

PARLEMENT EUROPÉEN

1999



2004

Document de séance

FINAL
A5-0264/2001
Partie 1

11 juillet 2001

RAPPORT

sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))

Partie 1 Proposition de résolution
 Exposé des motifs

Commission temporaire sur le système d'interception ECHELON

Rapporteur: Gerhard Schmid

"Sed quis custodiet ipsos custodes."

Juvenal (v. 60 – v. 130), Sat. 6, 347

SOMMAIRE

	Page
PAGE RÉGLEMENTAIRE.....	11
PROPOSITION DE RÉOLUTION.....	12
EXPOSÉ DES MOTIFS.....	23
1. Introduction.....	23
1.1. Motif de la constitution de la commission.....	23
1.2. Affirmations formulées dans les deux études du STOA sur un système d'interception mondial appelé ECHELON.....	23
1.2.1. Premier rapport du STOA de 1997.....	23
1.2.2. Rapports du STOA de 1999.....	23
1.3. Mandat de la Commission.....	24
1.4. Pourquoi n'avoir pas opté pour une commission d'enquête?.....	25
1.5. Méthodes et plan de travail	25
1.6. Caractéristiques attribuées au système ECHELON.....	26
2. Activité des services de renseignements extérieurs.....	28
2.1. Introduction.....	28
2.2. Que faut-il entendre par espionnage?.....	28
2.3. Objectifs de l'espionnage.....	28
2.4. Méthodes de l'espionnage.....	29
2.4.1. Recours à l'être humain dans l'espionnage.....	29
2.4.2. Exploitation des signaux électromagnétiques.....	30
2.5. Activité de certains services de renseignements.....	30
3. Conditions techniques minimales requises pour l'interception des télécommunications.....	32
3.1. Possibilité d'interception des différents supports des télécommunications.....	32
3.2. Possibilités d'interception sur place.....	32
3.3. Possibilités d'un système d'interception fonctionnant à l'échelle mondiale.....	33
3.3.1. Accès aux supports des télécommunications.....	33
3.3.2. Possibilités d'exploitation automatique des communications interceptées: utilisation de filtres.....	37
3.3.3. Exemple du service de renseignements allemand.....	38
4. Technique des communications satellitaires.....	40

4.1. Importance des satellites de télécommunications.....	40
4.2. Fonctionnement d'une liaison satellitaire.....	41
4.2.1. Satellites géostationnaires.....	41
4.2.2. Cheminement d'une liaison satellitaire de télécommunications.....	41
4.2.3. Principaux systèmes de communications satellitaires existants.....	42
4.2.3.1. Systèmes de satellites fonctionnant à l'échelle mondiale.....	43
4.2.3.2. Systèmes de satellites nationaux.....	45
4.2.3.3. Systèmes de satellites régionaux.....	46
4.2.4. Attribution de fréquences.....	46
4.2.5. Zones couvertes par les satellites (empreintes au sol).....	47
4.2.6. Dimensions des antennes requises pour une station terrienne.....	48
4.3. Communications par satellites à finalités militaires.....	49
4.3.1. Généralités.....	49
4.3.2. Fréquences utilisées par les militaires.....	49
4.3.3. Taille des stations de réception.....	49
4.3.4. Exemples.....	49
5. Preuve par indices de l'existence d'au moins un système d'interception mondial.....	50
5.1. Pourquoi une preuve par indices.....	50
5.1.1. Preuve de l'activité d'interception des services de renseignements étrangers....	50
5.1.2. Preuve de l'existence de stations dans les zones géographiques requises.....	51
5.1.3. Preuve d'une association étroite entre les services de renseignement.....	51
5.2. Comment reconnaît-on une station d'interception des communications par satellite?.....	51
5.2.1. Critère 1: accès de l'installation.....	51
5.2.2. Critère 2: type d'antenne.....	52
5.2.3. Critère 3: dimension de l'antenne.....	52
5.2.4. Critères 4: Preuves officielles.....	53
5.3. Données pouvant être obtenues par chacun, concernant les stations d'interception connues.....	53
5.3.1. Méthode.....	53
5.3.2. Analyse approfondie.....	54
5.3.2.1. Le parallélisme entre le développement des INTELSAT et la construction de stations.....	54
5.3.2.2. La couverture globale par stations qui écoutent manifestement des satellites de communication.....	57
5.3.2.3. Les stations: détails.....	58
5.3.2.3.1. Stations destinées à l'écoute de satellites de communication.....	58
5.3.2.3.2. Autres stations.....	61
5.3.3. Résultats: résumé.....	63
5.4. L'accord UKUSA.....	64
5.4.1. Genèse de l'accord UKUSA.....	64
5.4.2. Éléments attestant de l'existence de l'accord.....	65
5.4.2.1. Rapport annuel 1999/2000 de la commission britannique du	

renseignement et de la sécurité.....	65
5.4.2.2. Informations fournies par les services du Premier Ministre de Nouvelle- Zélande.....	66
5.4.2.3. Liste des acronymes utilisés par la Navy.....	66
5.4.2.4. Déclaration du directeur du DSD.....	66
5.4.2.5. Rapport du Canadian Parliamentary Security and Intelligence Committee.....	66
5.4.2.6. Déclaration de M. Louis Torella, ancien directeur adjoint de la NSA..	66
5.4.2.7. Lettre de M. Joe Hooper, ancien directeur du GCHQ.....	67
5.4.2.8. Interlocuteurs du rapporteur.....	67
5.5. Exploitation des documents américains ayant cessé d'être classés confidentiels.....	67
5.5.1. Nature des documents.....	67
5.5.2. Contenu des documents.....	67
5.5.2.1. Mission et conception de la NSA (documents 1, 2b, 4, 10 et 16).....	68
5.5.2.2. Pouvoirs des services de renseignement (document 7).....	69
5.5.2.3. Coopération avec d'autres services (documents 2 a et 2 b).....	69
5.5.2.4. Mention des unités actives sur les "sites ECHELON" (documents 9 et 12).....	69
5.5.2.5. Mention de stations (documents 6, 9 et 12, nouveaux documents).....	69
5.5.2.6. Protection de la vie privée des citoyens américains (documents 7, 7 a à f, 9, 11 et 16).....	70
5.5.2.7. Définitions (documents 4, 5 a et 7).....	71
5.5.3. Résumé.....	71
5.6. Renseignements émanant d'auteurs spécialisés et de journalistes.....	72
Nicky Hager.....	72
Duncan Campbell.....	73
Jeff Richelson.....	74
James Bamford.....	75
Bo Elkjaer et Kenan Seeberg.....	76
5.7. Déclarations d'anciens collaborateurs des services de renseignement.....	76
5.7.1. Margaret Newsham (ex-collaboratrice de la NSA).....	76
5.7.2. Wayne Madsen (ancien collaborateur de la NSA).....	77
5.7.3. Mike Frost (ancien collaborateur des services secrets canadiens).....	77
5.7.4. Fred Stock (ancien collaborateur des services secrets canadiens).....	78
5.8. Informations de sources gouvernementales.....	78
5.8.1. Déclarations américaines.....	78
5.8.2. Déclarations anglaises.....	79
5.8.3. Déclarations australiennes.....	79
5.8.4. Déclarations néo-zélandaises.....	80
5.8.5. Déclarations néerlandaises.....	80
5.8.6. Déclarations italiennes.....	80
5.9. Questions au Conseil et à la Commission.....	80
5.10. Rapports parlementaires.....	82
5.10.1. Rapports du comité permanent R de contrôle belge.....	82
5.10.2. Rapport de la commission de la défense nationale de l'Assemblée nationale française.....	82
5.10.3. Rapport de la commission du Parlement italien chargée des services de	

renseignements et de sécurité ainsi que de la sûreté de l'État.....	83
6. Peut-il exister d'autres systèmes d'interception mondiaux?.....	84
6.1. Conditions nécessaires pour un tel système	84
6.1.1. Conditions technico-géographiques.....	84
6.1.2. Conditions politico-économiques.....	84
6.2. France.....	84
6.3. Russie.....	85
6.4. Autres pays du G8 et Chine.....	86
7. Compatibilité d'un système d'interception des communications du type "ECHELON" avec le droit de l'Union européenne.....	87
7.1. Commentaires sur la question.....	87
7.2. Compatibilité d'un système de renseignement avec le droit de l'Union européenne...	87
7.2.1. Compatibilité avec le droit communautaire.....	87
7.2.2. Compatibilité avec d'autres dispositions législatives de l'Union européenne..	88
7.3. Problème de la compatibilité en cas d'utilisation du système aux fins de l'espionnage économique.....	89
7.4. Conclusions.....	90
8. La surveillance des communications par les services de renseignement est-elle compatible avec le droit fondamental au respect de la vie privée.....	91
8.1. La surveillance des communications, atteinte au droit fondamental au respect de la vie privée.....	91
8.2. La protection de la vie privée garantie par les conventions internationales.....	91
8.3. Les dispositions de la convention européenne des droits de l'homme.....	92
8.3.1. L'importance de la convention dans l'UE.....	92
8.3.2. Portée de la protection offerte par la convention.....	93
8.3.3. Surveillance des télécommunications au regard de l'article 8 de la convention	93
8.3.4. Importance de l'article 8 de la convention sous l'angle des activités des services de renseignements.....	94
8.4. Obligation de vigilance vis-à-vis des activités de services de renseignements étrangers.....	96
8.4.1. Caractère inadmissible d'une violation de l'article 8 de la convention liée à l'intervention de services de renseignements étrangers.....	96
8.4.2. Conséquences sous l'angle des activités de services de renseignements extra-européens sur le territoire de pays signataires de la convention.....	96
8.4.2.1. Jurisprudence de la Cour européenne des droits de l'homme.....	96
8.4.2.2. Conséquences en ce qui concerne les stations.....	97
8.4.2.3. Conséquences en ce qui concerne les écoutes pratiquées sur instructions de l'étranger.....	97
8.4.2.4. Obligation de vigilance par rapport aux pays tiers.....	97

9. Les citoyens de l'UE sont-ils suffisamment protégés face aux activités des services de renseignements?	99
9.1. Protection face aux activités des services de renseignements: rôle des parlements nationaux.....	99
9.2. Pouvoirs des autorités nationales en matière de mesures de surveillance.....	99
9.3. Les contrôles des services de renseignements.....	100
9.4. Analyse de la situation du citoyen européen.....	103
10. Protection contre l'espionnage économique	105
10.1. Économie et espionnage.....	105
10.1.1. Les objectifs de l'espionnage.....	105
10.1.1.1. Branches.....	105
10.1.1.2. Départements d'entreprise.....	105
10.1.2. Espionnage de concurrence.....	106
10.2. Les préjudices causés par l'espionnage.....	106
10.3. Qui espionne?.....	107
10.3.1. Collaborateurs de l'entreprise (délict d'initié).....	107
10.3.2. Officines spécialisées.....	108
10.3.3. Hackers.....	108
10.3.4. Services de renseignements.....	108
10.4. Comment espionne-t-on?.....	108
10.5. Espionnage économique d'État.....	109
10.5.1. Espionnage économique stratégique effectué par les services de renseignements.....	109
10.5.2. Les services de renseignements, agents de l'espionnage de concurrence... ..	109
10.5.2.1. Pays très avancés sur le plan technologique.....	109
10.5.2.2. Pays moins avancés sur le plan technique.....	109
10.6. ECHELON est-il adapté à l'espionnage industriel?.....	110
10.7. Cas divulgués.....	110
10.8. Protection contre l'espionnage économique.....	116
10.8.1. Protection juridique.....	116
10.8.2. Autres entraves à l'espionnage économique.....	116
10.9. Les États-Unis et l'économie après la guerre froide.....	117
10.9.1. Le défi lancé au gouvernement américain: l'espionnage économique contre les entreprises américaines.....	118
10.9.1.1. Les acteurs.....	119
10.9.1.2. Objectifs de l'espionnage économique.....	119
10.9.1.3. Méthodes.....	120
10.9.2. Attitude du gouvernement américain face à l'espionnage économique actif.....	120
10.9.3. Situation juridique en matière de corruption d'agents publics.....	121
10.9.4. Rôle de l'Advocacy Center dans la promotion des exportations américaines.....	123
10.9.4.1. Missions de l'Advocacy Center.....	123
10.9.4.2. Méthodes de travail.....	124
10.9.4.3. Participation de la CIA aux travaux du TPCC.....	124

10.9.4.4. Questions sans réponse.....	125
10.10. Sécurité des réseaux informatiques.....	125
10.10.1. Importance du présent chapitre.....	125
10.10.2. Risque inhérent à l'utilisation de la technologie de l'information moderne dans les milieux économiques.....	125
10.10.2.1. Augmentation du risque.....	126
10.10.2.2. Analyse détaillée de certains des risques.....	126
10.10.3. Fréquence des attaques contre les réseaux.....	127
10.10.4. Acteurs et méthodes.....	128
10.10.5. Piratage de l'extérieur.....	129
10.11. Sous-estimation des risques.....	129
10.11.1. Conscience des risques dans les milieux économiques.....	129
10.11.2. Conscience du risque dans les milieux scientifiques.....	129
10.11.3. Conscience du risque dans les institutions européennes.....	130
10.11.3.1. Banque centrale européenne.....	130
10.11.3.2. Conseil de l'Union européenne.....	130
10.11.3.3. Parlement européen.....	130
10.11.3.4. Commission européenne.....	131
11. Le cryptage en tant qu'instrument d'autoprotection.....	132
11.1. Objectif et mode de fonctionnement du cryptage.....	132
11.1.1. Objectif du cryptage.....	132
11.1.2. Mode de fonctionnement du cryptage.....	132
11.2. Sécurité des systèmes de cryptage.....	134
11.2.1. Généralités.....	134
11.2.2. Sécurité absolue: one-time pad.....	134
11.2.3. Sécurité relative en fonction de l'état de la technique.....	134
11.2.3.1. Utilisation de machines de cryptage et de décryptage.....	134
11.2.3.2. Utilisation de l'ordinateur.....	135
11.2.4. Normalisation et limites de la sécurité.....	135
11.3. Problème de sécurité en matière de diffusion des clés.....	136
11.3.1. Cryptage asymétrique: procédé de la public-key.....	136
11.3.2. Cryptage par public-key pour les particuliers.....	137
11.3.3. Méthodes à venir.....	138
11.4. Sécurité des produits de cryptage.....	138
11.5. Cryptage et intérêts nationaux.....	138
11.5.1. Tentatives de limitation du cryptage.....	138
11.5.2. Importance d'un cryptage sûr pour le commerce électronique.....	139
11.5.3. Problème des hommes d'affaires en déplacement.....	139
11.6. Problèmes pratiques du cryptage.....	139
12. Relations extérieures de l'UE et collecte de renseignements.....	141
12.1. Introduction.....	141
12.2. Possibilités de coopération au sein de l'UE.....	141
12.2.1. La coopération actuelle.....	141

12.2.2.	Avantages d'une politique commune dans le domaine du renseignement.....	142
	12.2.2.1. Avantages pratiques.....	142
	12.2.2.2. Avantages financiers.....	142
	12.2.2.3. Avantages politiques.....	142
12.2.3.	Remarques finales.....	142
12.3.	Coopération au-delà de l'Union.....	143
12.4.	Remarques finales.....	144
13.	Conclusions et recommandations.....	145
13.1.	Conclusions.....	145
13.2.	Recommandations.....	149

L'OPINION MINORITAIRE ET LES ANNEXES SONT PUBLIÉES SÉPARÉMENT DANS
LA PARTIE 2

PAGE RÉGLEMENTAIRE

Au cours de sa séance du 5 juillet 2000, le Parlement européen a décidé, conformément à l'article 150, paragraphe 2 de son règlement, de créer une commission temporaire sur le système d'interception ECHELON et de définir le mandat de celle-ci (v. chapitre 1, point 1.3 de l'exposé des motifs). Au cours de sa réunion constitutive du 6 juillet 2000, la commission temporaire a nommé Gerhard Schmid rapporteur.

Au cours de ses réunions des 29 mai, 20 juin et 3 juillet, elle a examiné le projet de rapport.

Au cours de la dernière de ces réunions, elle a adopté la proposition de résolution par 27 voix contre 5 et 2 abstentions.

Étaient présents au moment du vote Carlos Coelho, président, Elly Plooij-van Gorsel, Neil MacCormick et Giuseppe Di Lello Finuoli, vice-présidents, Gerhard Schmid, rapporteur, Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard M.J. Deprez, Giorgos Dimitrakopoulos, Robert J.E. Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klant, Alain Krivine, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hugues Martin, Patricia McKenna, William Francis Newton Dunn, (suppléant Jorge Salvador Hernández Mollar conformément à l'article 153, paragraphe 2, du règlement), Reino Paasilinna, Bernd Posselt, (suppléant Hubert Pirker), Jacques Santkin (suppléant Catherine Lalumière), Ilka Schröder, Gary Titley (suppléant Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian von Bötticher, Jan Marinus Wiersma, Christos Zacharias (suppléant Enrico Ferri).

