la situation. Le mode de fonctionnement des serrures est normalement connu de tous, ne serait-ce que parce que les serrures sont brevetées. La protection d'une porte tient au fait que, pour un type déterminé de serrure, il peut y avoir de nombreuses clés différentes. Il en va de même du cryptage des informations: une méthode de cryptage connue de tous (algorithme) permet de tenir secrètes de nombreuses informations différentes grâce à des clés tenues secrètes.

Pour illustrer les notions évoquées ci-dessus, citons l'exemple du cryptage de César. Général romain, César cryptait les informations en remplaçant chaque lettre par celle venant trois lettres plus loin dans l'alphabet – A par D, B par E et ainsi de suite. Le codage du mot **ÉCHELON** donne alors le mot **HFKHORQ**. L'algorithme consiste ici à déplacer les lettres dans l'alphabet et la clé consiste à se décaler de trois lettres dans l'alphabet. Le cryptage et le décryptage s'effectuent de la même manière, à savoir en se décalant de trois lettres dans l'alphabet. Le procédé est donc symétrique. Aujourd'hui, un tel procédé n'assurerait pas une protection d'une seconde.

Une bonne méthode de cryptage peut être connue de tous tout en méritant quand même le qualificatif de sûre. Il faut pour cela que le nombre des clés possibles soit si grand qu'il devienne impossible de les essayer toutes dans un délai raisonnable, même en utilisant l'ordinateur. Toutefois, le nombre des clés n'est pas en soi une garantie de sécurité dès lors que la méthode de cryptage débouche sur un texte offrant des éléments permettant le décryptage (par exemple fréquence de certaines lettres)[157]. Sous ces deux angles, le cryptage de César n'est pas une méthode sûre. En raison de la fréquence différente des lettres dans une langue, la simple substitution permet de forcer rapidement le procédé, d'autant qu'il n'y a que 25 possibilités de décalage, c'est-à-dire 25 clés, l'alphabet ne comptant que 26 lettres. À force d'essais, il est facile de trouver la bonne clé et de déchiffrer le texte.

Les caractéristiques d'un système sûr seront examinées ci-après.

11.2. Sécurité des systèmes de cryptage

11.2.1. Généralités

Demander qu'un système de cryptage soit sûr peut signifier deux choses. Premièrement, on attend peut-être qu'il soit absolument sûr, c'est-à-dire qu'il soit impossible de déchiffrer le

[157] Voir Vom diplomatischen Code zur Fallfürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999, 26 ff.

message si l'on ne connaît pas la clé, cette impossibilité pouvant être prouvée mathématiquement. Deuxièmement, il peut suffire que le code ne puisse être forcé dans l'état actuel de la technique, la sécurité étant ainsi assurée temporairement, c'est-à-dire nettement plus longtemps que le laps de temps critique pendant lequel une information doit rester secrète.

11.2.2. Sécurité absolue: one-time pad

À l'heure actuelle, seul le one–time pad représente un procédé entièrement sûr. Il a été mis au point à la fin de la première guerre mondiale[158] et également appliqué ultérieurement aux téléscripteurs de crise entre Moscou et Washington. Il repose sur une clé constituée par une séquence tout à fait aléatoire de lettres, séquence qui n'est pas répétitive. L'expéditeur et le destinataire cryptent au moyen de ces séquences puis détruisent la clé après usage. Étant donné que la clé ne présente aucun ordre interne, il est impossible à un analyse de venir à bout du code. Cela peut être prouvé mathématiquement[159].

L'inconvénient du système tient au fait qu'il n'est pas facile de produire de grandes quantités de telles clés aléatoires[160] et qu'il est difficile et peu pratique de répartir les clés de manière sûre. La méthode n'est donc pas utilisée largement dans les transactions.

11.2.3. Sécurité relative en fonction de l'état de la technique

11.2.3.1 Utilisation de machines de cryptage et de décryptage

Dès avant l'invention du one–time pad, on avait mis au point des procédés de cryptage offrant un grand nombre de clés et produisant des textes cryptés présentant le moins possible de régularité, c'est-à-dire d'éléments permettant une analyse. Pour rendre ces méthodes praticables à bref délai, des machines de cryptage et de décryptage furent mises au point. La plus fameuse fut ENIGMA[161], employée par l'Allemagne durant la deuxième guerre mondiale. L'armée de spécialistes du décryptage en activité a Beltchley Park au Royaume–Uni parvint à venir à bout du cryptage d'ENIGMA grâce à des machines spéciales appelées "bombes". Comme ENIGMA, les "bombes" étaient des machines mécaniques.

11.2.3.2. Utilisation de l'ordinateur

L'invention de l'ordinateur représenta une percée dans le domaine du cryptage car ses performances rendent possible l'emploi de systèmes de plus en plus complexes. Si cela ne change rien aux principes fondamentaux de cryptage, il y eut cependant des innovations. Pour commencer, le degré de complexité des systèmes de cryptage fut multiplié car le matériel n'était plus soumis aux contraintes de la mécanique. De plus, la vitesse de cryptage fut nettement accrue.

---

158 Introduit par le major Joseph Mauborgne, chef du service cryptographique de l'armée américiane. Voir Singh, Messages secrets (1999), 151.

159 Voir Singh, Geheime Botschaften (1999), 151 ff.

160 Voir Wobst, Abenteuer Kryptologie[2] (1998), 60.

161 Mise au point et brevetée en 1928 par Arthur Scherbius. Elle s'apparentait dans une certaine mesure à une machine à écrire car elle était munie d'un clavier qui permettait de transcrire le texte en clair. Un dispositif rotatif permettait le cryptage et le texte pouvait être décrypté avec la même machine grâce à des codes.