L'opinion minoritaire et les annexes sont publiées séparément (A5-0264/2001-Par2).

Le rapport a été déposé le 11 juillet 2001.

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.

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) (2001/2098 (INI))

Le Parlement européen,

- vu sa décision du 5 juillet 2000, relative à la création d'une commission temporaire sur le système d'interception ECHELON, ainsi que le mandat de ladite commission¹,
- vu le traité CE, qui vise la mise en place d'un marché commun présentant un degré élevé de compétitivité,
- vu les articles 11 et 12 du traité sur l'Union européenne qui lient les Etats membres à l'obligation de renforcer et développer leur solidarité politique mutuelle,
- 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 l'article 12 de la Déclaration universelle des droits de l'homme,
- 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 et l'article 8 protège les données à caractère personnel,
- vu la Convention européenne relative aux droits de l'homme, en particulier l'article 8 de celle-ci, qui protège la vie privée et la confidentialité des correspondances, ainsi que les nombreux autres traités internationaux qui protègent la vie privée,
- vu les travaux de la commission temporaire sur le système d'interception Echelon, qui a tenu de nombreuses auditions et réunions avec les experts les plus divers, en particulier avec des responsables des secteurs public et privé dans les domaines des télécommunications et de la protection des données, avec des membres des services de renseignements, des journalistes, des avocats experts en la matière, des députés des parlements des États membres, etc.,
- vu l'article 150, paragraphe 2, de son règlement,
- vu le rapport de la commission temporaire sur le système d'interception ECHELON (A5-0264/2001),

¹ JO C 121 du 24.4.2001, p. 36.

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 et à de nombreuses déclarations concordantes provenant d'horizons très divers – y compris de sources américaines –, que l'on peut penser que le système ou certaines parties de celui-ci portaient, du moins pendant quelque temps, le nom de code ECHELON,
- B. considérant qu'il est incontestable qu'il est utilisé au moins pour intercepter des communications privées et économiques, mais non militaires, et que l'analyse menée dans le cadre du rapport a montré que la capacité technique de ce système n'est peut être pas aussi grande, tant s'en faut, que ce que certains médias ont supposé,
- C. considérant qu'il est dès lors étonnant, voire inquiétant, que de nombreux responsables communautaires auditionnés, notamment des commissaires européens, aient déclaré ne pas avoir connaissance de ce phénomène,

en ce qui concerne les limites du système

- D. considérant que le système de surveillance repose notamment 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'UKUSA 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 encore plus limitée, considérant également que, aussi importants que soient les moyens et la capacité existants pour pouvoir intercepter les communications, il est impossible dans la pratique, eu égard au nombre très élevé de celles-ci, de toutes les contrôler de manière exhaustive et détaillée,

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

- E. 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 est le seul État membre de l'UE qui, grâce à ses territoires d'outre-mer, serait en mesure, des points de vue géographique et technique, d'exploiter de manière autonome un système d'interception mondial et qu'elle possède aussi l'infrastructure technique et organisationnelle nécessaire pour ce faire; qu'il existe de très nombreux indices prouvant que la Russie exploite vraisemblablement aussi un tel système,

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

- F. 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,
- G. considérant les déclarations faites par le Conseil lors de la séance plénière du 30 mars 2000, selon lesquelles : "le Conseil ne peut accepter la création ou l'existence d'un système d'interception des télécommunications qui ne respecte pas les règles de droit des États membres et qui viole les principes fondamentaux visant à préserver la dignité humaine";

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)

- H. 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,
- I. considérant qu'un système de renseignements qui intercepterait de manière aléatoire et en permanence les communications serait contraire au principe de proportionnalité et 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 ou si l'atteinte n'était pas proportionnée; 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,
- J. 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,
- K. 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

- L. 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; considérant que le fait d'obliger les services de renseignements à informer un citoyen a posteriori, par exemple cinq ans après l'interception, que ses communications ont été interceptées, encouragerait des pratiques d'interception proportionnée,
- M. considérant que, compte tenu de leur dimension, des stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment,
- N. considérant qu'en cas de coopération entre services de renseignements dans le cadre de la PESC ou de la JAI, les institutions seraient appelées à mettre en place des dispositions de protection suffisantes pour les citoyens européens,

en ce qui concerne l'espionnage économique

- O. 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,
- P. considérant que les services de renseignements des États-Unis s'occupent non seulement de problèmes économiques généraux mais aussi qu'ils interceptent des communications d'entreprises dans le contexte de passation de marchés, justifiant cela en invoquant la lutte contre les tentatives de corruption, que cette pratique porte en elle le risque que des informations soient utilisées non pas pour lutter contre la corruption mais à des fins d'espionnage concurrentiel même si les États-Unis affirment ne pas pratiquer celui-ci; que le rôle de l'Advocacy Center du ministère américain du commerce n'est toujours pas absolument clair et qu'un entretien avec cet organisme, qui devait contribuer à la clarification, a été refusé,

- Q. considérant qu'une convention en matière de lutte contre la corruption de fonctionnaire a été adoptée en 1997 dans le cadre de l'OCDE, laquelle prévoit que la corruption est passible de sanctions internationales, de sorte que dans les cas d'espèce la corruption ne saurait justifier l'interception de communications,
- R. 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,
- S. considérant que, lors de la visite effectuée aux États-Unis par une délégation de la commission temporaire, des sources autorisées ont confirmé le rapport Brown, indiquant que 5 % des informations collectées grâce à des sources non publiques sont utilisées à des fins économiques; que les mêmes sources estiment que cette surveillance pourrait permettre aux entreprises des États-Unis d'emporter jusqu'à 7 milliards de dollars de marchés,
- T. considérant que les données sensibles se trouvent principalement à l'intérieur des entreprises, de sorte que l'espionnage consiste notamment à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées et, de plus en plus, 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,
- U. considérant que, d'une manière générale, les petites et moyennes entreprises n'ont pas suffisamment conscience des risques et de la sécurité et ne reconnaissent pas les dangers de l'espionnage économique et de l'interception des communications,
- V. considérant que le sens de la sécurité n'est pas toujours très développé dans les institutions européennes (hormis à la Banque centrale européenne, à la direction générale des relations extérieures du Conseil et à la direction générale des relations extérieures de la Commission), et qu'il y a donc lieu d'agir,

en ce qui concerne les possibilités de protection

- W. 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

- X. 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,
- Y. considérant que le Conseil européen a décidé en décembre 1999 à Helsinki de se doter d'une capacité militaire européenne plus efficace afin de pouvoir s'acquitter de l'ensemble des missions de Petersberg dans le contexte de la PESD; qu'il a en outre décidé que, pour atteindre cet objectif d'ici à 2003, l'Union devait être en mesure de déployer rapidement des troupes d'environ 50 à 60 000 hommes qui seraient autonomes, disposant des capacités de commandement, de contrôle et de renseignements nécessaires; que les premiers pas dans la voie de la mise en place d'une telle capacité autonome en matière de renseignements ont déjà été franchis dans le cadre de l'UEO et du comité politique et de sécurité,
- Z. 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 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; qu'un contrôle par le Parlement européen devrait, dans ce cas, être assuré,
- AA. 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. affirme, sur la base des informations recueillies par la commission temporaire 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 doute;
2. 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 privée 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;
3. demande aux États membres dont les dispositions législatives réglementant le pouvoir d'interception des services secrets créent des discriminations en matière de protection de la

vie privée de garantir à tous les citoyens européens les mêmes garanties légales en ce qui concerne la protection de la vie privée et la confidentialité de la correspondance;

4. invite les États membres de l'Union européenne à mettre en place une plate-forme 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;
5. invite les États membres à adopter, lors de la prochaine conférence intergouvernementale, la Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux, notamment en ce qui concerne la vie privée;
6. 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;
7. demande, en attendant, aux institutions de l'Union européenne, dans le cadre de leur sphère de compétence et d'action respective, de mettre en application les droits fondamentaux établis par la Charte;
8. 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;
9. estime nécessaire la négociation et la signature d'une convention entre l'Union européenne et les États-Unis établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises;
10. 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

11. demande instamment aux États membres de vérifier la conformité aux droits fondamentaux, tels qu'ils sont définis dans la convention relative aux droits de l'homme et dans la jurisprudence de la Cour des droits de l'homme, de leur législation relative aux activités des services de renseignements et, au besoin, de lui apporter les adaptations nécessaires;
12. invite les Etats membres à se doter d'instruments contraignants garantissant une protection effective des personnes physiques et morales contre toute forme d'interception extralégale de leurs communications;
13. invite les États membres à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements et, à cette fin, à élaborer un code de conduite (voir paragraphe 4) 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;
14. invite les États membres à négocier avec les États-Unis un code de conduite analogue à celui de l'UE;
15. invite les Etats membres qui ne l'ont pas encore fait à garantir un contrôle parlementaire et juridictionnel adéquat de leurs services secrets;
16. invite le Conseil et les États membres à mettre en place d'urgence un système de contrôle démocratique de la capacité de renseignements européenne autonome ainsi que des autres activités de renseignements communes ou coordonnées au niveau européen; suggère que le Parlement européen joue un rôle important dans ce système de contrôle;
17. invite les Etats membres à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission;
18. invite les États membres à conclure avec les pays tiers une convention visant à renforcer la protection de la vie privée des citoyens de l'Union, convention dans laquelle toutes les parties s'engagent à ce que, en cas d'interception pratiquée par l'une d'entre elles dans un autre pays signataire, la première informe ce dernier des actions envisagées;

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

19. 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; invite les États-Unis, l'Australie, la Nouvelle-Zélande et le Canada à se joindre à cette initiative;
20. invite les Etats membres à s'engager à inclure dans le traité CE une clause interdisant

l'espionnage économique et à ne pas pratiquer l'espionnage économique entre eux, directement ou sous couvert d'une puissance étrangère qui pourrait intervenir sur leur sol, et à ne pas autoriser une puissance étrangère à mener des activités d'espionnage à partir du territoire d'un État membre de l'Union, afin de respecter l'esprit et la lettre du traité CE;

21. invite les États membres à s'engager, au moyen d'un instrument clair et contraignant, à ne pas pratiquer l'espionnage économique, proclamant ainsi le respect de l'esprit et de la lettre du traité CE; demande aux États membres de transposer ce principe contraignant dans leur législation nationale régissant les services de renseignements;
22. invite les États membres et le gouvernement des États-Unis à nouer un dialogue franc sur la collecte de renseignements économiques;

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

23. 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;
24. 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;
25. invite les États membres à s'assurer que leurs dispositifs de renseignements ne sont pas utilisés abusivement pour collecter des renseignements dans le cadre de la concurrence, au mépris de l'obligation de loyauté des États membres ainsi que de l'idée d'un marché unique fondé sur la libre concurrence;
26. 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

27. invite la Commission et les États membres à informer les citoyens et les entreprises qu'il est possible que leurs communications internationales soient, dans certaines circonstances, interceptées; demande instamment que cette information s'assortisse d'une assistance pratique en matière de conception et de mise en œuvre de mesures de protection globales, englobant la sécurité des techniques d'information;
28. invite la Commission, le Conseil et les États membres à élaborer et à appliquer une politique efficace et active en matière de sécurité de la société de l'information; demande instamment que, dans le cadre de cette politique, une attention particulière soit accordée à la sensibilisation de tous les utilisateurs des systèmes de communication modernes en ce

qui concerne la protection des informations confidentielles; demande en outre que soit mis en place un réseau européen coordonné d'organismes capables de fournir une assistance pratique en matière de conception et de mise en œuvre de stratégies de protection globale;

29. 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;
30. 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");
31. 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"); invite la commission à définir une qualification du niveau de sécurité des logiciels destinés à l'échange de correspondances électroniques en plaçant les logiciels dont le code source n'est pas publié dans la catégorie la moins fiable;
32. 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;
33. invite les institutions communautaires et les administrations publiques des États membres à prévoir la formation de leur personnel et la familiarisation de celui-ci avec les nouvelles technologies et les techniques de cryptage en organisant les stages et les cours de formation nécessaires;
34. demande que la situation des pays candidats fasse l'objet d'une attention particulière; demande que ceux-ci soient aidés s'ils ne sont pas en mesure de se doter des moyens de protection nécessaires faute d'indépendance technologique;

en ce qui concerne d'autres démarches

35. 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;
36. invite la Commission à faire réaliser une analyse de sécurité destinée à préciser ce qui doit être protégé et à faire élaborer un schéma de protection;
37. invite la Commission à actualiser son système de cryptage, une modernisation s'imposant d'urgence, et demande à l'autorité budgétaire (Conseil et Parlement) de prévoir les moyens financiers à cette fin;
38. invite sa commission compétente à élaborer un rapport d'initiative sur la sécurité et la protection du secret dans les institutions européennes;
39. invite la Commission à assurer la protection des données dans le contexte du traitement

interne de celles-ci et à renforcer la protection des documents non accessibles au public;

40. invite la Commission et les États membres à investir, dans le cadre du 6^e programme de recherche, dans les nouvelles technologies de cryptage et de décryptage;
41. demande qu'en cas de distorsion de concurrence due à des aides d'État ou à un recours abusif à l'espionnage économique, les États préjudiciés informent les autorités et les organes de contrôle de l'État d'origine de ces activités pour qu'il soit mis fin à celles-ci;
42. invite la Commission à proposer la création, en coopération étroite avec les entreprises et les États membres, d'un réseau européen et coordonné de centres de conseil, notamment dans les États membres qui ne possèdent pas de tels organes, en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;
43. 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 plate-forme 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;
44. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission, ainsi qu'au secrétaire général et à l'Assemblée parlementaire du Conseil de l'Europe, aux gouvernements et aux parlements des États membres et des pays candidats, des États-Unis, d'Australie, de Nouvelle-Zélande et du Canada.

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 STOA² avait commandée sur le système appelé ECHELON³ 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 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'ECHELON⁵.

² 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, à la demande des commissions. Les études ne font pas l'objet d'une vérification scientifique.

³ *Duncan Campbell*, 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 dans PE 168.184 (octobre 1999).

⁴ *Steve Wright*, Une évaluation des techniques de contrôle politique, étude intérimaire STOA, PE 166.499 (1998), p. 20.

⁵ *Duncan Campbell*, Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmitleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung, dans PE 168.184 (octobre 1999).

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 exemples d'espionnage économique présumés, qui auraient été la cause de préjudices notamment pour Airbus et Thomson CFS. Campbell s'appuie sur des informations fournies par la presse américaine⁶.

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 mandat⁷. 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."

⁶ Raytheon Corp Press release, <http://raytheon.com/sivam/contract.html>; *Scott Shane, Tom Bowman, America's Fortress of Spies*, Baltimore Sun, 3.12.1995.

⁷ Résolution du Parlement européen du 5 juillet 2000, B-5 – 0593/2000, JO C 121/131 du 24.4.2001.

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 interinstitutionnelle⁸, 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 commission d'enquête aurait impliqué 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,
9. conséquences sous l'angle des relations extérieures de l'UE.

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

⁸ 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.

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, télécopieur, 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 UKUSA)⁹ 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.

⁹ V. chapitre 5, point 5.4.

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 renseignement¹⁰. 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.

¹⁰ 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" (1996) constate que 95 % de tous les renseignements d'ordre économique proviennent de sources publiques (chapitre 2 "The Role of intelligence").
<http://www.gpo.gov/int/report.html>

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 généralement que le citoyen et les autres personnes qui se trouvent 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, télécrypteur, 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 UKUSA

Signification des différentes colonnes:

1^{re} colonne: pays concerné

2^e colonne: communications extérieures, c'est-à-dire communications en provenance et à destination de l'étranger (civiles, militaires, diplomatiques)¹¹

3^e colonne: communications publiques (militaires, diplomatiques, etc.)

4^e colonne: communications privées

+ : interception

- : pas d'interception

¹¹ Si le service de renseignement a accès au câble, il peut intercepter à la fois les communications provenant de l'étranger et les communications destinées à l'étranger. S'il a accès aux communications pas satellite, celui-ci se limite au *downlink*, mais l'ensemble des communications transportées peuvent être interceptées, y compris donc celles qui ne sont pas destinées à son territoire. Étant donné que la couverture des satellites s'étend généralement à l'ensemble de l'Europe ou à des régions plus vastes encore (voir 4.4.2.5.), une station de réception de satellite permet d'intercepter les communications par satellite de toute l'Europe dans un pays européen.

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 place¹²

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, télécopieurs et courriers électroniques** peuvent être interceptés, si l'espion se branche sur le câble sortant du bâtiment.
- Un **téléphone portable** peut être intercepté – moyennant un gros effort technique – si la station d'interception se situe dans la même cellule (rayon: 150 m en ville, 15 km à la campagne).
- Un **émetteur de radio interne** peut être intercepté dans la limite des ondes radio ultracourtes.

¹² *Manfred Fink*, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, 1996.