L'ordinateur traite l'information au moyen de nombres binaires. L'information est traduite sous forme de deux signaux, zéro et un. Un correspond à une tension électrique, zéro à l'interruption de la tension. Dans ce contexte, c'est la norme ASCII[162] qui s'est imposée: chaque lettre est représentée par une combinaison à 6 chiffres de 0 et de 1[163]. Un texte se présente donc sous la forme d'une multitude de 0 et de 1 et ce sont des chiffres et non des lettres qui sont cryptés.

Cela permet de recourir aux formules de transposition et de substitution. La substitution peut par exemple passer par l'insertion d'une clé prenant la forme d'une suite de chiffres. Suivant les règles de la mathématique binaire, la somme de chiffres identiques donne O (0+0=0 et 1+1=0). La somme de deux chiffres différents donne 1 (0+1=1). La nouvelle séquence cryptée résultant de l'insertion est donc une suite binaire qui peut être numérisée ou qui peut être rendue lisible en retirant la clé ajoutée.

L'ordinateur permet, grâce à des algorithmes de cryptage puissants, de produire des textes cryptés n'offrant pour ainsi dire aucune prise à l'analyse. Une tentative de décryptage ne peut plus être effectuée qu'en essayant toutes les clés possibles. Plus la clé est longue et plus la tentative est vouée à l'échec même si l'on utilise des ordinateurs très performants et si l'on y consacre le temps nécessaire. Il existe donc des méthodes praticables qui peuvent être considérées comme sûres à la lumière de l'état de la technique.

11.2.4. Normalisation et limites de la sécurité

La propagation de l'ordinateur au cours des années 70 a rendu plus nécessaire la normalisation des systèmes de cryptage, indispensable pour permettre aux entreprises de communiquer avec leurs partenaires en toute sécurité et moyennant un effort raisonnable. Les premières tentatives en ce sens eurent lieu aux États-Unis.

Un système de cryptage puissant peut aussi être utilisé à des fins malveillantes ou par un éventuel adversaire militaire. Il peut rendre difficile ou impossible l'espionnage électronique. C'est pourquoi la NSA demanda avec insistance qu'une norme de cryptage suffisamment sûre soit retenue pour l'économie. Elle conservait toutefois une possibilité de décryptage grâce à son équipement technique particulier. La longueur de la clé fut limitée à 56 bits. Cela réduit le nombre des clés possibles à 100 000 000 000 000 000[164]. C'est le 23 novembre 1976 que le chiffre de Lucifer d'Horst Feistel fut officiellement adopté dans la version à 56 bits sous la dénomination de Data Encryption Standard (DES), qui fut durant un quart de siècle la norme de cryptage officielle américaine. Elle fut adoptée en Europe et au Japon, notamment dans le secteur bancaire. L'algorithme de cette norme n'a jamais été percé, en dépit de ce qu'ont affirmé différents médias, mais il existe aujourd'hui des machines suffisamment puissantes pour essayer toutes les clés ("brute force attack"). La DES–Triple, dont la clé compte 112 bits, est toujours considérée comme sûre. Le successeur de la DES, à savoir l'AES (Advanced Encryption Standard) est une méthode européenne[165], conçue sous le nom Rijndael à Louvain,

---

162 American Standard Code for Information Interchange.

163 A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc.

164 Ce nombre, sous forme binaire, compte 56 zéros et uns. Voir Singh, Geheime Botschaften (1999), 03.

165 Définie par deux cryptographes belges de l'Université catholique de Louvain , Joan Daemen et Vincent

en Belgique. Ce procédé est rapide et considéré comme sûr car il échappe à la contrainte de la longueur de la clé. Cela s'explique par une modification de l'approche américaine (voir point 1.4).

La normalisation a représenté une simplification notable du cryptage pour les entreprises. Le problème de la distribution des clés subsiste cependant.

11.3. Problème de sécurité en matière de diffusion des clés

11.3.1. Cryptage asymétrique: procédé de la public–key

Aussi longtemps qu'un système fonctionne avec un clé permettant à la fois le cryptage et le décryptage (symétrie), il est difficile à utiliser avec de nombreux partenaires de communication. En effet, la clé doit être communiquée préalablement à chaque nouveau partenaire, et ce de telle manière qu'aucun tiers ne puisse en avoir connaissance. Dans la pratique, cela est très difficile dans le monde économique et possible seulement dans des cas isolés pour les particuliers.

Le codage asymétrique offre une solution: on n'utilise pas la même clé pour coder et pour décrypter. L'information est cryptée au moyen d'une clé qui peut être connue de tous et que l'on appelle la clé publique. Toutefois, le système fonctionne à sens unique: la clé publique ne permet pas le décryptage du texte. Toute personne qui souhaite obtenir une information cryptée peut transmettre sa clé publique à son partenaire par une voie peu sûre pour qu'il code l'information. Le décryptage de l'information reçue s'effectue au moyen d'une autre clé, la clé privée, qui est gardée secrète et n'est pas transmise[166]. La comparaison la plus éclairante pour comprendre ce système est celle du cadenas: n'importe qui peut le verrouiller et ainsi condamner un coffre, mais seule la personne qui possède la bonne clé peut l'ouvrir[167]. La clé publique et la clé privée ne sont pas dissociables, mais la clé publique ne permet pas de déterminer la clé privée.