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, 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 être 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 UKUSA**, 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 télécopieur. 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 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 Internet et l'apparition de fournisseurs 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-Unis¹³;
- une petite partie des communications intraeuropéennes sont acheminées via un commutateur à Londres, auquel le GCHQ britannique (Centre national de communications) a accès – étant donné qu'il s'agit de communications avec l'étranger. 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 UKUSA ne peuvent avoir accès qu'à une **partie très limitée** des communications Internet tributaires du câble.

3.3.1.2. Communications hertziennes¹⁴

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;

¹³ Une version de démonstration de *Visual Route*, programme qui indique le chemin suivi par une communication Internet, a permis de montrer qu'une communication avec le Royaume-Uni, la Finlande ou la Grèce à partir de l'Allemagne passe par les États-Unis et le Royaume-Uni. De même pour une communication d'Allemagne vers la France. À partir du Luxembourg, la communication vers la Belgique, la Grèce, la Suède ou le Portugal passe par les États-Unis, les communications à destination de l'Allemagne, de la Finlande, de la France, de l'Italie, des Pays-Bas ou de l'Autriche par le *switch* londonien. <http://visualroute.cgan.cpm.hk/>

¹⁴ U. Freyer, *Nachrichtenübertragungstechnik*, Hanser Verlag, 2000.

- 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 réfléctée. 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 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 UKUSA ne peuvent avoir accès, grâce aux stations d'interception terrestres, qu'à une partie très limitée des communications hertziennes.

3.3.1.3. Communications via des satellites de télécommunication géostationnaires¹⁵

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 UKUSA 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.

¹⁵ Hans Dodel, Satellitenkommunikation, Hüthig Verlag, 1999.

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 complété par un système d'identification d'objectifs donnés, qui peut repérer des rayonnements électroniques, les classer et les corrélérer avec des contacts radar. Il n'existe pas une capacité SIGINT distincte¹⁶. 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 militaires¹⁷.

De plus, des navires de surface et, à proximité des terres des sous-marins sont utilisés pour intercepter les communications radio militaires¹⁸.

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 pas possible de filtrer les signaux¹⁹. Ces satellites ne se prêtent pas à une surveillance en continu des communications radio civiles.

Parallèlement, il existe des satellites SIGINT américains dits quasi-stationnaires sur orbite haute (42 000 km)²⁰. 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 périégée 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

¹⁶ Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense au rapporteur, en date du 14.2.2001.

¹⁷ Süddeutsche Zeitung, n° 80 du 5.4.2001, 6.

¹⁸ Jeffrey T. Richelson, *The U.S. Intelligence Community*, Ballinger, 1989, 188 et 190.

¹⁹ Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense, en date du 14.2.2001.

²⁰ Major A. Andronov, *Zarubezhnoye voyennoye obozreniye*, n° 12, 1993, 37 à 43.

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-ci²¹. Par contre, la reconnaissance automatique de mots prononcés par une voix quelconque n'est, selon les informations en possession de votre rapporteur, pas possible actuellement avec une précision suffisante. 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 froide²².

3.3.3. Exemple du service de renseignements allemand

La deuxième section du service fédéral de renseignement allemand (BND) se procure des informations par l'interception des communications étrangères. Cette activité a fait l'objet d'un examen par la Cour constitutionnelle allemande. Les détails qui ont été rendus publics à cette occasion²³ 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 (jusqu'au mois de mai 2001, l'interception de communications par câble avec l'étranger n'était pas autorisée en Allemagne).

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,

²¹ Communication faite en privé au rapporteur, source protégée.

²² Communication faite en privé au rapporteur, source protégée.

²³ BVerfG, 1 BvR 2226/94 du 14.7.1999, paragraphe 1.

en Allemagne, doivent être autorisées préalablement par la commission G10²⁴).

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

²⁴ Gesetz zur Beschränkung des Brief-,Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 GG) du 13.8.1968.

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. Elle se situe entre 0,4 et 5 %²⁵. 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 percevoir le décalage. 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 câbles²⁶.

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

²⁵ Indications fournies par les opérateurs de quelques États membres à la demande de la commission.

²⁶ 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 satellitaire²⁷

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 environ 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.

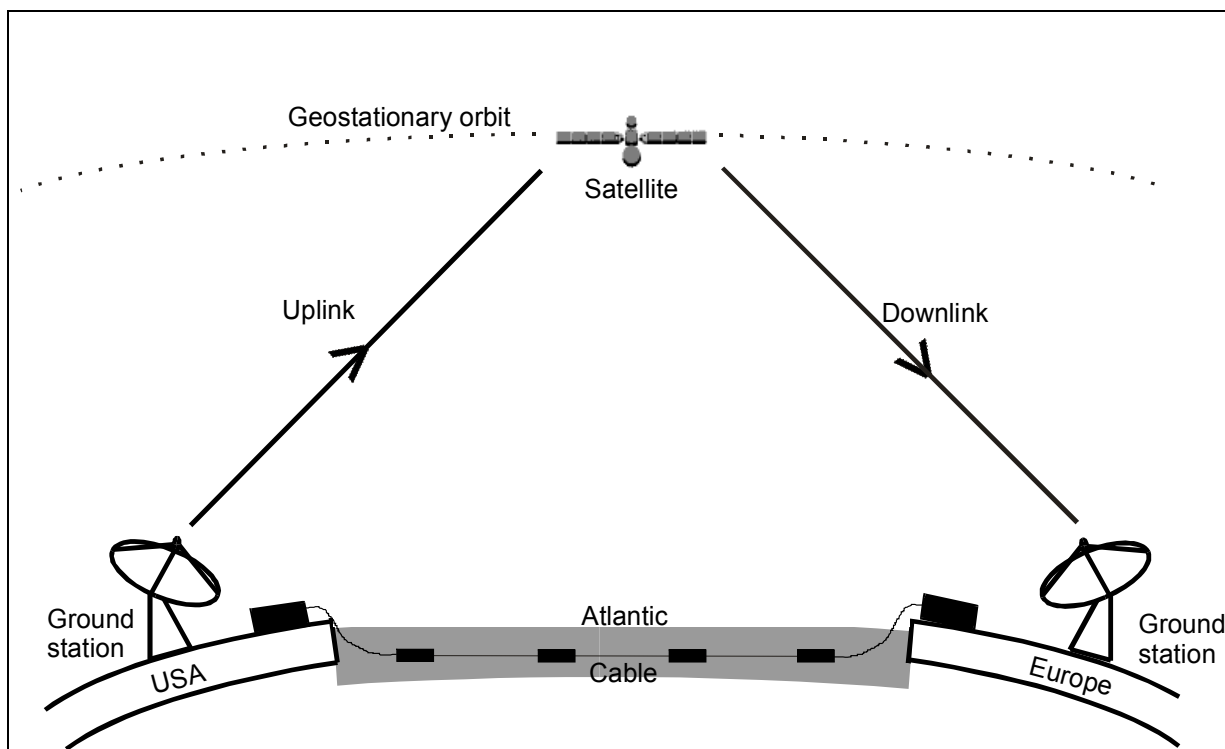
4.2.2. Cheminement d'une liaison satellitaire de télécommunication

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.

²⁷ Hans Dodel, Satellitenkommunikation, Hüthig Verlag (1999), Georg E. Thaller, Satelliten im Erdorbit, Franzisverlag (1999).

Dans le cas de la communication mobile (par satellite), 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 orbites²⁸.

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 plus de la moitié de leur période orbitale. Deux satellites de ce genre permettent en principe ainsi une couverture régionale²⁹, qui ne peut être obtenue à partir d'une position géostationnaire au-dessus de l'équateur. S'agissant des satellites russes Molnyia, en service depuis 1974 pour les

²⁸ Georg E. Thaller, Satelliten im Erdorbit, Franzisverlag, 1999.

²⁹ Vgl. dazu Hans Dodel, Satellitenkommunikation, Hüthig Verlag (1999)

communications (prototype dès 1964), 3 satellites parcourent en 12 heures une orbite circum-terrestre, à 120° de distance, assurant ainsi la transmission continue des communications³⁰.

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 communication 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 a 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-même³¹.

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.

INTELSAT³²

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 20 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).

³⁰ Homepage der Federation of American Scientists <http://www.geo-orbit.org>

³¹ Hans Dodel, déclaration faite en privé.

³² Page d'accueil d'INTELSAT – <http://www.intelsat.com>.

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.

INTERSPUTNIK³³

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 interétatique, 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 Lockheed-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).

INMARSAT³⁴

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, 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).

³³ Page d'accueil d'INTERSPUTNIK: <http://www.intersputnik.com>.

³⁴ Page d'accueil d'INMARSAT, <http://www.inmarsat.com>

PANAMSAT³⁵

PanAmSat a vu le jour en 1988 en tant qu'opérateur commercial d'un système de satellites mondial ayant son siège aux États-Unis. Aujourd'hui, il dispose d'une flotte de 21 satellites fournissant différents services de télévision et de télécommunication dans le monde entier, mais principalement aux États-Unis.

Les télécommunications sont acheminées sur les bandes C et Ku. Sept des vingt-et-un satellites couvrent la zone atlantique, deux la pacifique et deux l'indienne. La couverture des autres satellites s'étend à l'Amérique (Nord et Sud). Ces satellites ne jouent qu'un rôle mineur en ce qui concerne les communications en Europe.

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.

EUTELSAT³⁶

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.

ARABSAT³⁷

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.

³⁵ Page d'accueil de PANAMSAT, <http://www.panamsat.com>

³⁶ Page d'accueil d'EUTELSAT: <http://www.eutelsat.com>.

³⁷ Page d'accueil d'ARABSAT: <http://www.arabsat>.

PALAPA³⁸

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 nationaux³⁹

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 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 (ITU). 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,

³⁸ Hans Dodel, Satellitenkommunikation, Hüthig Verlag, 1999.

³⁹ Hans Dodel, Satellitenkommunikation, Hüthig Verlag, 1999 et recherches Internet.

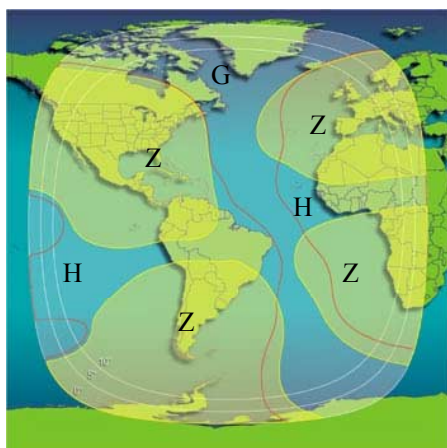
- la bande C (3,6 - 6,6 GHz) pour les stations hertziennes terrestres, par exemple via INTELSAT,
- la bande Ku (10 - 20GHz) pour les stations hertziennes terrestres, par exemple INTELSAT-Ku-Spot et EUTELSAT,
- la bande Ka (20 - 46 GHz) pour les stations hertziennes terrestres, par exemple les satellites de communication militaires (v.4, 4.3.),
- 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'INTELSAT⁴⁰:

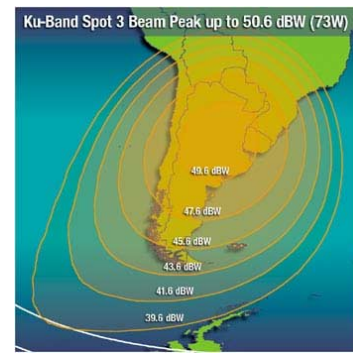
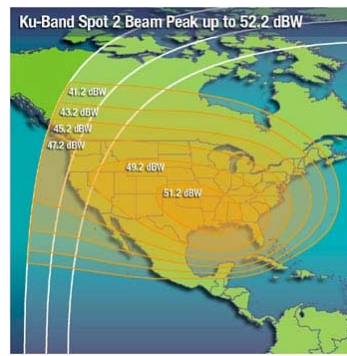
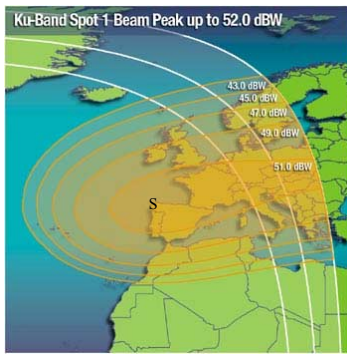


Les zones d'empreinte des satellites d'INTELSAT se répartissent entre différents faisceaux:

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 pincesaux, c'est-à-dire des zones d'empreinte précises et réduites(cf. infra).

⁴⁰ INTELSAT Satellit 706, 307°E, Ausleuchtzonen von Homepage von INTELSAT: <http://www.intelsat.com>



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 dont la limite va de 0,5 à 3 m. 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 antennes 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 (v. aussi 5, 5.2.3).

Les antennes actuellement nécessaires pour les communications INTELSAT dans la bande C ont un diamètre compris entre 13 et 20 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 15 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 0,5 et 3,7 m est suffisant (p.ex., VSAT d'EUTELSAT ou INMARSAT).

4.3. Communications par satellite à finalités militaires

4.3.1. Généralités

Dans le domaine militaire aussi, les satellites de communication jouent un rôle important. De nombreux pays – notamment les États-Unis, le Royaume-Uni, la France et la Russie – exploitent des satellites de communication militaires géostationnaires qui rendent possibles les communications mondiales indépendamment d'autres vecteurs. Avec 32 positions orbitales, les États-Unis disposent d'un satellite tous les 10° en moyenne. Il est parfois fait usage aussi de satellites commerciaux géostationnaires pour des communications militaires.

4.3.2. Fréquences utilisées par les militaires

Les bandes utilisées pour les communications militaires vont de 4 GHz à 81 GHz. Les bandes utilisées par les satellites militaires sont plus particulièrement la bande X (SHF), 3-30 GHz, et la bande Ka (EHF), 20-46 GHz.

4.3.3. Taille des stations de réception

Celles-ci sont mobiles, leur taille ne dépassant pas alors dans certains cas quelque dizaines de centimètres, ou stationnaires – dans ce cas, leur diamètre n'est pas supérieur à 11 mètres. On compte cependant deux types d'antennes (réception de satellites DSCS) d'un diamètre de 18 mètres.

4.3.4. Exemples

Le programme américain **MILSTAR** (Military Strategy, Tactical and Relay Satellite System) utilise 6 satellites géostationnaires. Il permet à l'armée des États-Unis de faire communiquer entre eux et avec les commandements, au moyen de petits postes, les avions, les navires et les troupes. L'interconnexion des satellites assure la disponibilité continue, même en cas de défaillance de l'ensemble des stations non américaines au sol.

Le **DSCS** (Defense Satellite Communications System) permet également des communications mondiales grâce à 5 satellites géostationnaires. Il est utilisé par les militaires et par certains services gouvernementaux.

Le système militaire britannique **SKYNET** est également un système mondial.

Le système français **SYRACUSE**, le système italien **SICRAL** et le système espagnol "empruntent" des satellites de communication civils et permettent des communications militaires dans la bande X, mais limitées au plan régional.

Les Russes assurent leurs communications militaires par transpondeur sur la bande X grâce à leurs satellites Molnya.

L'OTAN exploite ses propres satellites (**NATO IIID**, **NATO IVA** et **IVB**). Ils transmettent communications vocales, télex et données entre les différentes unités.

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 UKUSA reconnaîtraient coopérer à l'exploitation d'un système d'interception mondial. Dès lors, 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 UKUSA 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 UKUSA;
- 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 UKUSA 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 UKUSA, 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.⁴¹

⁴¹ 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 UKUSA 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 UKUSA 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 exceptionnel; 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 assurent également une partie au moins de l'interception. Ainsi, dans les stations gérées par les États-Unis, par exemple, c'est le Naval Security Group (NAVSECGRU) ou l'Air Intelligence Agency des forces aériennes américaines (AIA) ou le United States Army Intelligence and Security Command (INSCOM) qui assure avec la NSA le fonctionnement des stations. Dans les stations britanniques, c'est la Royal Airforce qui gère les installations avec le 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) ou 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 satellites de communication militaires,
- stations de réception des satellites-espions (photos, radar)
- stations de réception des satellites 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, leur diamètre fournit certaines indications à cet égard. Pour les satellites de communication civils destinés à recevoir le faisceau à couverture mondiale dans la bande C des communications internationales civiles par satellites, il existe des dimensions minimales, fonction de la technique. 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 20 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.

Pour les communications militaires, on observe dans les centres de commandement deux types d'antennes dont le diamètre est proche de 18 m (AN/FSC-78 et AN/FSC-79). La plupart des antennes destinées aux communications militaires ont toutefois un diamètre beaucoup plus faible étant donné qu'elles doivent être transportables (stations tactiques).

Les stations au sol destinées aux satellites SIGINT ne nécessitent que de petites antennes, ce qui s'explique par les caractéristiques du signal renvoyé à la station (faisceau et fréquence importants). Cela concerne aussi les antennes captant les signaux de satellites d'espionnage.

Si une installation présente au moins deux antennes pour satellites de plus de 18 m, il est certain que l'interception des communications civiles y est pratiquée. S'agissant d'une station accueillant des militaires des États-Unis, une des antennes peut servir aux communications militaires.

5.2.4. Critère 4: Preuves officielles

Pour certaines stations, on dispose d'une description officielle précise des missions. Les sources sont considérées comme officielles s'il s'agit d'informations gouvernementales ou d'informations fournies par les militaires.

S'il est satisfait à ce critère, il n'est pas nécessaire d'examiner les autres pour classer une station parmi les stations d'interception de communications civiles.

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 (Hager⁴², Richelson⁴³, Campbell⁴⁴), les documents déclassés⁴⁵, la page d'accueil de la Federation of American Scientists⁴⁶ ainsi que les pages d'accueil de NSA, AIA, etc. et d'autres publications sur Internet ont été consultés⁴⁷. Pour la station néo-zélandaise de Waihopai, on dispose d'une description officielle de ses missions

⁴² *Nicky Hager*: Exposing the global surveillance system. <http://www.ncoic.com/echelon1.htm>
Nicky Hager: Secret Power. New Zealand's Role in the international Spy Network, Craig Potton Publishing 1996.

⁴³ *Jeffrey T. Richelson*, Desperately Seeking Signals, The Bulletin of the Atomic Scientists Vol 56 Nr. 2,47-51, <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html>
Jeffrey T. Richelson, The U.S. Intelligence Community, Westview Press 1999.

⁴⁴ *Duncan Campbell*, dans PE 168.184 (octobre 1999)
<http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf>
Duncan Campbell: Inside Echelon, 25.7.2000 <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>
Duncan Campbell: 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> .

⁴⁵ *Jeffrey T. Richelson*: 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> .

⁴⁶ Federation of American Scientists (FAS), <http://www.fas.org/> .

⁴⁷ Military.com; *.mil-Homepages.

fournie par le gouvernement du pays⁴⁸. 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 en principe être captés par une seule antenne, car il est techniquement possible de séparer différentes bandes de fréquence à la réception, mais cela est à l'origine d'une dégradation du rapport signal/bruit.

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 militaires⁴⁹; 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 30 mètres, pour les autres générations, supérieure à 15-18 m. Les descriptions officielles d'une partie des stations sont considérées comme preuves du rôle d'interception de ces stations.

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.

⁴⁸ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, Securing our Nation's Safety (2000), <http://www.dmpc.govt.nz/dess/securingoursafety/index.html> .

⁴⁹ Abréviations utilisées: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

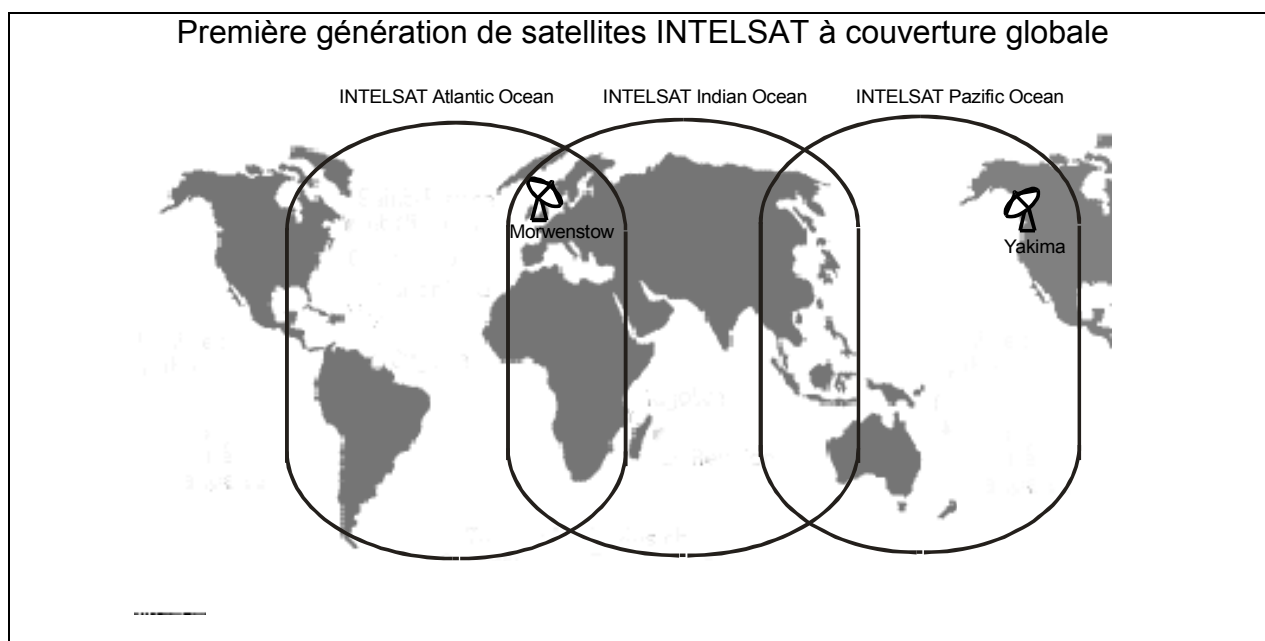
Par conséquent, à l'inverse, lorsque l'on crée de nouvelles zones de couverture et que l'on construit de nouvelles stations et de nouvelles antennes satellitaires, cela n'est pas par hasard: on peut voir là l'indice de l'existence d'une station d'écoute de communications.

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 mondiale

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.

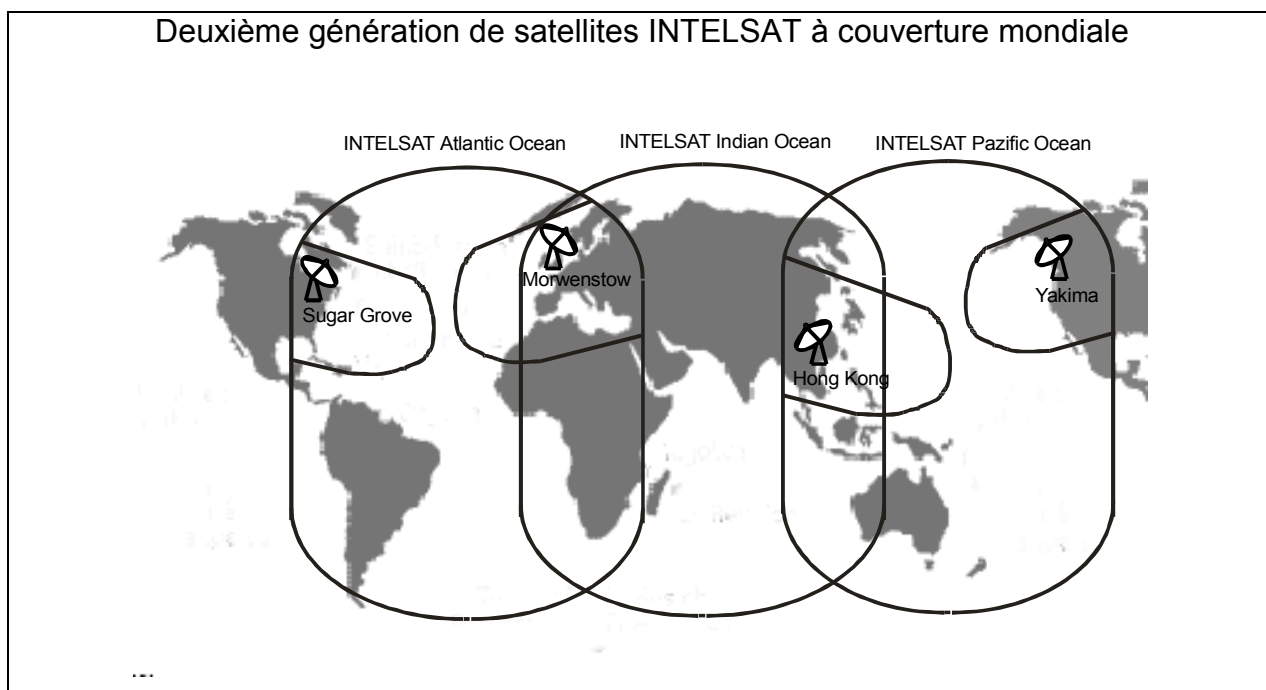
Avec les générations INTELSAT II et III, mises en service respectivement en 1967 et en 1968, on obtint, pour la première fois, une couverture globale. Les *global beams* des satellites couvraient les zones atlantique, pacifique et indienne. Il n'y avait pas encore de zones de couverture plus petites. Pour capter la totalité des communications, il fallait donc trois satellites. Comme deux des *global 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.



Au début des années 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.

La deuxième génération mondiale

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 *global beams*, des *zone beams* dans l'hémisphère nord (voir chapitre 4). Un *zone 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 *zone beam* de "Ouest des États-Unis"; Morwenstow couvrait le *zone beam* "Europe". Pour couvrir les deux autres *zone beams*, il fallait disposer d'une station à l'est des États-Unis et d'une autre dans la région est-asiatique.



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 satellites INTELSAT ultérieurs, avec *zone beams* et *spot beams* en plus des *global 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 sur la base des informations disponibles.

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 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 et pour lesquelles on ne dispose pas d'autres éléments concluants, peuvent cependant faire partie du système d'écoute global. Ces stations permettraient, par exemple, d'intercepter les *zones beams* ou *spot beams* de satellites dont les *global beams* sont écoutés par d'autres stations ou pour les *global beams* desquels il n'est pas nécessaire de disposer de grandes antennes satellitaires.

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 dans les années 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 satellitaires) 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 satellites normale, 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 communication⁵⁰.

De plus, Sugar Grove est située à proximité (60 miles) de la station de réception de satellites normale d'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 satellites Intelsat, au début des années 70. Morwenstow est desservie par le service de renseignements britannique (GCHQ). Morwenstow compte environ 21 antennes satellitaires, dont trois d'un diamètre de 30 mètres; on ne dispose pas de données concernant la dimension des

⁵⁰ „It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations.“ aus der Homepage der (44th Intelligence Group <http://www.aia.af.mil> .

autres antennes.

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. Au moins une des grandes antennes, mais certainement pas l'ensemble de celles-ci, est une antenne de réception de communications militaires (AN/FSC-78). 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 d'interception 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, quatre antennes satellitaires, de même diamètre (quelque 20 m), 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 civils⁵¹.

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 NAVSECGRU⁵².

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.

⁵¹ Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra, <http://www.aph.gov.au/hansard>.

⁵² Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra, <http://www.aph.gov.au/hansard>.

Misawa, Japon (141°O, 40°N)

La station de Misawa est dotée depuis 1948 d'une antenne HFDF. 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.

Waihopai, Nouvelle-Zélande (173°O, 41°S)⁵³

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. Selon Hager, les antennes sont orientées sur des Intelsat 701 en orbite au-dessus du Pacifique. La mission de Waihopai consiste d'après les indications officielles du GCSB (General Communications Security Bureau) à intercepter les communications par satellite, à décrypter et à traiter les signaux.⁵⁴ Étant donné que la station ne dispose que de deux antennes pour satellites, le service secret néozélandais ne peut intercepter qu'une petite partie des communications dans l'espace pacifique. La station n'est intéressante qu'en liaison avec une autre station de la même zone. Hager cite généralement Geraldton, en Australie, comme "station soeur" de Waihopai.⁵⁵

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)

⁵³ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety", décembre 2000, <http://www.dpmc.gov.nz/dess/securingoursafety/index.html>.

⁵⁴ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety", décembre 2000, <http://www.dpmc.gov.nz/dess/securingoursafety/index.html>: "In 1989,[...] the GCBS opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCBS not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on to the appropriate Minister or government department."

⁵⁵ *Nicky Hager*, *Secret Power, New Zealand's Role in the International Spy Network*, Craig Potton Publishing (1996), 182.

La station est implantée à proximité de Bad Aibling. Y travaillent quelque 750 Américains. Sont stationnés à Bad Aibling l'INSCOM (66th IG, 718 IG), qui assure le commandement, le NAVSECGRU 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 pour l'interception de satellites de communication russes. Le 30 septembre 2002, la station devrait être fermée, en vertu d'une décision du ministère de la défense. Le personnel serait réparti sur d'autres unités.⁵⁶

Ayios Nikolaos, Chypre (32°O, 35°N)

Ayios Nikolaos (Chypre) est une station britannique. Elle compte 14 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 4 antennes satellitaires, dont 2 de 15 m de diamètre.

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.

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.

⁵⁶ Communication du 31.5.2001, Homepage d'INSCOM, http://www.vulcan.belvoir.army.mil/bas_to_close.asp.

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 Meade, États-Unis (76°O, 39°N)

Fort Meade 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 *global beams*, des stations d'écoute munies chacune d'au moins une antenne d'un diamètre supérieur à 20 mètres et desservies par des Américains ou des Britanniques et/ou où des Américains ou des Britanniques exercent des activités de renseignement.
2. Le développement des communications par INTELSAT et l'apparition simultanée de stations d'écoute correspondantes attestent l'orientation globale du système.
3. Certaines de ces stations ont pour mission, d'après les informations officielles, l'interception de satellites de communication.
4. Les données figurant dans les documents déclassifiés 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 satellites, 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 UKUSA⁵⁷

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'initiative visant à la création d'une alliance SIGINT fut prise par les Américains, en août 1940, lors d'une rencontre entre Américains et Britanniques, à Londres⁵⁸. 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 1941⁵⁹. 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 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-Uni⁶⁰. 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 unique⁶¹.

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 algorithmes des codes et clés de cryptage. Les Américains étaient compétents pour le Japon; les Britanniques pour l'Allemagne et l'Italie⁶².

⁵⁷ Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in Hayden B., Peake, Samuel Halpern (Eds), In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, (NIBC Press 1994, 95 – 109).

⁵⁸ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, ibidem, 99: "At a meeting 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'". (zitiert nach COS (40) 289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, 38, 43f-4. Sir F.H. Hinsley, et al., British Intelligence in the Second World War, Vol. I, 312f).

⁵⁹ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, ibidem, 100: "In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O'Connor, [...], to advise him on cryptologic collaboration".

⁶⁰ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, ibidem, 100 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, Vol. II, 56).

⁶¹ Christopher Andrew, The making of the Anglo-American SIGINT Alliance, ibidem, 101 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, Vol. II, 48).

⁶² Christopher Andrew, The making of the Anglo-American SIGINT Alliance, ibidem, 101f: Interviews mit

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 paix⁶³. 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 aboutit à un accord de quelque 25 pages, toujours classifié, qui arrêta 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 1948⁶⁴.

5.4.2. Éléments attestant l'existence de l'accord

5.4.2.1. Rapport annuel 1999/2000 de la commission britannique du renseignement et de la sécurité

Pendant longtemps, les États signataires n'ont jamais reconnu officiellement l'existence de l'accord UKUSA. Dans le rapport annuel de la commission du renseignement et de la sécurité, organe de contrôle parlementaire au Royaume-Uni, l'accord UKUSA est mentionné explicitement.⁶⁵

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.

⁶³ *Harry S. 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 to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations 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.“ (cité par *Bradley F. Smith*, *The Ultra-Magic Deals and the Most Secret Special Relationship* (Presidio 1993)).

⁶⁴ *Christopher Andrew*, "The making of the Anglo-American SIGINT Alliance" in *Hayden, Peake and Samuel Halpern* eds, *In the Name of Intelligence. Essays in Honor of Walter Pforzheimer*, (NIBC Press 1995), 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.

⁶⁵ Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8 Rz 14.

Texte original: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ."

5.4.2.2. Informations fournies par les services du Premier Ministre de Nouvelle-Zélande

Des informations publiées l'an dernier par les services du Premier ministre de Nouvelle-Zélande au sujet des services nationaux de sécurité et de renseignements en font mention explicitement.⁶⁶ D'autres éléments attestent clairement son existence.

5.4.2.3. Liste des acronymes utilisés par la Navy

Selon la marine américaine⁶⁷, UKUSA veut dire "United Kingdom, USA" et désigne "un accord SIGINT entre cinq nations".

5.4.2.4. 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 UKUSA⁶⁸.

5.4.2.5. 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.

5.4.2.6 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'accord⁶⁹.

⁶⁶ Domestic and External Secretariat du Department of the Prime Minister and Cabinet de Nouvelle Zélande, *Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies* (2000). Texte original: "The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD) and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own."

⁶⁷ „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>.

⁶⁸ *Martin Brady*, Direktor des DSD, Lettre du 16.3.1999 à Ross Coulthart, Sunday Program Channel 9.

⁶⁹ *Andrew, Christopher* "The growth of the Australian Intelligence Community and the Anglo-American Connection", 223-4.

5.4.2.7 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.

5.4.2.8 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 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)⁷⁰. 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 SIGINT⁷¹. Comme suite à l'entretien avec Jeffrey Richelson à Washington, ce dernier a transmis à la commission d'autres documents qui ne sont plus couverts par le secret. Il a été tenu compte de ceux qui étaient intéressants du point de vue de l'enquête.

5.5.2. Contenu des documents

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

⁷⁰ Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Briefing Book n°. 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>.

⁷¹ Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Briefing Book n°. 24, George Washington University <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html>.

5.5.2.1. Mission et conception de la NSA (documents 1, 2b, 4, 10 et 16)

Dans la directive 9 du National Security Council Intelligence (NSCID 9) du 10 mars 1950⁷², 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)⁷³ stipule que le FBI est seul responsable pour la sécurité intérieure.