Ron Rivest, Adi Shamir et Leonard Adleman ont mis au point un système de cryptage asymétrique appelé RSA. Le résultat de la multiplication de deux très gros nombres premiers est introduit à sens unique dans la clé publique. Cela permet de crypter le texte. Le décryptage n'est possible qu'à condition de connaître la valeur des deux nombres premiers utilisés. Il n'existe cependant aucune méthode mathématique permettant, à partir du résultat de la multiplication de deux nombres premiers, de calculer les nombres premiers d'origine. Pour l'heure, cela n'est possible qu'à force d'essais systématiques. En d'autres termes, le procédé est sûr compte tenu de l'état actuel des connaissances, dès lors que sont retenus des nombres premiers suffisamment élevés. Le seul risque réside dans le fait qu'un jour un mathématicien brillant pourrait trouver le moyen de décomposer les facteurs. Personne à ce jour n'est parvenu à le faire, en dépit d'efforts massifs[168]. Nombreux sont ceux qui affirment au contraire que le problème est impossible à résoudre, mais cela n'a pas encore été prouvé[169].

Rijmen.

166 L'idée du cryptage asymétrique (public–key) est due à Whitfield Diffie et Martin Hellmann.

167 Singh, Geheime Botschaften (1999), 327.

168 Voir à ce sujet Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, 6 ff.

169 Voir Singh, Geheime Botschaften (1999), 335 f.

Par rapport aux procédés symétriques (par exemple DES) le cryptage au moyen d'une clé publique nécessite un délai de calcul beaucoup plus long ou le recours à des machines puissantes et rapides.

11.3.2. Cryptage par public–key pour les particuliers

Afin de rendre le système de public–key accessible à tous, Phil Zimmerman eut l'idée d'associer audit système, très exigeant du point de vue du calcul, un dispositif symétrique plus rapide. L'information est codée au moyen d'un système symétrique – le système IDEA développé à Zurich – cependant que la clé de cryptage symétrique est transmise simultanément grâce au système de public–key. Zimmerman créa un programme convivial – dénommé Pretty Good Privacy – qui créait les clés nécessaires en cliquant et opérait le cryptage. Le programme fut mis sur Internet, ce qui permettait à tout un chacun de le charger. PGP fut finalement racheté par l'entreprise américaine NAI mais toujours mis gratuitement à la disposition des particuliers[170]. Le code d'origine des premières versions a été publié, de sorte que l'on peut considérer qu'il n'y a pas de "porte de derrière". Le code d'origine de la nouvelle version PGP 7, qui se caractérise par un graphisme convivial, n'est malheureusement plus publié.

Il existe toutefois une autre application de la norme ouverte PGP, à savoir GnuPG. Celle-ci offre les mêmes méthodes de cryptage que PGP et est compatible avec PGP. Cependant, il s'agit d'un logiciel dont le code source est connu. Chacun peut l'utiliser et le communiquer. Le ministère fédéral de l'économie et de la technologie a soutenu la possibilité d'importer GnuPG sur Windows ainsi que le développement de l'aspect graphique mais les efforts en ce sens n'ont pas encore abouti. D'après les informations dont dispose le rapporteur, ils se poursuivent.

Il existe des normes concurrentes telles que S/MIME à laquelle adhèrent nombre de programmes de courrier électronique. Le rapporteur ne dispose d'aucune information concernant l'accès libre à ces solutions.

11.3.3. Méthodes à venir

La cryptographie quantique pourrait ouvrir de nouvelles perspectives à la transmission sûre des clés: si la communication de la clé fait l'objet d'une interception, l'opération est détectée. Si l'on envoie des photons polarisés, la polarisation ne peut être constatée sans la modifier. Les intrus peuvent donc être détectés à coup sûr. Seule une clé qui n'a pas été interceptée est donc employée. Lors des essais, des transmissions sur 48 km de fibres optiques et sur 500 mètres dans l'atmosphère ont été couronnées de succès[171].

11.4 Sécurité des produits de cryptage

Dans le débat sur la sécurité réelle du cryptage, est sans cesse soulevé le problème que le produits américains comportent des "portes dérobées" (backdoors). Excel, par exemple, a fait la une des journaux: il a été avancé que dans la version européenne, la moitié de la clé

---

170 Pour des informations sur le logiciel: voir www.pgpi.com.

171 171 Voir Wobst , Abenteuer Kryptographie^2 (1998), 234 ff.

apparaissait en clair dans le header. Microsoft a également attiré l'attention de la presse car un hacker a trouvé une clé NSA dans le programme, ce que Microsoft dément évidemment avec la dernière énergie. Étant donné que Microsoft n'a pas publié son code source, porter un jugement sur la question relève de la spéculation. En ce qui concerne les versions antérieures de PGP et de GnuPG, on peut exclure la présence d'une telle "backdoor" étant donné que le code source a été publié.

11.5 Cryptage et intérêts nationaux

11.5.1. Tentatives de limitation du cryptage

Certains pays interdisent l'utilisation de logiciels de cryptage ou d'appareils de cryptage et soumettent les dérogations à autorisation. Il s'agit notamment, mais pas seulement, de dictatures comme la Chine, l'Iran ou l'Irak. Les pays démocratiques aussi ont limité par la voie législative l'utilisation ou la vente de programmes ou de machines de cryptage. Les communications doivent être protégées des intrusions de particuliers mais l'État doit conserver la possibilité de procéder le cas échéant à des écoutes en toute légalité. La perte de supériorité technique des autorités doit être compensée par des interdictions juridiques. C'est ainsi que la France a frappé d'une interdiction générale l'utilisation de la cryptographie, la subordonnant à autorisation au cas par cas. En Allemagne, il y a eu débat voici quelques années sur la limitation du cryptage. Les États-Unis quant à eux ont limité la longueur des clés.

11.5.2. Importance d'un cryptage sûr pour le commerce électronique

Aujourd'hui, ces tentatives ont peut-être échoué définitivement. Au souci de l'État d'accéder au décryptage et, partant, aux textes en clair, s'opposent non seulement le droit au respect de la vie privée mais aussi des intérêts économiques concrets. En effet, le commerce et la banque électronique sont tributaires de communications sûres sur Internet. Si cela ne peut être garanti, ces formules sont vouées à l'échec car la confiance du client n'est plus assurée. Ce lien explique la mutation de la politique américano–française en matière de cryptage.