La directive du ministère de la défense du 23 décembre 1971⁷⁴ (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 2000⁷⁵ 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 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.

⁷² Document 1. NSCID 9, "Communications Intelligence," March 10, 1950.

⁷³ Document 2b. National Security Council Intelligence Directive n° 9, Communication Intelligence, December 29, 1952.

⁷⁴ Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971.

⁷⁵ Document 16. Statement for the Record of NSA Director Lt Gen Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12, 2000.

Dans un mémorandum du vice-amiral des forces navales américaines, W.O. Studeman, établi au nom du gouvernement, en date du 8 avril 1992⁷⁶, 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)⁷⁷

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.⁷⁸

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

Dans les instructions C5450.48A⁷⁹ 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"⁸⁰, 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, nouveaux documents)

- Sugar Grove (Virginie occidentale), cité comme Station SIGINT dans les NAVSECGRU INSTRUCTIONS C5450.48A,⁸¹

⁷⁶ Document 10. Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8, 1992.

⁷⁷ Document 7. United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures", July 27, 1993.

⁷⁸ Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24, 1952.

⁷⁹ Document 9. navsecgru Instruction C5450.48A, Subj.:Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

⁸⁰ Document 12. "Activation of Echelon Units", from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

⁸¹ Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

- Misawa Air Base (Japon), cité comme station SIGINT dans History of the Air Intelligence Agency – January to 31 December 1994⁸², et dans la description des activités du Naval Security Group dans les documents du ministère de la Marine⁸³
- Porto Rico (Sabana Seca), cité comme station SIGINT dans History of the Air Intelligence Agency – January to 31 December 1994, et dans la description des activités du Naval Security Group dans les documents du ministère de la Marine⁸⁴
- Guam, cité comme station SIGINT, ibidem
- Yakima (Washington), cité comme station SIGINT, 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.⁸⁵
- Menwith-Hill, Royaume-Uni, description des activités du Naval Security Group dans les documents du ministère de la marine⁸⁶
- Bad Aibling, Allemagne, description des activités du Naval Security Group dans les documents du ministère de la marine⁸⁷
- Medina, Texas, description des activités du Naval Security Group dans les documents du ministère de la marine⁸⁸
- Kunia, Hawaii, description des activités du Naval Security Group dans les documents du ministère de la marine⁸⁹

5.5.2.6. Protection de la vie privée des citoyens américains (documents 7, 7a à f, 9, 11 et 16)

Les NAVSECGRU INSTRUCTIONS C5450.48A arrêtent qu'il faut protéger la vie privée des citoyens.⁹⁰

⁸² Document 12. "Activation of Echelon Units, "from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

⁸³ Department of the Navy, Naval Security Group Instruction C5450.32E du 9.5.1996.

⁸⁴ Naval Security Group Instruction C5450.33B du 8.8.1996.

⁸⁵ COMINT Report de la NSA de Fort George G. Meade, Maryland du 31 août 1972.

⁸⁶ Department of the Navy, Fact and Justification Sheet for the Establishment of U.S. Naval Security Group Activity.

⁸⁷ Department of the Navy, Naval Security Group Instruction C55450.63 du 25.10.1995.

⁸⁸ Department of the Navy, Naval Security Group Instruction C5450.60A du 8.4.1996

⁸⁹ Naval Security Group Instruction C5450.55B du 8.8.1996

⁹⁰ Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991

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 suppléments⁹¹.

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

La directive du ministère de la défense du 23 décembre 1991⁹² donne des définitions précises de SIGINT, COMINT, ELINT et TELINT, tout comme la directive n° 6 du National Security Council Intelligence du 17 février 1972.⁹³

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.
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

⁹¹ 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).

⁹² Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971

⁹³ Document 5a. NSCID 6, "Signals Intelligence," February 17, 1972.

de Washington).

8. D'autres stations où opère le Naval Security Group sont citées mais non décrites comme stations SIGINT.
9. 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. Nicky Hager

Dans le livre de l'auteur néo-zélandais, 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. Il se base sur des entretiens avec plus de 50 personnes employées par le service de renseignements néozélandais ou engagées par ailleurs dans des activités de renseignement. De plus, il a analysé de nombreux documents provenant des archives nationales de journaux et d'autres sources publiques. D'après Hager, le système est dénommé ECHELON et les ordinateurs du réseau sont dénommés "dictionnaires ECHELON".

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 satellites⁹⁴ – 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'Inmarsat⁹⁵, organisation dont les activités concernent principalement les communications maritimes.

⁹⁴ Cf.: <http://www.intelsat.int/index.htm>.

⁹⁵ Cf.: <http://www.inmarsat.org/index3.html>.

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

Dans l'exposé qu'il a fait le 24 avril 2001 devant la commission, Hager a souligné que le système d'interception n'était pas tout-puissant. Étant donné qu'il faut utiliser au mieux les ressources limitées, tout ne peut pas être intercepté: il faut se contenter de ce qui promet des informations importantes. Les objectifs sont donc en général constitués par des informations politiques et diplomatiques. Si l'interception a pour objectif d'obtenir des informations économiques, celles-ci s'inscrivent plutôt dans un contexte macroéconomique que microéconomique.

S'agissant des méthodes de travail du système, chaque partenaire a ses propres listes de mots-cibles. En outre, les communications sont également analysées sur la base de mots-clés injectés dans le système par les États-Unis au moyen de "dictionary managers". Les Britanniques n'ont aucun contrôle sur cet aspect et ignorent quelles informations sont collectées à Morwenstow parce que celles-ci sont directement transmises aux États-Unis.

Dans ce contexte, Hager a souligné le risque que peuvent constituer les stations d'interception britanniques pour l'Europe continentale. Citant de nombreux exemples, il a fait observer que les partenaires UKUSA du Pacifique espionnaient leurs alliés et leurs partenaires commerciaux. Les seules personnes qui échappaient à l'espionnage étaient les partenaires UKUSA. Il a estimé que les services secrets britanniques et les Néozélandais seraient sans doute très réticents à compromettre le partenariat UKUSA en refusant de coopérer et d'écouter l'Europe continentale. Rien n'inciterait le Royaume-Uni à renoncer à des informations intéressantes et, étant donné qu'elles sont toujours secrètes, l'espionnage pratiqué dans le cadre de l'accord UKUSA n'exclurait pas une politique officielle de loyauté vis-à-vis de l'Europe.

5.6.2. Duncan Campbell

Le journaliste britannique Duncan Campbell s'appuie dans ses nombreuses publications sur les travaux de Hager et Richelson ainsi que sur des entretiens avec d'anciens collaborateurs des services secrets, de même que sur d'autres recherches. Selon lui, ECHELON fait partie du système mondial qui intercepte et analyse les communications internationales par satellite. Chaque État membre dispose d'ordinateurs "Dictionary" qui analysent les communications interceptées à partir de mots-clés.

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 pas⁹⁶.

Dans l'exposé qu'il a fait devant la commission le 22 janvier 2001, Campbell a estimé que les USA faisaient appel à leurs services de renseignements pour aider les entreprises américaines à obtenir des marchés. Les informations intéressantes sont transmises aux entreprises via la CIA, avec l'aide de l'Advocacy Center et de l'Office of Executive Support au Department of Commerce. À l'appui de cette hypothèse, il a présenté des documents desquels il ressort que l'Advocacy Center est intervenu à l'avantage d'entreprises américaines. L'information figure aussi largement sur la page d'accueil de l'Advocacy Center.⁹⁷ Dire que la réussite de l'Advocacy Center s'explique par les écoutes relève de la spéculation et cela ne ressort pas des documents.

Campbell a souligné au cours de son exposé que les capacités d'interception de plusieurs pays européens s'étaient nettement accrues au cours des dernières années – notamment en Suisse, au Danemark et en France. On observe par ailleurs un renforcement de la coopération bilatérale et multilatérale dans le domaine du renseignement.

5.6.3. Jeff Richelson

Jeff Richelson, auteur américain et 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)⁹⁸.

Il est en outre l'auteur de différents ouvrages et articles sur les activités des services de renseignements des États-Unis. Ses travaux s'appuient sur de nombreux documents ayant cessé d'être secrets, sur le travail de recherche de Hager ainsi que sur ses recherches personnelles. Lors de sa rencontre avec la délégation de la commission à Washington DC, le 11 mai 2001, il a déclaré qu'ECHELON désignait un réseau d'ordinateurs, au moyen duquel seraient filtrées des données échangées entre les services de renseignements.

Dans son livre intitulé "The ties that binds"⁹⁹, 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"¹⁰⁰, de 1999, il donne un aperçu des activités des services secrets des États-Unis et décrit les structures d'organisation des services ainsi que 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 dépeint les relations des États-Unis avec d'autres services de renseignements, notamment l'accord UKUSA.

⁹⁶ *Duncan Campbell*, Inside Echelon. The history, structure and function of the global surveillance system known as Echelon, <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>

⁹⁷ Homepage des Advocacy Centers, <http://www.ita.doc.gov/td/advocacy/index.html>

Le rapporteur a souhaité permettre à l'Advocacy Center de prendre position sur ces allégations lors de sa mission à Washington DC. Le Commerce Department Center a cependant annulé le rendez-vous.

⁹⁸ Jeffrey T. Richelson, The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University, <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>

⁹⁹ Jeffrey T. Richelson, Desmond Ball, The Ties That Bind, Boston UNWIN HYMAN (1985).

¹⁰⁰ Jeffrey T. Richelson, The U.S. Intelligence Community, Westview Press (1999).

Dans un article intitulé "Desperately seeking Signals"¹⁰¹, publié en 2000, il expose brièvement le contenu de l'accord UKUSA, cite des installations d'interception de communications par satellites et renseigne les possibilités et les limites de l'interception de communications civiles.

5.6.4. James Bamford

L'auteur américain James Bamford, qui fonde également ses travaux sur des recherches dans les archives ainsi que sur l'interrogatoire de collaborateurs des services de renseignement, fut le premier à s'intéresser à l'activité SIGINT de la NSA. En 1982 déjà, il publiait "The Puzzle palace"¹⁰², décrivant dans le détail, en son chapitre 8 "Partners", l'accord UKUSA. Selon son nouveau livre "Body of Secrets"¹⁰³, qui fait fond sur les faits révélés dans "The Puzzle Palace", le réseau informatique qui relie les services de renseignement s'appelle "Plattform", ECHELON désignant pour sa part le logiciel, utilisé dans toutes les stations, qui permet un traitement unique et un accès direct aux données¹⁰⁴. Dans les chapitres qui suivent, il emploie toutefois également le nom ECHELON pour désigner le système d'interception dans le cadre de l'accord UKUSA.

Dans "Body of Secrets" – et ce en son chapitre "Muscle" tout particulièrement intéressant en l'occurrence –, Bamford brosse l'histoire du développement de la surveillance des communications par la NSA et décrit la capacité du système, le fonctionnement du partenariat UKUSA et les objectifs de celui-ci. Il souligne que les interviews de dizaines d'agents actuels et anciens de la NSA démontrent que celle-ci n'est pas impliquée dans l'espionnage de concurrence.

Ce dire, il l'a confirmé lors de son audition devant la commission ECHELON le 23 avril dernier. L'utilisation de la NSA aux fins de l'espionnage de concurrence nécessiterait une décision politique claire au plus haut niveau politique, décision qui n'a toujours pas été prise jusqu'ici. Au cours de ses vingt années de recherche, il n'a jamais eu la preuve que la NSA transmettait à des entreprises américaines des informations obtenues par les services de renseignement, y compris dans le cas, par exemple, où elle intercepte les communications d'entreprises privées pour s'assurer du respect d'embargos.

Selon les déclarations de Bamford, le problème majeur pour l'Europe résiderait dans la question de savoir non pas si le système ECHELON vole des secrets d'entreprises et les communique à leurs concurrents mais bien s'il y a violation du droit fondamental à la vie privée. Dans "Body of Secrets", il décrit de façon détaillée comment la protection des "US persons" (c'est-à-dire les citoyens américains et les personnes résidant légalement aux États-Unis) s'est développée, faisant observer qu'il existe également pour d'autres résidents UKUSA à tout le moins des restrictions internes. Parallèlement, il signale qu'il n'existe pas de protection pour d'autres personnes ni d'obligation d'élimination des données, et que les capacités de mémorisation de la NSA sont pour ainsi dire incommensurables.

¹⁰¹ Jeffrey T. Richelson, Desperately seeking Signals, The Bulletin of the Atomic Scientists, Vol. 56, No. 2/2000, 47-51, <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html>

¹⁰² James Bamford, The Puzzle Palace, Inside the National Security Agency, America's most secret intelligence organization (1983).

¹⁰³ James Bamford, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001).

¹⁰⁴ James Bamford, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001), 404.

Néanmoins, Bamford met aussi l'accent sur les limites du système qui procèdent du fait, d'une part, qu'une petite partie seulement des communications internationales est effectuée par satellite et qu'il est beaucoup plus difficile d'intercepter les communications par câbles à fibres optiques, et, d'autre part, que la NSA ne dispose que de capacités limitées d'exploitation finale, alors que le flux des communications, en particulier via le réseau internet, ne cesse de croître.

5.6.5. 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. Le Danemark, qui avait nettement renforcé ses capacités d'interception au cours de la dernière décennie, collabore avec les États-Unis depuis 1984.

Dans un article paru dans Ekstra Bladet¹⁰⁵, où ils se référaient à la présentation de diapositives (25 diapositives) par un officier non nommé du 544^e Intelligence Group de l'Air Intelligence Agency, ils signalaient que différentes ONG (au nombre desquelles la Croix-Rouge) étaient la cible de l'activité d'ECHELON.

5.7. Déclarations d'anciens collaborateurs des services de renseignements

5.7.1. Margaret Newsham (ex-collaboratrice de la NSA)¹⁰⁶

Margaret Newsham 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 de 1977 à 1981 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.

¹⁰⁵ *Bo Elkjaer, Kenan Seeberg*, ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Danemark, 8.3.2000, <http://cryptome.org/echelon-red.htm>

¹⁰⁶ *Bo Elkjaer, Kenan Seeberg*, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.

5.7.2. Wayne Madsen (ancien collaborateur de la NSA)

Wayne Madsen¹⁰⁷, 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 avantages 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.

Lors de sa rencontre avec la délégation de la commission à Washington DC, il s'est dit particulièrement préoccupé par le danger que représentait le système d'espionnage mondial pour la vie privée des citoyens européens.

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 CSE¹⁰⁸. La station d'interception d'Ottawa ne serait qu'un élément d'un réseau mondial de stations d'espionnage¹⁰⁹. 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 gouvernement¹¹⁰. 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 ambiguë 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 personnelles¹¹¹.

Les services de renseignement des pays UKUSA 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 côtés¹¹².

¹⁰⁷ Interview de NBC "60 Minutes" du 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

¹⁰⁸ Communication Security Establishment, service dépendant du ministère canadien de la défense, qui est chargé de l'activité Sigint.

¹⁰⁹ Interview de NBC "60 Minutes" du 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

¹¹⁰ Florian Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special.

¹¹¹ Interview de NBC "60 Minutes" du 27.2.2000; <http://cryptome.org/echelon-60min.htm>.

¹¹² Interview de la chaîne australienne Channel 9 du 23.3.1999; <http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm>.

5.7.4. Fred Stock (ancien collaborateur des services secrets canadiens)

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 mer¹¹³.

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 presse¹¹⁴, 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 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.

¹¹³ *Jim Bronskill*, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, <http://www.ottawacitizen.com/national/990522/2630510.html>.

¹¹⁴ *James Woolsey*, Remarks at the Foreign Press Center, Transcript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

5.8.2. Déclarations anglaises

Il ressort de différentes questions posées au sein de la chambre des Communes¹¹⁵, 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 NSA¹¹⁶, un membre du personnel de celle-ci étant le chef de la station¹¹⁷, en tant qu'installation de communication¹¹⁸. 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 GCHQ¹¹⁹. La présence des troupes américaines est régie par le traité de l'Atlantique nord et par des accords administratifs spéciaux et secrets¹²⁰, qui sont jugés conformes aux relations existant entre les gouvernements du Royaume-Uni et des États-Unis dans le contexte d'une défense commune¹²¹. 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'OTAN¹²².

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 inopérantes, le GCHQ pourrait, trois jours plus tard, servir non seulement ses clients britanniques mais aussi ses clients américains¹²³.

5.8.3. Déclarations australiennes¹²⁴

Martin Brady, directeur de la DSD, service de renseignement australien¹²⁵, 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 stades¹²⁶.

¹¹⁵ Commons Written Answers, House of Commons Hansard Debates.

¹¹⁶ 12.7.1995.

¹¹⁷ 25.10.1994.

¹¹⁸ 3.12.1997.

¹¹⁹ 12.5.2000.

¹²⁰ 12.7.1995.

¹²¹ 8.3.1999 et 6.7.1999.

¹²² 3.12.1997.

¹²³ Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, présenté au Parlement par le Premier ministre en novembre 2000.

¹²⁴ *Martin Brady*, directeur de la DSD, lettre du 16 mars 1999 à Ross Coulthart, Sunday Program, channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.

¹²⁵ Defence Signals Directorate, Service de renseignement australien gérant le MRE (SIGINT).

¹²⁶ *Martin Brady*, directeur de la DSD, lettre du 16 mars 1999 à Ross Coulthart, Sunday Program, channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.

5.8.4. Déclarations néo-zélandaises

Comme il a déjà été expliqué au point 5.4.2.2., une publication, de 2000, des services du Premier ministre néo-zélandais concernant les services de la sûreté et du renseignement fait clairement état du partenariat existant entre les services de renseignement de 5 pays – États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande – et des avantages qu'il présente pour la Nouvelle-Zélande¹²⁷.

5.8.5. 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 modernes¹²⁸. 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.

5.8.6. 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'ECHELON¹²⁹. 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. Questions au Conseil et à la Commission

Dès le 17 février 1998, le Conseil se vit poser par la députée Elly Plooi-j-van Gorsel¹³⁰, une première question générale sur le rapport STOA et sur l'existence d'un système d'interception

¹²⁷ Domestic and External Secretariat du Department of the Prime Minister and Cabinet de Nouvelle-Zélande Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000). Pour le texte original, cf. supra note du point 5.4.2.2..

¹²⁸ 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.

¹²⁹ Francesco Sorti, Dossier. esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998.

¹³⁰ Question écrite P-0501/98 posée par Elly Plooi-j-van Gorsel (ELDR) au Conseil (17.1.1998). Le 14.5.1997, Jonas Sjöstedt avait déjà posé une question (H-0330/97) sur la résolution du Conseil du 17.1.1995 sur la surveillance légale des télécommunications, où il demandait s'il y avait un lien avec ECHELON. Cette dernière partie de la question n'a pas reçu de réponse. Aux questions de Mihail Papayannakis (G-004/98) et Nel van Dijk (H-0035/98) sur l'activité d'espionnage britannique, il fut répondu le 18.2.1998 que les questions ressortissant aux services de renseignement étaient de la seule compétence des autorités nationales et que le Conseil ne disposait d'aucune information en la matière.

mondial des États-Unis auquel le Royaume-Uni participerait, ainsi que sur les préjudices qui en résulteraient pour les intérêts commerciaux d'entreprises européennes. De nombreuses autres questions sur le même thème suivirent¹³¹. La présidence y répondit que le Conseil ne disposait lui-même d'aucune information à ce sujet, qu'il n'était pas impliqué dans de telles choses, et qu'il ne pouvait, partant, fournir aucune réponse.

Aux questions similaires posées à la Commission européenne¹³², il fut répondu que la Commission avait connaissance du rapport, mais qu'il n'existait ni preuve ni plainte selon laquelle un État membre violerait le traité CE à cet égard¹³³. La Commission faisait toutefois preuve de vigilance et défendrait tous les intérêts communautaires non sans continuer à déployer des efforts pour améliorer la sécurité de son réseau informatique¹³⁴. Au cours de la séance plénière du 18 septembre, M. Bangemann, membre de la Commission, déclarait que la Commission ne disposait d'aucune information émanant des États membres ni de citoyens ou d'entreprises selon lesquelles le système d'interception existerait tel qu'il est décrit, ajoutant que si ce système existait bien, il s'agirait naturellement là d'une violation flagrante du droit, des droits individuels des citoyens et bien entendu également une atteinte à la sécurité des États membres, la chose est parfaitement claire, et que dès le moment où on constaterait officiellement un tel état de fait, le Conseil et, cela va de soi, la Commission et le Parlement se devaient de réagir. La Commission agirait également de tout son poids afin d'inciter les États membres à ne pas entrer en possession d'informations par cette voie illégale¹³⁵.

¹³¹ Question écrite E-0499/98 posée Elly Plooi-j-van Gorsel (ELDR) au Conseil (27.2.1998), question écrite E-1775/98 posée par Lucio Manisco (GUE-NGL) au Conseil (8.6.1998), question orale H-1086/98, posée au Conseil par Patricia McKenna (16.12.1998), question orale H-1172/98, posée au Conseil par Patricia McKenna (13.1.1999), question orale H-1172/98 posée au Conseil par Inger Schörling (13.1.1999), question orale H-0526/99, posée au Conseil par Pernille Frahm (6.10.1999), question orale H-0621/99, posée au Conseil par Lone Dybkjaer (19.11.1999), etc.

¹³² Question écrite E-1039/98 posée par Nel van Dijk (V) à la Commission (15.5.1998), question écrite E-1306/98 posée par Cristiana Muscardini (NI) à la Commission (15.6.1998), question écrite E-1429/98 posée par Daniela Raschofer (NI) à la Commission (25.6.1998), questions écrites E-1987/98 et E-2329/98 posées par Nikitas Kaklamanis à la Commission (3.9.1998 et 25.9.1998), question écrite 1776/98 posée par Lucio Manisco (GUE/NGL) à la Commission, question écrite 3014/98 posée par Paul Lannoye (V) à la Commission (6.11.1998), question orale H-0547/99 posée par Pernille Frahm à la Commission, question orale H-1067 posée par Patricia McKenna (V) à la Commission (16.12.1998), question orale H-1237/98 posée par Inger Schörling à la Commission (13.1.1999), question orale H-0092/99 posée par Ioannis Theonas à la Commission (13.1.1999), question orale H-0547/99 posée par Pernille Frahm à la Commission (6.10.1999), question orale H-0622/99 posée par Lone Dybkjaer à la Commission (17.12.1999), etc.

¹³³ Déclaration faite le 25.9.1998 au nom de la Commission, par M. Bangemann, membre de la Commission, en réponse à la question écrite E-1776/98 du député Lucio Manisco (GUE-NGL).

¹³⁴ Déclaration faite le 3.9.1998, au nom de la Commission, par M. Santer, Président de la Commission, en réponse à la question écrite E-1987/9.

¹³⁵ Débats du Parlement européen, séance du lundi 14.9.1998, point 7 de l'ordre du jour, relations transatlantiques/système ECHELON.

5.10. Rapports parlementaires

5.10.1. Rapports du comité permanent R de contrôle belge

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.

5.10.2. 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'écoute¹³⁶. Lors de sa réunion du 28 novembre 2000, le rapporteur, Arthur Paecht, a présenté à la commission ECHELON du Parlement européen les conclusions de son rapport.

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 ECHELON 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.

¹³⁶ 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.

Le système ECHELON 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.

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

5.10.3. Rapport de la commission parlementaire italienne des services d'information et de sécurité ainsi que de la sûreté de l'État

En Italie, la commission parlementaire des services d'information et de sécurité a présenté au président du Parlement, le 19 décembre 2000, un rapport sur le rôle des services d'information et de sécurité dans le cas ECHELON¹³⁷.

Les conclusions relatives à l'existence d'un système appelé ECHELON sont vagues. Selon le rapport, il a été en grande partie exclu lors des auditions au sein de la commission que pouvait exister un système d'interception intégré de ce nom, qui aurait été mis en place par les cinq pays parties à l'accord UKUSA (États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada) et qui servirait à intercepter les communications dans le monde entier. S'il était établi qu'il y avait une coopération plus étroite entre les pays anglo-saxons, les enquêtes de la commission ne permettraient cependant pas d'affirmer que cette coopération portait sur la création d'un système d'interception intégré ou d'un système d'interception à l'échelle mondiale. Selon la Commission, il était probable que l'appellation ECHELON désignait un stade du développement technologique dans le domaine de la technique d'interception satellitaire. Il est expressément constaté que le service secret italien SISMI a exclu l'existence, à l'époque, d'un procédé de reconnaissance automatique de mots prononcés au cours de conversations et constaté, dès lors, qu'une interception ciblée de conversations contenant ces mots-clés n'était pas possible.

¹³⁷ "Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'." Relazione del comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

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, à l'échelle mondiale, 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 UKUSA.

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 françaises. 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 français¹³⁸, 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 Alluets-le-Roi (près de Paris). Jauvert estime à 30 au total le nombre des antennes satellitaires. L'écrivain Erich Schmidt-Eenboom¹³⁹ affirme qu'une station serait également en service en Nouvelle-Calédonie et que le service de renseignement allemand utiliserait dans une certaine mesure cette installation.

En théorie, la France, qui réunit non seulement les conditions géographiques mais aussi les conditions techniques et financières, 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

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

Conformément à la base juridique, l'objectif de la FAPSI consiste à recueillir des informations d'ordre politique, économique, militaire et technico-scientifique aux fins de promouvoir le développement économique ainsi que le progrès scientifico-technique et militaire¹⁴⁰. De plus, le directeur de la FAPSI a constaté en 1997 que sa fonction première était l'interception des communications étrangères codées ainsi que l'écoute mondiale¹⁴¹.

¹³⁸ 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.

¹³⁹ Erich Schmidt-Eenboom, Strenge Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, 1999.

¹⁴⁰ Loi de la Fédération de Russie sur le renseignement étranger adoptée par la Douma le 8.12.1995, sections 5 et 11.

¹⁴¹ Citation in Gordon Bennett, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, août 2000, <http://www.csrc.ac.uk/pdfs/c105.pdf>

Dans la zone de l'Atlantique, il y a la station cubaine de Lourdes (82° O / 23° N), qui est exploitée en commun avec le service de renseignement cubain. Par l'intermédiaire de cette station, la Russie recueille à la fois des informations stratégiques, militaires et commerciales¹⁴². Pour la zone de l'océan Indien, il y a des stations en Russie, à propos desquelles on ne dispose d'aucune information précise. Une autre station située à Skrunda (Lettonie) a été fermée en 1998¹⁴³. 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 néanmoins également insuffisantes pour pouvoir affirmer avec certitude quelque chose.

6.4. Autres pays du G8 et Chine

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

¹⁴² Citation in *Gordon Bennett*, UK Ministry of Defence, The Federal Agency of Government Communications and Information, et page d'accueil de la Federation of American Scientists

¹⁴³ Page d'accueil de la Federation of American Scientists (FAS), <http://www.fas.org>

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 communautaire¹⁴⁴. 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 extérieur¹⁴⁵. 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 de concurrence, 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 corruption¹⁴⁶. S'il était exact que les systèmes sont utilisés aux fins de l'espionnage de concurrence, alors la question de la compatibilité avec le droit communautaire se poserait 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

¹⁴⁴ Cf. à ce propos chapitre 1, point 1.3. supra.

¹⁴⁵ Cf. à ce propos chapitre 2 supra..

¹⁴⁶ Cf. à ce propos chapitre 5, points 5.6 et 5.8.

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 et à la libre circulation de ces données¹⁴⁷ 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 télécommunications¹⁴⁸ ne s'appliquent pas "en tout état de cause aux traitements¹⁴⁹/activités¹⁵⁰ 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 électroniques¹⁵¹, 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 communautaires 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 données¹⁵². Ce règlement ne s'applique également que là où ces organes et institutions agissent dans le cadre du traité CE¹⁵³. 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 domaine¹⁵⁴.

¹⁴⁷ JO L 281 du 23.11.1995, p. 31.

¹⁴⁸ JO L 24 du 30.1.1998, p. 1.

¹⁴⁹ Directive 95/46/CE, art. 3, par. 2.

¹⁵⁰ Directive 97/66/CE, art. premier, par. 3.

¹⁵¹ COM(2000) 385, JO C 365 E, p. 223.

¹⁵² Règlement (CE) n° 45/2001, JO L 8 du 12.1.2001, p. 1.

¹⁵³ 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'application 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. (...)".

¹⁵⁴ 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

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 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 renseignement¹⁵⁵, 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 de concurrence

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 équivaldrait 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

219 du 30.7.1999, pp. 61 et ss.

¹⁵⁵ 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.

privée dans le secteur des télécommunications¹⁵⁶ 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 de concurrence, 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 (...)". 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 qu'en principe, 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 au sens large. 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.

¹⁵⁶ Directive 97/66/CE, JO L 24 du 30.1.1998, p. 1.

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 fin¹⁵⁷, 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 UKUSA 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".¹⁵⁸

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 public¹⁵⁹. Au plan mondial, le pacte international relatif aux

¹⁵⁷ 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."

¹⁵⁸ 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>, qui fait référence au Foreign Intelligence Surveillance Act (FISA), reproduit au titre 50 chapitre 36 U.S.C. § 1801 et ss. et à l'Exec. Order No. 12333, 3 C.F.R. 200 (1982), reproduit au titre 50, chapitre 15 U.S.C. § 401 et ss., <http://www4.law.cornell.edu/uscode/50/index.html>.

¹⁵⁹ Art. 12 Déclaration universelle des droits de l'homme; Art 17, Pacte des Nations unies relatif 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 sur des lignes directrices pour la sécurité des systèmes informatiques adoptée les 26 et 27.11.1993 C(92) 188/Final; Art 7 Convention du Conseil de l'Europe sur la protection des personnes dans le domaine du traitement automatique des données à caractère personnel; cf. à ce propos l'étude commandée par le STOA "Development of surveillance technology 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), octobre 1999, 2.

droits civils et politiques¹⁶⁰, conclu en 1966 dans le cadre de l'ONU, garantit en son article 17 la protection de la vie privée. Tous les pays UKUSA 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 protocole additionnel¹⁶¹, 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 communications¹⁶². 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 parties 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

¹⁶⁰ Pacte international relatif aux droits civils et politiques, adopté par l'AG des Nations unies le 16. 12. 1966.

¹⁶¹ Protocole facultatif au pacte international relatif aux droits civils et politiques, adopté par l'AG des Nations unies le 16.12.1966.

¹⁶² "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications".

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.

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 être 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 national¹⁶³.

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 convention¹⁶⁴. 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

¹⁶³ CEDH *Loizidou/Turquie*, 23.3.1995, n° 62 avec d'autres éléments à l'appui "...the concept of 'jurisdiction' 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" avec référence à la CEDH, *Drozd und Janousek*, 26.6.1992, n° 91. Pour plus de détails, cf. *Francis G. Jacobs, Robin C. A. White, The European Convention on Human Rights*², Clarendon Press (1996), 21 et ss, *Jochen Abr. Frowein, Wolfgang Peukert, Europäische Menschenrechtskonvention*, N. P. Engel Verlag (1996), Rz 4 et ss.

¹⁶⁴ CEDH, *Klass et autres*, 6.9.1978, n° 41.

vie privée¹⁶⁵.

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 national¹⁶⁶. Le droit doit être accessible à tous et prévisible dans ses effets¹⁶⁷.

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 pays¹⁶⁸, 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 domaines¹⁶⁹. 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 privée¹⁷⁰.

Une organisation conforme aux droits de l'homme des activités des services de renseignements

¹⁶⁵ CEDH, Malone, 2.8.1984, n° 83 et suivants; Davy, B/Davy/U, Aspekte staatlicher Informationsammlung und Art 8 MRK, JBl 1985, 656.

¹⁶⁶ 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. Pour plus de détails, Wolfgang Wesseley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ss, 495.

¹⁶⁷ Silver et autres, 25.3.1983, Z 87 et ss.

¹⁶⁸ 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./Suède, 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 devenue caduque Ciliz/Pays-Bas, 11.7.2000, p. 65.

¹⁶⁹ CEDH, Leander, 26.3.1987, p. 51.

¹⁷⁰ CEDH, Malone, 2.8.1984, p. 67.

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 privée¹⁷¹. Les ingérences ne sont certes pas limitées à ce qui est indispensable mais il ne suffit pas qu'elles soient opportunes ou souhaitables¹⁷². 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.

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 abus¹⁷³. 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 secrets¹⁷⁴, pas plus que de système de contrôle comparable au médiateur parlementaire des pays nordiques¹⁷⁵. 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 contrôle¹⁷⁶, d'autant que la France dispose de capacités de renseignements notables, tant du point de vue technique que du point de vue géographique.

¹⁷¹ CEDH, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, p. 46 ss.

¹⁷² CEDH, Silver et autres, 24.10.1983, Z 97.

¹⁷³ CEDH, Leander, 26.3.1987, p. 60.

¹⁷⁴ Le rapporteur sait que ni le Luxembourg ni l'Irlande ne disposent ni de services de renseignements à l'étranger ni de SIGINT. La nécessité d'une instance de contrôle particulière ne concerne que les activités de renseignements à l'intérieur du pays.

¹⁷⁵ Au sujet du contrôle des services de renseignements dans les États membres, voir chapitre 9.

¹⁷⁶ Proposition de loi tendant à la création de délégations parlementaires pour le renseignement, et rapport afférent du député Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'Assemblée nationale le 23 novembre 1999.

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 la 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.

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 convention¹⁷⁷.

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 personne¹⁷⁸. Si un pays autorise un

¹⁷⁷ *Dimitri 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.*

¹⁷⁸ CEDH, *Abdulaziz, Cabales et Balkandali*, 28.5.1985, p. 67; *X et Y/Pays-Bas*, 26.3.1985, p. 23; *Gaskin* –

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.