Il convient de faire observer ici que le commerce électronique a besoin de méthodes de cryptage sûres pour deux raisons: il faut non seulement crypter l'information, mais aussi pouvoir établir avec certitude l'identité du partenaire. La signature électronique peut passer par l'application inverse du procédé de public–key: la clé privée est utilisée pour crypter, la clé publique pour décrypter. Cette forme de cryptage confirme l'authenticité de la signature. Il est possible de se convaincre de l'identité d'une personne en utilisant la clé publique, mais la signature ne peut être imitée. PGP offre également cette fonction.

11.5.3. Problème des hommes d'affaires en déplacement

Dans de nombreux pays, l'utilisation de programmes de cryptage sur ordinateur portable est interdite aux hommes d'affaires en déplacement. Cela fait obstacle à toute protection des communications avec l'entreprise ou à la protection des données emportées contre les interceptions.

11.6. Problèmes pratiques du cryptage

S'agissant du problème des personnes qui peuvent avoir accès au cryptage, il semble opportun d'établir une distinction entre particuliers et entreprises.

Pour ce qui est des particuliers, il faut souligner que le cryptage de fax ou de conversations téléphoniques par cryptotéléphone ou fax crypté n'est pas faisable, notamment parce que les frais d'acquisition de ces dispositifs sont relativement élevés, mais aussi parce que leur utilisation suppose que le partenaire dispose du même équipement, ce qui n'est que très rarement le cas.

Le courrier électronique doit pouvoir être crypté par tout un chacun. À l'affirmation selon laquelle il n'y a pas de secret et, partant, rien à crypter, on peut répondre que les informations écrites ne sont normalement pas envoyées sur carte postale. Un courrier électronique non crypté n'est rien d'autre qu'une lettre sans enveloppe. Le cryptage du courrier électronique est sûr et ne pose pas de problème. Sur Internet, on trouve déjà des systèmes conviviaux tels que PGP/GnuPG, qui sont même mis gratuitement à la disposition des particuliers. Malheureusement, ils ne sont pas encore répandus. Il serait souhaitable que les pouvoirs publics montrent l'exemple et fassent du cryptage la règle afin de le démythifier.

En ce qui concerne les entreprises, il est indispensable que des informations sensibles ne soient transmises que grâce à des moyens de communication sûrs. Cela paraît évident, notamment pour les grandes entreprises, mais aussi pour les petites et les moyennes qui transmettent souvent par e-mail, sans cryptage, des informations internes et ce parce qu'elles ne sont pas suffisamment sensibilisées au problème. Il est à espérer que les associations professionnelles et les chambres économiques redoubleront leurs efforts d'information. Certes, le cryptage du courrier électronique n'est qu'un aspect de sécurité parmi de nombreux autres et il ne sert à rien lorsque l'information est accessible à des tiers avant d'avoir été cryptée. En d'autres termes, il faut sécuriser l'ensemble de l'environnement de travail afin d'assurer la sécurité des locaux et de contrôler l'accès physique aux bureaux et aux ordinateurs. Il faut aussi empêcher au moyen de fire-walls l'accès non autorisé à l'information via le réseau. L'interconnexion du réseau interne et d'Internet constitue un danger particulier. Dès lors que l'on se soucie de sécurité, il importe de n'utiliser que des systèmes dont le code source est public et a été vérifié. C'est la seule manière d'être certain de ce qu'il advient des données. Les entreprises ont donc beaucoup à faire dans le domaine de la sécurité. Sont déjà présentes sur le marché de nombreuses sociétés qui offrent des conseils et des services de sécurité à des prix raisonnables. L'offre suit la demande en hausse. Par ailleurs, il est à espérer que les associations professionnelles et les chambres économiques vont s'atteler à ce problème afin d'y sensibiliser les petites entreprises et de les aider à définir et à mettre en place un schéma global de protection.

12. Relations extérieures de l'UE et collecte de renseignements

12.1. Introduction

L'adoption du traité de Maastricht en 1991 a marqué la mise en place de la politique étrangère et de sécurité commune (PESC), nouvel instrument politique de l'Union européenne. Six ans plus tard, le traité d'Amsterdam étoffait la structure de la PESC et créait la possibilité d'initiatives de défense commune au sein de l'Union, sans préjudice des alliances existantes. Sur la base du traité d'Amsterdam et compte tenu de l'expérience du Kosovo, le Conseil européen de décembre 1999 (Helsinki) a lancé l'initiative de sécurité et de défense européenne. Cette initiative vise la création d'une force multinationale de 50 à 60 000 hommes pour la deuxième moitié de 2003. L'existence de cette force multinationale rendra inévitable la mise en place d'une capacité autonome en matière de renseignements. La simple intégration de celle de l'UEO serait insuffisante. Un renforcement de la coopération entre les services de renseignements des États membres allant bien au-delà de ce qui se fait actuellement, est inévitable.

Toutefois, le développement de la PESC n'est pas le seul élément qui devrait aboutir au renforcement de la coopération entre les services de renseignements de l'Union. Les progrès de l'intégration économique eux aussi rendent cette démarche nécessaire. Une politique économique commune suppose une perception commune de la réalité économique à l'extérieur de l'Union. Une position commune dans les négociations commerciales menées au sein de l'OMC ou avec les pays tiers suppose une protection commune. Des entreprises fortes en Europe supposent une protection commune contre l'espionnage économique venant de l'extérieur.

Enfin, il convient de souligner que le développement du deuxième pilier et des activités de l'Union dans le domaine de la justice et des affaires intérieures doit également déboucher sur un renforcement de la coopération entre les services de renseignements. La lutte contre le terrorisme, contre le trafic illicite d'armes, contre le trafic d'êtres humains et contre le blanchiment de l'argent ne peut se faire sans une coopération poussée entre les services de renseignements.

12.2. Possibilités de coopération au sein de l'UE

12.2.1. La coopération actuelle

Il est de tradition depuis longtemps que les services de renseignements ne se fient qu'aux informations qu'ils recueillent eux–mêmes et qu'ils se méfient de leurs homologues. Il n'empêche que la coopération entre ces services se renforce progressivement. Des contacts fréquents ont lieu dans le cadre de l'OTAN, de l'UEO et de l'Union européenne. Si les services de renseignements de l'OTAN restent largement tributaires de l'apport considérable des États-Unis, la création du centre de satellites de l'UEO à Torrejon (Espagne) et celle d'une section de renseignements au niveau du quartier général de l'UEO ont contribué à rendre l'Europe autonome dans ce domaine.

12.2.2. Avantages d'une politique commune dans le domaine du renseignement

Abstraction faite de l'évolution qui s'opère, il faut souligner les avantages que présenterait une politique commune en matière de renseignement.

12.2.2.1. Avantages professionnels

Premièrement, les informations secrètes ou non à collecter, à analyser et à évaluer sont trop nombreuses pour un seul organisme ou pour faire l'objet d'accords bilatéraux en Europe occidentale. Les activités des services de renseignements englobent la défense, les politiques économiques nationales et internationales, la lutte contre la criminalité et le trafic de la drogue. Même si elle n'existait qu'au niveau élémentaire, par exemple pour la collecte des renseignements (OSINT), la coopération donnerait des résultats d'une grande importance sous l'angle des politiques de l'Union.

12.2.2.2. Avantages budgétaires

Dans le passé récent, les budgets du renseignement ont fait l'objet de coupes sombres, démarche qui, dans certains cas, se poursuit. Simultanément, la demande d'informations a grandi. Il s'ensuit que la coopération serait non seulement possible, mais, à court terme, avantageuse. Elle serait intéressante notamment pour la mise en place et l'entretien d'infrastructures techniques ainsi que dans le domaine de l'évaluation des renseignements recueillis. La coopération accroîtrait l'efficacité de la collecte.

12.2.2.3. Avantages politiques

En principe, les renseignements recueillis sont utilisés pour permettre aux gouvernements de prendre des décisions mieux fondées. L'intégration politique et économique de l'Union suppose que les renseignements soient accessibles au niveau européen, ce qui nécessite plus d'une source.

12.2.3. Remarques finales

Ces avantages objectifs illustrent l'importance croissante de la coopération au sein de l'Union. Les États nations d'hier assuraient chacun de leur côté leur sécurité extérieure, l'ordre public intérieur, la prospérité nationale et l'identité culturelle. Aujourd'hui, l'Union européenne prend peu à peu un rôle qui est complémentaire à celui des États nations. Il est exclu que les services de renseignements soient le dernier ou le seul domaine à ne pas être touché par l'intégration européenne.

12.3. Coopération au–delà de l'Union

Depuis la deuxième guerre mondiale, la coopération dans le domaine de la collecte du renseignement s'est faite non au niveau européen mais au niveau transatlantique. Il est déjà apparu que des relations très étroites en matière de collecte de renseignements avaient été établies entre le Royaume–Uni et les États–Unis. Dans le domaine de la défense et dans le

cadre de l'OTAN et au–delà de celui–ci, les États–Unis étaient et restent le partenaire dominant. La grande question est de savoir si le développement de la coopération européenne dans le domaine de la collecte de renseignements perturbera les relations avec les États–Unis ou entraînera le renforcement de ces relations. Comment les relations entre l'UE et les États–Unis évolueront–elles sous l'administration Bush? Comment les relations particulières entre les États-Unis et le Royaume-Uni se maintiendront-elles dans ce contexte?

D'aucuns estiment qu'il n'y a pas nécessairement contradiction entre les relations États-Unis Royaume-Uni et l'évolution de la PESC. D'autres sont d'avis que le problème de la collecte de renseignements peut être celui qui amènera le Royaume–Uni à déterminer si sa destinée est européenne ou transatlantique. Les liens étroits entre le Royaume–Uni et les États–Unis (et les autres parties à l'accord UK/USA) pourraient rendre plus difficile le partage de renseignements entre les autres États de l'Union, le Royaume–Uni se montrant peut être moins enclin à partager l'information à l'intérieur de l'Europe et les partenaires de l'UE se montrant moins confiants à l'égard du Royaume-Uni. De la même manière, si les États–Unis estiment que le Royaume–Uni a développé des liens spéciaux avec ses partenaires de l'UE, ils pourraient hésiter à partager l'information avec le Royaume-Uni. La coopération dans le domaine du renseignement peut donc constituer une pierre de touche des ambitions européennes du Royaume–Uni ainsi que de la capacité d'intégration de l'Union elle–même.

Dans les circonstances actuelles, il est peu vraisemblable que même des progrès rapides de la coopération entre les partenaires européens permettent, à court et même à long terme, de remplacer l'avantage technique des États–Unis. L'Union européenne ne sera pas en mesure de mettre en place un réseau évolué de satellites SIGINT et de stations au sol. L'Union européenne ne sera pas en mesure de mettre en place à court terme le réseau d'ordinateurs nécessaire pour faire le tri et analyser le matériel collecté. L'Union européenne ne sera pas disposée à mobiliser les ressources budgétaires nécessaires pour supplanter les efforts des États–Unis. Du point de vue technique et budgétaire, il est dans l'intérêt de l'Union de maintenir des relations étroites avec les États–Unis dans le domaine de la collecte du renseignement. Du point de vue politique aussi, il importe de maintenir et, au besoin, de renforcer les relations avec les États–Unis, notamment en ce qui concerne la lutte contre la criminalité organisée, le terrorisme, le trafic de drogue et d'armes et le blanchiment de l'argent. Des opérations communes sont nécessaires pour soutenir les efforts communs. Des actions communes en matière de maintien de la paix supposent une contribution accrue de l'Europe dans tous les domaines.