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 en considération:

Royaume-Uni 7.7.1989, Z 38; Powell et Rayner, 21.2.1990, p. 41.

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 nationales¹⁷⁹. 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 corruption¹⁸⁰. 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 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.

¹⁷⁹ 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.

¹⁸⁰ *James Woolsey* (ancien directeur de la CIA), *Why America Spies on its Allies*, *The Wall Street Journal Europe*, 22.3.2000, 31 ders., Remarks at the Foreign Press Center, Transskript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>.

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 matière¹⁸¹, 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)¹⁸².

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 requise¹⁸³. 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

¹⁸¹ Voir à ce propos également chapitre 7.

¹⁸² Ces objectifs sont reconnus comme justification d'atteinte à la vie privée par l'article 8, paragraphe 2, de la CEDH. Voir 8.3.2. ci-dessus.

¹⁸³ 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).

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.

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'étranger¹⁸⁴. 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 interdite¹⁸⁵. Dans d'autres, elle peut, dans certains cas, sous réserve de l'approbation d'une commission indépendante¹⁸⁶, être autorisée par un ministre¹⁸⁷ et ce sans restriction aucune pour de nombreux moyens de communication¹⁸⁸. 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

¹⁸⁴ Pour l'activité des services de renseignement étranger, voir les commentaires détaillés du chapitre 2.

¹⁸⁵ Autriche et Belgique.

¹⁸⁶ En Allemagne, Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Conformément au § 9, la Commission doit être informée avant l'exécution (sauf risque de retard).

¹⁸⁷ 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).

¹⁸⁸ En France (Art. 20 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

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 au niveau national. Sauf en cas d'urgence, une commission indépendante, non liée par un mandat (G 10-Kommission¹⁸⁹) 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)¹⁹⁰ 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 des services de renseignements constitue cependant une exception parmi les États membres.

En France¹⁹¹, 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

¹⁸⁹ Pour des commentaires détaillés: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, publié par le Deutscher Bundestag, Sekretariat des PKGr.

¹⁹⁰ Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) du 17 juin 1999 BGBl I 1334 idgF.

¹⁹¹ Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications.

commission de la défense de l'Assemblée nationale a adopté une proposition¹⁹², 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 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)¹⁹³, 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 Belgique¹⁹⁴, au Danemark¹⁹⁵, en Allemagne¹⁹⁶, en Italie¹⁹⁷, aux Pays-Bas¹⁹⁸ et au Portugal¹⁹⁹, il

¹⁹² Voir "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", et rapport afférent du député Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'Assemblée nationale le 23 novembre 1999.

¹⁹³ Intelligence Services Act 1994, Section 10.

¹⁹⁴ 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.

¹⁹⁵ Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarrets og politiets efterretningstjenester, lov 378 af 6/7/88.

¹⁹⁶ Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idGF.

existe des commissions de contrôle parlementaires qui assurent à la fois le contrôle des services militaires et des services civils. Au Royaume-Uni²⁰⁰, 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 Autriche²⁰¹, les deux branches du service de renseignements sont contrôlées par deux commissions distinctes qui sont toutefois organisées de la même manière et qui bénéficient des mêmes droits. En Finlande²⁰² et en Suède²⁰³ 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 influencer 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

¹⁹⁷ 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.

¹⁹⁸ Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-Generaal, Art. 22.

¹⁹⁹ Conselho de Fiscalização dos Serviços de Informações (CFSI), loi 30/84 du 5 septembre 1984, modifiée par la loi 4/95 du 21 février 1995, loi 15/96 du 30 avril 1996 et loi 75-A/97 du 22 juillet 1997.

²⁰⁰ Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

²⁰¹ Ständiger 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 verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art 52a B-VG, §§ 32b et ss. Geschäftsordnungsgesetz 1975.

²⁰² Ombudsman, base juridique pour le contrôle pour la police (SUPO): Poliisilaki 493/1995 §33 et Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, pour l'armée: Poliisilaki 493/1995 §33 et Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

²⁰³ Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (règlement (1989:773) relatif à la police nationale).

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.

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 sont 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'armement²⁰⁴.

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 chapitre 10, point 10.1.4).

²⁰⁴ Informationen für geheimschutzbetrente Unternehmen, Bundesministerium für Wirtschaft 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'oeuvre²⁰⁵. 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-Unis²⁰⁶. 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 allemandes²⁰⁷ 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.

²⁰⁵ *Michael E. Porter*, *Competitive Strategy*, Simon & Schuster (1998).

²⁰⁶ *Roman Hummelt*, *Wirtschaftsspionage auf dem Datenhighway*, Hanserverlag, 1997.

²⁰⁷ Détails et noms confidentiels.

Dès 1988, l'institut Max Planck évaluait le préjudice dû à l'espionnage économique en Allemagne à 8 milliards de marks au moins²⁰⁸. Le président de l'association des entreprises de conseil en sécurité d'Allemagne, Klaus-Dieter Matschke, 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, chiffre le préjudice à 20 milliards de dollars par an. Le FBI²⁰⁹ 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'emplois²¹⁰.

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 LLP²¹¹, 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 secrets²¹².

10.3.1. Collaborateurs de l'entreprise (délict 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.

²⁰⁸ IMPULSE, 3/97, pp.13 et ss.

²⁰⁹ *Louis J. Freeh*, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington D.C., 9.5.1996.

²¹⁰ *Robert Lyle*, Radio Liberty/Radio Free Europe, 10 février 1999.

²¹¹ *Computerzeitung*, 30.11.1995, p. 2.

²¹² *Roman Hummelt*, Spionage auf dem Datenhighway, Hanserverlag (1997) pp. 49 et suiv.

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.

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 chapitre 10, 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 plus qu'auparavant 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 cas²¹³:

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 chapitre 10, 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.

²¹³ 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'en 1994	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, 1/98
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.	Campbell in Stoa 1999, vol. 2/5, avec référence au Baltimore Sun, America's fortress of Spies, de Scott Shane et Tom Bowman, 3.12.1995, et au Washington Post, French Recent US Coups in New Espionage, de William Drozdiak
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. Octobre 1992
Ministère fédéral de l'économie (Allemagne)	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 (Allemagne)	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	2 Allemands en mission.	Collecte de renseignements sur les systèmes d'armes	SZ/30.5.2000:	„Anmerkungen zur Sicherheitslage der

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			technologies d'armement d'une entreprise munichoise (d'après SZ/30.5.2000: Dasa à Ottobrunn)		(blindés et DCA).	Trahison "pas très grave" du point de vue militaire. Cela s'applique également au préjudice économique, constate le tribunal.	deutschen Wirtschaft", ASW; Bonn, 2001 „Haftstrafe wegen Spionage für Russland“, 30 mai 2000
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, avril 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 (infraction au droit des brevets).	„Aktenkrieger“, SZ, 29. mars 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 août 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 pour collecte illicite d'informations touchant à des secrets d'entreprise. Selon un collaborateur de la NSA, ce qu'Enercon savait avait été communiqué à Kenetech par ECHELON.	Non précisé.	„Klettern für die Konkurrenz“, SZ 13. octobre 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 Japon	CIA	1996	Négociations relatives à des quotas d'importation de voitures américaines sur le	Piratage du système informatique du ministère japonais du commerce.	L'américain M. Kantor approuverait l'offre la plus basse.	Kantor accepte l'offre la plus basse.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			marché japonais.				Schütze, 1/98
Automobiles japonaises	Gouvernement américain	1995	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.	Duncan Campbell in STOA 2/5 (1999) avec référence au Financial Post, Canada, 28.2.1998
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 E. Schmidt-Eenboom, cité dans „Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López et 3 de ses collaborateurs	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. en 1996 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.	„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. novembre 2000 „Abgehört“, Berliner Zeitung, 22 janvier 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 juillet 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	Piratage.	Collecte de renseignements sur de nouveaux détonateurs nucléaires américains.	Aucune conséquence particulière; les pirates s'enfuient en Israël; l'un d'entre	„Maulwürfe in Nadelstreifen“, Andreas Förster, p. 137

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			l'ordinateur central du laboratoire nucléaire de Los Alamos.			eux est arrêté mais aucun lien avec les services secrets 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, p. 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 janvier 1996
Thomson-Alcatel contre 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, p. 91
Thomson-Alcatel contre 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 novembre 2000
Thomson-Alcatel contre Raytheon	NSA Ministère 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: Raytheon 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.	Duncan Campbell in STOA 2/5 de 1999 avec référence au New-York Times, How Washington Inc makes a sale de David Sanger, 19.2.1995 et http://www.raytheon.com/sivam/contract.html
Thyssen	BP	1990	Marché (plusieurs millions) 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, p. 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. août 1996
VW	Non précisé.	1996	Circuit d'essais de VW (Ehra-Lessien).	Caméra cachée.	Informations concernant les nouveaux modèles de VW.	Non précisé.	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25,

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
							11 juin 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.

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'économie après la guerre froide

Depuis 1990, le gouvernement américain tend de plus en plus à mettre sur le même plan la sécurité économique et la sécurité nationale. Le rapport annuel de la Maison blanche "National Security Strategy"²¹⁴ ne cesse de souligner que **la sécurité économique fait partie intégrante non seulement des intérêts nationaux mais aussi de la sécurité nationale.**

À l'origine de cette évolution, il y a plusieurs causes. En fait, trois facteurs ont contribué à ce qu'elle ait lieu:

- l'intérêt que les services de renseignement attachent à une mission se poursuivant après la guerre froide,
- la simple reconnaissance par le ministère américain des affaires étrangères que désormais, le rôle dirigeant des États-Unis dans le monde, la guerre froide ayant pris fin, doit se fonder non pas uniquement sur la force militaire mais aussi sur la puissance économique,
- l'intérêt attaché, en politique intérieure, par le Président Clinton, au renforcement de l'économie américaine et à la création d'emplois.

²¹⁴ Stratégie de sécurité nationale.

Cette convergence d'intérêts de l'administration américaine a eu des conséquences pratiques.

En toute logique, le FBI a, depuis 1992, concentré ses activités de contre-espionnage sur l'espionnage économique et lancé en 1994 un "Economic Counterintelligence Program", qui est, selon Freeh, directeur du FBI, devant le Parlement, un programme **défensif**. Ce programme doit empêcher que la compétitivité de l'économie américaine soit mise en danger par le vol d'informations.

Logiquement, du moins dans l'optique américaine, le gouvernement a fait appel à la CIA et, par la suite, à la NSA pour lutter contre les distorsions de concurrence par la corruption. James Woolsey, ancien directeur de la CIA, n'a laissé plané aucun doute à ce propos lors d'une conférence de presse qu'il a donnée le 7 mars 2000 à la demande du ministère américain des affaires étrangères²¹⁵.

Logiquement, le ministère américain du commerce a organisé ses activités de promotion des exportations de telle façon qu'une entreprise américaine ne se trouve en face que d'un seul interlocuteur lorsqu'elle veut exporter. En l'occurrence, toutes les possibilités du gouvernement ont été concentrées dans une perspective non seulement passive mais aussi active (pour plus de détails à ce propos, voir chapitre 10, point 10.9.4.).

10.9.1. Le défi pour le gouvernement américain: l'espionnage économique contre les entreprises américaines

Les actions de renseignement visant l'économie américaine ne sont ni inhabituelles ni nouvelles. Les États-Unis, comme d'autres grandes nations industrielles, ont été pendant des dizaines d'années la cible de l'espionnage économique. Toutefois, pendant la guerre froide, l'obtention d'informations économiques et technologiques n'était qu'une activité corollaire de l'espionnage classique. Après la fin de la guerre froide, l'espionnage économique est devenu un objectif en soi²¹⁶.

²¹⁵ State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

²¹⁶ Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Louis J. Freeh, directeur du FBI, a expliqué en 1996 dans le détail, devant le Congrès que l'économie américaine était la cible de l'espionnage économique auquel se livraient des services de renseignement d'autres pays. Il a dit, mot pour mot, que des gouvernements étrangers prenaient pour cible – et ce par différents moyens – des personnes, des firmes, des industries et le gouvernement américain lui-même pour voler ou obtenir de façon illicite des technologies, données et informations critiques, afin de procurer des avantages concurrentiels à leur propre industrie²¹⁷. Il n'empêche que le vol d'informations par les Américains progresse également de la même façon. Les autres déclarations faites par le directeur Freeh devant le parlement américain sont résumées ci-après. Votre rapporteur déplore ici que le gouvernement américain n'ait pas autorisé une délégation de la commission à s'entretenir de ces questions avec le FBI, ce qui aurait permis d'actualiser les informations. Aussi votre rapporteur part-il du principe que dans l'esprit du gouvernement américain, l'audition devant la Chambre des représentants en 1996 reflète l'état actuel de la menace que représente l'espionnage économique pour l'économie américaine, et se réfère-t-il à cette source.

10.9.1.1. Les acteurs

Au moment de l'audition, le FBI enquêtait sur des personnes ou des organisations de 23 pays soupçonnées d'espionnage économique contre les États-Unis. Si certains opposants idéologiques ou militaires des États-Unis poursuivent purement et simplement leurs activités du temps de la guerre froide²¹⁸, d'autres gouvernements pratiquent un espionnage économique et technologique, alors qu'ils sont depuis longtemps des alliés militaires et politiques des États-Unis. En l'occurrence, ils profitent souvent de leurs facilités d'accès aux informations américaines. Certains d'entre eux ont développé une infrastructure propre pour exploiter les informations concernant les technologies de pointe et les utiliser dans la concurrence avec les entreprises américaines. Concrètement, aucun pays n'est cité, ce qui n'empêche qu'il est question, en termes voilés, de la Russie, d'Israël et de la France²¹⁹.

10.9.1.2. Objectifs de l'espionnage économique

Les objectifs de l'espionnage économique que cite le FBI correspondent à ce qui est dit au chapitre 10, point 10.1.1. Toutefois, la haute technologie et l'industrie de la défense sont citées en tant qu'objectifs prioritaires. Il est intéressant de constater que sont mentionnées en tant qu'objectifs de l'espionnage économique poursuivis de façon **agressive** les informations sur des offres, des contrats, des clients et l'information stratégique dans ces secteurs²²⁰.

²¹⁷ „Consequently foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. government itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage.”

²¹⁸ „The end of the Cold War has not resulted in a peace dividend regarding economic espionage“, *Freeh*, Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996 .

²¹⁹ Interprétation par votre rapporteur des déclarations évasives faites par *Louis J. Freeh* devant la commission.

²²⁰ En la matière, l'interception des communications est une méthode pleine de promesses!

10.9.1.3. Méthodes

Dans le cadre de l'Economic Counterintelligence Program, le FBI a conçu une série de méthodes d'espionnage. La plupart du temps, différentes méthodes sont utilisées ensemble, et ce n'est que rarement qu'une seule méthode est utilisée. Le FBI convient que la meilleure source est une personne dans une entreprise ou une organisation, ce qui, en règle générale, vaut également pour des contextes autres qu'américains (cf. chapitre 10, points 10.3 et 10.4). Lors de l'audition, le FBI a fait état de l'utilisation de personnes aux fins de l'espionnage, ne disant mot – ce qui est étonnant – des méthodes électroniques.

10.9.2. Attitude du gouvernement américain face à l'espionnage économique actif

L'ancien directeur de la CIA Woolsey a, lors d'une conférence de presse²²¹ et d'un entretien avec des membres de la commission à Washington, résumé comme suit l'activité d'interception du service secret américain:

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. Interrogé à ce propos, Woolsey n'a cité aucun exemple concret.

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. Il a exclu de façon catégorique tout espionnage de concurrence pur et simple.

George J. Tenet, directeur de la CIA, s'est exprimé dans le même sens à l'occasion d'une audition devant la commission de contrôle des services secrets de la Chambre des représentants le 12 avril 2000²²²: les États-Unis n'ont ni pour politique ni pour pratique de se livrer à des activités d'espionnage pour procurer un avantage déloyal aux entreprises américaines. Au cours de la même audition, Tenet a également expliqué que lorsqu'il s'agit d'informations portant sur la corruption, ces informations sont transmises à d'autres services gouvernementaux, afin que ceux-ci puissent aider les entreprises américaines²²³. En réponse à

²²¹ James Woolsey, Remarks at the Foreign Press Center, Transskript, 7.3.2000, <http://cryptome.org/echelon-cia.htm>

²²² „It is not the policy nor the practice of the U.S. to engage in espionage that would provide an unfair advantage to U.S. Companies“

²²³ „As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense, and we never will play offense.“

une question du député Gibbons, Tenet a reconnu que l'espionnage de concurrence n'était pas interdit par la loi, faisant toutefois observer qu'il ne voyait pas la nécessité d'une telle interdiction, dès lors que les services ne se livreraient pas à ce genre d'activités.

Porter Goss, président de la commission du contrôle des services secrets de la Chambre des représentants, a, lors d'un entretien qu'il a accordé à Washington, décrit de la même façon les activités d'interception.