Cela dit, la sensibilisation de l'Europe doit s'accompagner d'une responsabilité accrue. L'Union européenne doit devenir un partenaire à part égale non seulement sur le plan économique, mais aussi dans le domaine de la défense et dans celui de la collecte du renseignement. Des capacités autonomes de l'Europe en matière de renseignements ne devraient pas être considérées comme affaiblissant les relations transatlantiques. Au contraire, elles devraient permettre de renforcer celles-ci en rétablissant l'équilibre et en faisant de l'Union un partenaire plus performant. Parallèlement, l'Union doit s'employer de manière autonome à protéger son économie et ses entreprises contre des menaces telles que l'espionnage économique, la cybercriminalité et les attentats terroristes. Par ailleurs, la compréhension transatlantique est nécessaire dans le domaine de l'espionnage industriel. L'Union européenne et les États-Unis devraient convenir de normes concernant ce qui est autorisé et ce qui ne l'est pas dans ce domaine. Pour renforcer la coopération transatlantique,

une initiative commune devrait être lancée au niveau de l'OMC: il s'agirait d'utiliser les mécanismes de cette organisation pour protéger un développement économique loyal dans le monde.

12.4. Remarques finales

Le développement d'une capacité commune de l'Union européenne en matière de renseignements doit être considéré comme nécessaire et inévitable, non sans maintenir l'indispensable protection de la vie privée des citoyens européens. La coopération avec les pays tiers, en particulier les États-Unis, doit être maintenue et si possible renforcée. Cela ne signifie pas nécessairement que les activités SIGINT de l'Europe doivent automatiquement être intégrées dans un système ECHELON indépendant pour l'Union européenne ou que l'Union doit devenir partenaire à part entière de l'accord UK/USA. Toutefois, l'exercice d'une responsabilité proprement européenne dans le domaine de la collecte du renseignement doit être sérieusement envisagé. Une capacité européenne intégrée dans ce domaine suppose un système de contrôle politique concernant ces activités. Des décisions devront être prises sur les moyens d'analyser les renseignements et de prendre les décisions politiques découlant de l'analyse. Faute d'un tel système de contrôle politique et donc d'une responsabilité politique, le processus de collecte d'informations porterait préjudice au processus d'intégration européenne.

13. Conclusions et recommandations

13.1. Remarque préliminaire

Le présent chapitre regroupe des constats et des conclusions possibles. Il ne saurait être conçu comme définitif. Le rapporteur souhaite plutôt poser les jalons du débat politique à mener en commission. Le texte devra être revu par la suite afin de tenir compte de l'échange de vues.

13.2. Conclusions

Existence d'un système mondial d'interception des communications privées et économiques (système ECHELON)

L'existence d'un système d'écoute des communications fonctionnant, avec la participation des États-Unis, des Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande dans le cadre de l'accord UKUSA, ne fait plus de doute. Il est vraisemblable, eu égard aux indices disponibles, qu'il est dénommé ECHELON, mais cet aspect est d'une importance secondaire. Ce qui compte, c'est qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires.

L'analyse a montré que la puissance de ce système ne peut être aussi grande, tant s'en faut, que ce que certains médias supposent.

Limites du système

Le système de surveillance repose sur l'interception de communications par satellite. Or, dans les régions à forte densité de communications, seule une très modeste partie des communications s'effectue par satellite. Cela signifie que la majeure partie des communications ne peuvent être interceptées par des stations au sol mais uniquement par branchement sur câble ou par écoute radio. Les investigations ont montré que les pays membres d'ECHELON n'ont accès qu'à une partie très restreinte des communications par câble ou par radio. Par ailleurs, il faut un tel effectif qu'une partie seulement des communications peut être analysée.

Existence d'autres systèmes d'écoute

Étant donné que l'écoute des communications est un moyen d'espionnage traditionnel des services de renseignements, un tel système pourrait être exploité par d'autres pays à condition qu'ils disposent des moyens financiers et des conditions géographiques nécessaires. La France serait en mesure, du moins en ce qui concerne les conditions géographiques – elle est en effet le seul État membre de l'UE à posséder des territoires outre mer – de mettre sur pied à elle seule un système d'écoute mondial. Il ressort de certains indices que la Russie pourrait également exploiter un tel système.

Compatibilité avec le droit de l'UE

S'agissant de la compatibilité d'un tel système avec le droit de l'UE, il y a lieu de souligner

que si ledit système n'est utilisé qu'à des fins de renseignements, il n'y a aucune contradiction avec le droit de l'UE dans la mesure où les activités qui relèvent de la sécurité de l'État ne sont pas couvertes par le traité CE. Elles ne relèvent que du titre V du traité UE (PESC), qui ne contient encore aucune disposition en la matière, de sorte qu'une base fait défaut. Si le système est utilisé de manière abusive pour espionner la concurrence, il y a manquement à l'obligation de loyauté et atteinte à l'idée d'un marché commun où la concurrence est libre. Si un État membre participe à une telle démarche, il viole le droit de l'Union.

Compatibilité avec le droit fondamental au respect de la vie privée (article 8 de la convention des droits de l'homme)

Toute écoute de communication constitue une atteinte grave à la vie privée de la personne. L'article 8 de la convention des droits de l'homme, qui protège la vie privée, n'autorise des atteintes à celle–ci que pour préserver la sécurité nationale, à condition que les dispositions du droit national les prévoient et soient accessibles à tous. Il faut aussi que soient définies les circonstances et conditions dans lesquelles les pouvoirs publics peuvent y recourir. Ces atteintes doivent être proportionnées et il doit donc y avoir mise en balance des intérêts en jeu. Il ne suffit pas que l'intervention soit opportune ou souhaitable.

Un système de renseignements qui intercepterait les communications sans garantir le respect du principe de proportionnalité serait contraire à la convention. De la même manière, il y aurait violation de la convention si les dispositions en vertu desquelles la surveillance est opérée étaient dépourvues de fondement juridique, si celui–ci n'était pas accessible à tous ou s'il était formulé de telle manière que l'individu ne puisse percevoir ses conséquences. Étant donné que les dispositions sur la base desquelles les services de renseignements américains opèrent à l'étranger sont en grande partie secrètes, le respect du principe de proportionnalité est à tout le moins sujet à caution. Il n'en reste pas moins qu'il y a violation des principes d'accès au droit et de prévisibilité de ses effets. Même si les États-Unis ne sont pas partie à la Convention relative aux droits de l'homme, les États membres doivent respecter celle-ci. Ils ne peuvent se soustraire aux obligations qu'elle leur impose en autorisant les services de renseignements d'autres pays soumis à des dispositions moins rigoureuses à opérer sur leur territoire. Autrement, le principe de l'égalité et ses deux composantes – accès et prévisibilité – serait privé de ses effets et la jurisprudence de la Cour des droits de l'homme serait vidée de sa substance. Il est essentiel pour les citoyens européens que les parlements nationaux disposent d'organes de contrôle spécifiques dûment structurés pour surveiller les activités des services de renseignement.

La conformité aux droits fondamentaux d'une activité légale d'un service de renseignements suppose en outre que des dispositifs de contrôle suffisants soient prévus afin de parer aux risques inhérents à l'action secrète d'une partie de l'appareil administratif. Considérant que la Cour des droits de l'homme a souligné l'importance d'un système de contrôle efficace dans le domaine des activités de renseignements, il apparaît préoccupant que certains États membres ne disposent pas d'organes de contrôle parlementaires des services secrets.

Les citoyens de l'UE sont–ils suffisamment protégés des services de renseignements?

Étant donné que la protection des citoyens de l'UE dépend des situations juridiques qui existent dans les États membres, lesquelles sont très différentes, et dans certains cas

caractérisées par l'absence d'organes de contrôle parlementaires, on ne peut guère parler de protection suffisante. Même la où des organes de contrôle existent, la tentation est forte de s'intéresser davantage aux activités des services de renseignements intérieurs qu'aux activités extérieures étant donné que normalement les citoyens du pays ne sont concernés que dans le premier cas.

En cas de coopération entre services de renseignements dans le cadre de la PESC, les institutions sont invitées à mettre en place des dispositions de protection suffisantes pour les citoyens européens.

Espionnage économique

Il relève des missions des services de renseignements à l'étranger de s'intéresser aux données économiques tels que développement de branches, évolution des marchés des matières premières, respect d'embargos, respect des dispositions relatives à l'approvisionnement en biens à usage mixte, etc.. C'est la raison pour laquelle les entreprises exerçant des activités dans ces domaines sont généralement surveillées. La situation devient intolérable dès lors que des services de renseignements sont utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales. Il est avancé mais non prouvé que le système d'interception mondial est utilisé à cette fin.

En fait, les données sensibles se trouvent principalement à l'intérieur des entreprises de sorte que l'espionnage consiste principalement à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées ou encore en pénétrant dans les réseaux informatiques. Ce n'est que lorsque les données sensibles sont acheminées vers l'extérieur par câble ou par radio (satellite) qu'un système de surveillances des communications peut être utilisé pour espionner. Trois cas se présentent:

- entreprises travaillant dans trois zones horaire, de sorte que les résultats intérimaires peuvent être envoyés d'Europe en Amérique puis en Asie;
- vidéoconférences d'entreprises multinationales se déroulant par satellite ou par câble;
- négociations de marchés importants sur place (construction d'usines, infrastructures de télécommunications, construction de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place.

Possibilités de protection

Les entreprises doivent protéger tout leur environnement de travail c'est–à–dire aussi les moyens de communication servant à transmettre des informations sensibles. Les systèmes de cryptage sûrs à prix abordable sont suffisamment nombreux sur le marché européen. Les particuliers doivent eux aussi être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe. Sur Internet, on trouve des systèmes conviviaux qui sont mis à la disposition des particuliers, parfois même gratuitement.

Coopération entre services de renseignements de l'UE

L'UE est convenue de coordonner la collecte du renseignement dans le cadre du développement de sa politique de sécurité et de défense, non sans poursuivre la coopération avec d'autres partenaires dans ces domaines.Une coopération entre services de renseignements

de l'UE apparaît souhaitable car, d'une part, une politique commune de sécurité excluant les services secrets serait absurde et, d'autre part, cela comporterait de nombreux avantages d'ordre professionnel, financier et politique. Cela serait en outre conforme à l'idée d'un partenariat à égalité de droits avec les États–Unis et pourrait regrouper l'ensemble des États membres au sein d'un système mis sur pied dans le respect de la convention des droits de l'homme. Un contrôle par le Parlement européen devrait dans ce cas être assuré. Le Parlement européen est sur le point d'adopter des dispositions relatives à l'accès aux informations et documents confidentiels et sensibles.

13.3. Recommandations

Lutte contre l'espionnage économique

en ce qui concerne la conclusion et modification de conventions relatives à la protection des citoyens et des entreprises

1. le Secrétaire général du Conseil de l'Europe est invité à proposer au comité des ministres de déterminer s'il serait opportun d'adapter la protection de la vie privé garantie à l'article 8 de la Convention relative aux droits de l'homme aux méthodes de communication et aux possibilités d'interception modernes, et ce dans un protocole additionnel ou dans le contexte de la réglementation relative à la protection des données, dans le cadre d'une révision de la Convention afférente, étant entendu que cela ne saurait déboucher sur un abaissement du niveau de protection assuré par la Cour des droits de l'homme ni sur une réduction de la souplesse nécessaire pour suivre l'évolution;

2. les États membres sont invités à mettre en place une plateforme européenne appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications, à se mettre d'accord sur un texte commun garantissant la protection de la vie privée, telle qu'elle est définie à l'article 7 de la Charte européenne des droits fondamentaux, à tous les citoyens européens sur le territoire des États membres et garantissant en outre que les activités des services de renseignements s'effectuent dans le respect des droits fondamentaux et, partant, des conditions énoncées au chapitre 8 du rapport, en particulier du point 8.3.4, en vertu de l'article 8 de la Convention relative aux droits de l'homme;

3. les États membres du Conseil de l'Europe sont invités à adopter un protocole additionnel permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme ou d'envisager d'autres moyens d'éviter les conflits de jurisprudence entre la Cour européenne des droits de l'homme et la Cour de justice européenne;

4. le Secrétaire général des Nations unies est invité à charger l'organe compétent de l'Organisation de présenter des propositions visant à adapter l'article 17 de la Convention internationale relative aux droits civils et politiques, qui garantit la protection de la vie privée, aux innovations techniques;

5. les États-Unis sont invités à signer le protocole additionnel à la Convention internationale relative aux droits civils et politiques afin de rendre possibles, en cas de violation, les

recours individuels devant la commission des droits de l'homme prévue par la Convention; invite les ONG américaines compétentes, notamment l'ACLU (American Civil Liberties Union) et l'EPIC (Electronic Privacy Information Center) à faire pression en ce sens sur le gouvernement américain;

en ce qui concerne l'action législative nationale en matière de protection des citoyens et des entreprises

6. les États membres sont invités à vérifier la conformité aux droits fondamentaux de leur législation relative aux activités des services de renseignements;

7. les États membres sont invités à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements en fonction du niveau de protection national le plus élevé, les citoyens concernés par les activités d'un service de renseignements étranger appartenant généralement à un autre pays, c'est-à-dire aussi à un autre État membre;

8. les institutions de l'UE sont invitées, en cas de coopération entre services de renseignements dans le cadre de la PESC, à prévoir des garanties suffisantes pour les citoyens européens; le Parlement européen, organe de contrôle tout indiqué, doit, d'une part, créer les conditions nécessaires à la surveillance de ce domaine très sensible pour qu'il soit réaliste et responsable de réclamer les pouvoirs de contrôle nécessaires;

en ce qui concerne les mesures de lutte contre l'espionnage économique

9. les États membres sont invités à examiner si des dispositions du droit européen et international permettraient de lutter contre l'espionnage économique et la corruption visant à obtenir des marchés, notamment si une réglementation dans le cadre de l'OMC serait possible, qui tiendrait compte des distorsions de concurrence causées par de telles pratiques, par exemple en prévoyant la nullité de tels marchés;

10. les États membres sont invités à s'engager, dans une déclaration commune, à ne pas pratiquer l'espionnage économique entre eux, proclamant ainsi le respect de l'esprit et de la lettre du traité CE;

en ce qui concerne l'application du droit et le contrôle de celle-ci

11. les parlements nationaux qui ne disposent pas d'organe de contrôle parlementaire des services de renseignements sont invités à se doter d'un tel organe;

12. les organes de contrôle nationaux des services secrets sont invités à accorder une grande importance, dans l'exercice de leur pouvoir de contrôle, à la protection de la vie privée, que la surveillance concerne les ressortissants nationaux, les citoyens d'autres États membres de l'UE ou ceux de pays tiers;

13. les services de renseignements des États membres sont invités à ne se faire communiquer des informations par d'autres services de renseignements que lorsque celles-ci ont été obtenues dans des conditions prévues par le droit national, les États membres ne pouvant se soustraire aux obligations que leur impose la convention relative aux droits de

l'homme en faisant intervenir des services de renseignements étrangers;

14. l'Allemagne et le Royaume-Uni sont invités à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité, que la base juridique soit accessible et que les effets soient prévisibles pour les personnes et qu'un contrôle efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire;

en ce qui concerne la promotion de la protection des citoyens et des entreprises

15. la Commission et les États membres sont invités à élaborer des programmes de sensibilisation des citoyens et des entreprises aux problèmes de sécurité et, simultanément, à offrir une aide pratique pour la conception et la mise en œuvre de formules de protection globale;

16. la Commission et les États membres sont invités à élaborer des mesures de promotion, de développement et de fabrication de matériels et de logiciels de cryptage européens et surtout à soutenir les projets visant à développer des logiciels de cryptage conviviaux dont le texte-source soit publié;

17. la Commission et les États membres sont invités à promouvoir des projets de logiciels dont le texte-source soit publié, étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de "backdoors" ("open-source software");

18. les institutions européennes et les administrations publiques des États membres sont invitées à recourir systématiquement au cryptage du courrier électronique afin de faire de celui-ci la règle, à terme;

en ce qui concerne d'autres démarches

19. les entreprises sont invitées à coopérer davantage avec les services de contre-espionnage, à leur signaler les attaques extérieures relevant de l'espionnage économique, afin d'accroître leur efficacité;

20. la Commission est invitée à proposer la création d'un service de conseil européen en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;

21. le Parlement européen est invité à organiser un colloque non limité à l'Union sur la protection de la vie privée face à la surveillance des télécommunications afin de créer une plateforme permettant aux ONG d'Europe, des États-Unis et d'autres pays d'examiner les aspects transfrontaliers et internationaux et de coordonner les activités et démarches;