10.9.3. Situation juridique en matière de corruption d'agents publics²²⁴

La corruption aux fins de s'assurer des marchés n'est pas un phénomène européen mais bien mondial. Selon le Bribe Payers Index (BPI), publié en 1999 par Transparency International, qui classe les 19 principaux pays exportateurs selon leur propension à offrir des pots-de-vin, l'Allemagne et les États-Unis se partagent la neuvième place. La pratique de la corruption est jugée moindre dans le cas de la Suède, de l'Autriche, des Pays-Bas, du Royaume-Uni et de la Belgique. Seules l'Espagne, la France et l'Italie sont plus mal placées²²⁵.

Pour justifier l'espionnage économique, les Américains invoquent les pratiques de corruption des entreprises européennes. Cette approche est contestable non seulement parce que des comportements impropres isolés ne sauraient être un motif justifiant un espionnage général mais aussi et surtout parce que de telles pratiques s'apparentant à la loi du plus fort ne seraient tolérables que dans un environnement échappant au droit.

En Europe, la corruption est réprimée par la loi avec la même rigueur qu'aux États-Unis. La similitude des intérêts a conduit à l'adoption, en 1997, de la Convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales²²⁶. Cette convention oblige les États signataires à réprimer la corruption d'un agent public étranger et comporte, outre la définition du fait générateur du délit, des dispositions concernant les sanctions, la juridiction et l'exécution.

La Convention, qui est entrée en vigueur le 15 février 1999, a été transposée et ratifiée par tous les États membres de l'Union européenne, à l'exception de l'Irlande. Les États-Unis ont transposé la Convention par l'International Anti-Bribery and Fair Competition Act de 1998²²⁷ qui a adapté leur Foreign Corrupt Practices Act (FCPA) de 1977, qui fait obligation aux entreprises de tenir une comptabilité et qui interdit la corruption d'agents publics étrangers.

²²⁴ Albin Eser, Michael Überhofer, Barbara Huber (Eds), *Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz*, edition iuscrim (1997)

²²⁵ L'échelle va de 10 (taux de corruption bas) à 0 (taux de corruption élevé): Suède (8,3), Australie (8,1), Canada (8,1), Autriche (7,8), Suisse (7,7), Pays-Bas (7,4), Royaume-Uni (7,2) Belgique (6,8), Allemagne (6,2), États-Unis (6,2), Singapour (5,7), Espagne (5,3), France (5,2), Japon (5,1), Malaisie (3,9), Italie (3,7), Taïwan (3,5), Corée du Sud (3,4), Chine (3,1).

<http://www.transparency.org/documents/cpi/index.html#bpi>

²²⁶ Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales

<http://www.oecd.org/daf/nocorruption/20nov1e.htm>

²²⁷ OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, <http://www.ita.doc.gov/legal/>

Pas plus aux États-Unis que dans les États membres de l'Union européenne, les pots-de-vin payés aux agents publics étrangers ne sont regardés comme des charges déductibles²²⁸.

Alors que la convention de l'OCDE ne vise que la lutte contre la corruption d'agents publics étrangers, le Conseil de l'Europe a adopté en 1999 deux conventions plus ambitieuses, qui ne sont toutefois pas encore entrées en vigueur. La convention pénale en matière de corruption²²⁹ vise également la corruption dans le secteur privé. Si elle a été signée par tous les États membres de l'Union européenne, exception faite de l'Espagne, ainsi que par les États-Unis, elle n'a toutefois été ratifiée que par le Danemark.

La convention civile en matière de corruption²³⁰ arrête des règles dans le domaine de la responsabilité et de la réparation du préjudice, déclarant notamment nuls et non avenues les contrats et clauses contractuelles imposant le paiement de pots-de-vin. Elle a été signée par tous les États membres de l'Union européenne, hormis les Pays-Bas, le Portugal et l'Espagne. Les États-Unis ne l'ont pas signée.

Dans le cadre de l'Union européenne également, ont été adoptés deux actes concernant la lutte contre la corruption, à savoir la convention relative à la lutte contre la corruption impliquant des fonctionnaires et l'action commune relative à la corruption dans le secteur privé.

La convention relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne²³¹ a pour but de garantir que sont érigées en infractions pénales dans toute l'Union européenne la corruption passive et la corruption active de fonctionnaires. Les États membres sont tenus de sanctionner la corruption passive et la corruption active des fonctionnaires, qu'il s'agisse de l'un de leurs fonctionnaires, d'un fonctionnaire d'un autre État membre ou d'un fonctionnaire communautaire.

Par l'action commune relative à la corruption dans le secteur privé²³², il est garanti que la corruption passive et la corruption active d'entreprises sont érigées en infractions pénales. En l'occurrence, des sanctions pénales sont prévues non seulement pour les personnes physiques mais aussi pour les personnes morales. Le champ d'application de l'action commune est cependant plus limité que celui de la convention relative à la lutte contre la corruption impliquant des fonctionnaires, dans la mesure où les États membres sont tenus uniquement de sanctionner des faits commis au moins en partie sur leur territoire. Il appartient aux États membres de décider eux-mêmes si l'application des sanctions peut être étendue aux infractions commises à l'étranger par leurs propres ressortissants ou en faveur de personnes morales locales. L'Allemagne et l'Autriche ont érigé en infractions pénales les délits de

²²⁸ <http://www.oecd.org/daf/nocorruption/annex3.htm>

²²⁹ Criminal Law Convention on Corruption,
<http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01>

²³⁰ Civil Law Convention on Corruption ETS no.: 174,
<http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01>

²³¹ Convention établie sur la base de l'article K.3, paragraphe 2, point c) du traité sur l'Union européenne, relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne, JO C 195 du 25.6.1997, p. 2.

²³² Action commune du 22 décembre 1998, adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la corruption dans le secteur privé (98/742/JAI), JO L 358 du 31.12.1998, p. 2.

corruption commis à l'étranger dès lors que ceux-ci sont également punissables sur le territoire où ils ont été commis.

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

Par l'Executive Order 12870, le Président Clinton a constitué en 1993 le Trade Promotion Coordinating Committee (TPCC)²³³. Celui-ci doit coordonner le développement de la politique de promotion commerciale du gouvernement américain et concevoir une stratégie à cet effet. En vertu de l'Executive Order, un représentant du National Security Council (NSC)²³⁴ fait également partie du TPCC. Le NSC définit la politique de sécurité nationale des États-Unis en ce qui concerne tant les questions de politique intérieure, de politique étrangère et de politique militaire que les tâches des services de renseignement. Les priorités d'action du NSC se modifient en fonction des priorités fixées par le Président. Le 21 janvier 1993, le Président Clinton a élargi le NSC par le PDD2 et conféré dans le même temps davantage de poids aux questions économiques dans la formulation de la politique de sécurité. Font notamment partie du NSC le Président, le vice-président, le ministre des affaires étrangères et le ministre de la défense. Le Directeur de la CIA est membre à titre consultatif.

10.9.4.1. 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. Il représente le point de contact entre le TPCC et l'économie américaine. Créé en 1993, ce centre a, selon ses propres dires, aidé des centaines d'entreprises américaines à obtenir des marchés publics à l'étranger.

L'Advocacy Center²³⁵ aide les entreprises américaines:

- en mobilisant l'ensemble des moyens à la disposition du gouvernement américain: experts financiers et réglementaires par pays et secteur, réseau mondial des agents commerciaux, Maison blanche,
- en s'employant à homogénéiser les règles et à promouvoir une concurrence ouverte pour les appels d'offres internationaux, depuis les projets d'infrastructure portant sur plusieurs milliards de dollars jusqu'au contrat stratégique pour une petite entreprise,
- en menant des négociations au nom des entreprises américaines depuis le début jusqu'à la fin, par la voie d'un support concret,
- en soutenant l'emploi américain et en promouvant les exportations américaines en faisant en sorte que les entreprises américaines puissent s'assurer des projets et contrats outre-mer,
- en aidant les entreprises américaines confrontées à des négociations dans l'impasse par suite de l'inaction ou de la bureaucratie de gouvernements étrangers.

²³³ Archives de la Maison blanche, <http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html>.

²³⁴ Page d'accueil du National Security Council (NSC), <http://www.whitehouse.gov/nsc>.

²³⁵ Brochure du TPCC concernant l'Advocacy Center, octobre 1996.

10.9.4.2. Méthodes de travail²³⁶

Le centre n'occupe qu'un directeur et une petite équipe de 12 personnes (situation à la date du 6.2.2001). Les secteurs d'activité des responsables de projets sont la Russie et les nouveaux États indépendants; l'Afrique, l'Asie orientale et le Pacifique; le Proche-Orient et l'Afrique du Nord; l'Asie méridionale, le Bangladesh, l'Inde, le Pakistan et le Sri Lanka; l'Europe et la Turquie; la Chine, Hong-Kong et Taiwan; le Canada, les Antilles et l'Amérique latine, la construction aérienne et automobile et l'industrie de la défense dans le monde entier, les télécommunications, les technologies de l'information et l'industrie informatique dans le monde entier.

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.

10.9.4.3. Participation de la CIA aux travaux du TPCC

Duncan Campbell a présenté aux membres de la commission certains documents, qui ne sont plus considérés secrets, prouvant une participation de la CIA aux travaux de l'Advocacy Center, notamment des procès-verbaux du Trade Promotion Coordinating Committee relatifs à des réunions du groupe de travail Indonésie tenues en juillet et août 1994²³⁷. Selon les documents en question, plusieurs collaborateurs de la CIA participent à ce groupe, qui doit concevoir une stratégie commerciale à l'égard de l'Indonésie. Ces collaborateurs sont nommément désignés dans les procès-verbaux.

De plus, il ressort des procès-verbaux que l'un des collaborateurs de la CIA estime que l'un des objectifs du groupe consiste à déterminer les concurrents principaux et à communiquer aux entreprises cette information de base²³⁸.

²³⁶ Page d'accueil de l'Advocacy Center, <http://www.ita.doc.gov/td/advocacy/>.

²³⁷ TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, procès-verbal de la réunion du 17.8.1994, dossier de l'U.S. & Foreign Commercial Service du 25.8.1994.

²³⁸ *ibidem*: "Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information", Bob Beamer est l'un des représentants de la CIA .

10.9.4.4. Questions sans réponse

Le gouvernement américain n'a pas autorisé les entretiens que les membres de la commission souhaitaient avoir avec le Centre, lequel avait marqué son accord à cet effet. Deux questions qui suscitent des doutes n'ont donc pu être tirées au clair, ce que déplore votre rapporteur:

- a) la commission dispose de documents (cf. chapitre 10, point 10.9.4.3.) qui établissent une participation de la CIA aux activités du TPCC,
- b) dans les brochures d'information qu'il publie lui-même (citées précédemment), l'Advocacy Center indique qu'il mobilise les ressources de 19 "government agencies" des États-Unis. En d'autres endroits des brochures, il n'est fait état que de 18 agences. Pourquoi le nom de la dix-neuvième ne peut-il être rendu public?

Pour votre rapporteur, le refus d'autoriser les entretiens convenus avec l'Advocacy Center signifie qu'y ont lieu des activités dont le gouvernement américain ne souhaite pas parler.

10.10. Sécurité des réseaux informatiques

10.10.1. Importance du présent chapitre

Comme il a déjà été dit au chapitre 10, point 10.4, le piratage de réseaux informatiques ou le vols des données contenues dans les ordinateurs portables constitue actuellement la technique d'espionnage économique la plus efficace après l'utilisation d'espions. Les commentaires du présent chapitre n'ont pas directement trait à un système d'interception des communications internationales organisé à l'échelle mondiale. Compte tenu des objectifs de la commission, il n'est pas possible de renoncer dans le chapitre consacré à l'espionnage économique à un bref aperçu de l'un de ses instruments les plus efficaces. Une telle démarche est sans conteste utile pour juger de l'importance que revêt un système d'interception des communications internationales dans le contexte de l'espionnage économique.

10.10.2. Risque inhérent à l'utilisation de la technologie de l'information moderne dans les milieux économiques

Le traitement électronique des données a, depuis longtemps, envahi le monde économique. Des données de toutes sortes sont mémorisées de façon très compacte sur différents supports. Les données informatisées sont désormais l'un des principaux facteurs du savoir-faire des entreprises. S'il ouvre de nouvelles perspectives, le passage de la société industrielle à la société de l'information entraîne aussi des risques considérables sur le plan de la sécurité²³⁹.

²³⁹ Computerspionage, Dokumentation Nr. 44, Bundesministerium für Wirtschaft, juillet 1998.

10.10.2.1. Augmentation des risques

En résumé, les nouveaux risques apparaissant peuvent être décrits comme suit²⁴⁰:

De plus en plus d'entreprises sont en réseau et les informations toujours plus nombreuses qui sont compactées en un endroit peuvent facilement être recopiées par des pirates informatiques. Parallèlement, d'autres données sensibles sont décentralisées, ce qui rend difficile une gestion centrale de la sécurité. La mobilité des décideurs, qui emportent sur leurs ordinateurs portables des informations sensibles est à l'origine de risques supplémentaires. L'externalisation de services entraîne des transferts d'activités d'entretien, y compris dans le secteur des technologies de l'information, dont il conviendrait, du point de vue de la sécurité, de s'abstenir. L'importance relative attachée à la sécurité par la hiérarchie de l'entreprise entraîne, en combinaison avec les connaissances insuffisantes des décideurs en matière de sécurité, des décisions malheureuses.

10.10.2.2. Analyse détaillée des risques

Compression de l'information sur des supports compacts

De nos jours, les secrets des entreprises sont mémorisés de façon extrêmement concentrée sur des supports comprimés. Ainsi, il est possible de faire sortir d'une entreprise les plans complets d'une nouvelle unité sur un disque de la taille d'un paquet de cigarettes ou de l'extraire électroniquement, rapidement et sans trace, en piratant un réseau informatique.

Décentralisation des informations secrètes

À l'époque des gros ordinateurs, le contrôle de l'accès aux informations secrètes pouvait se concevoir simplement, dans la mesure où il ne fallait gérer qu'un seul ordinateur. Aujourd'hui, chaque utilisateur connecté au réseau dispose de capacités informatiques considérables à son poste de travail. S'il s'agit naturellement là pour l'utilisateur d'un avantage considérable, c'est aussi un désastre du point de vue de la sécurité.

Simplification du copiage des informations

À l'époque des plans dessinés à la main et des machines à écrire mécaniques, il était très difficile de copier de nombreux documents sans risquer d'être découvert. Aujourd'hui, à l'époque électronique, cela ne pose pas de problème. Les informations numériques peuvent être reproduites en quantité, facilement, rapidement et sans trace. Ainsi, l'acquisition du matériau souhaité ne nécessite souvent qu'une seule intervention. Le risque de découverte diminue donc de façon notable.

²⁴⁰ *Roman Hummelt, Wirtschaftsspionage auf dem Datenhighway, Hanser Verlag, Munich 1997.*

Mobilité des décideurs

Les décideurs d'une entreprise emportent, souvent sans en être suffisamment conscients, sur leurs ordinateurs portables des informations d'importance stratégique pour l'entreprise. Dès lors qu'un disque dur peut être copié rapidement lors d'un "contrôle douanier" ou à l'occasion de la fouille d'une chambre d'hôtel, les possibilités des service de renseignement sont considérables. Autre risque: le vol, pur et simple, du carnet électronique. Par ailleurs, il est difficile, compte tenu de la décentralisation, d'intégrer dans une gestion centrale de la sécurité les contenus des disques durs des ordinateurs portables des décideurs d'une entreprise.

Externalisation de l'entretien

L'externalisation peut permettre à une entreprise de réduire ses coûts. Elle a cependant aussi pour effet, dans le domaine de la technologie de l'information et de l'entretien des installations téléphoniques, de donner à des techniciens extérieurs à l'entreprise accès à pratiquement toutes les informations. On ne saurait souligner suffisamment les risques qui en résultent.

Insuffisance de la gestion des réseaux

Parallèlement aux failles de sécurité du logiciel lui-même, que les pirates informatiques s'emploient en permanence à découvrir, le principal danger procède des administrateurs des réseaux, qui sont insuffisamment conscients des risques. Dans sa version de base, Windows NT est configuré de telle façon qu'il permet de découvrir quasiment toutes les informations sur le réseau, qui sont nécessaires pour réussir un piratage²⁴¹. Si ces configurations et les mots de passe standard ne sont pas modifiés, l'accès au réseau est un jeu d'enfant. Une erreur répandue consiste également à consentir des dépenses importantes pour la sécurité de la cloison coupe-feu, sans protéger comme il se doit le réseau contre une attaque de l'intérieur²⁴².

10.10.3. Fréquence des attaques contre les réseaux

Le nombre des attaques contre les réseaux informatiques d'Internet augmente d'année en année²⁴³. Selon le Computer Emergency Response Team (CERT), organisation créée aux États-Unis en 1988 pour assurer la sécurité sur Internet, 132 incidents de sécurité ont été notifiés en 1989. En 1994, leur nombre était déjà passé à 2 241 et il atteignait, en 1996, 2 573. En l'occurrence, la zone d'ombre est extrêmement importante. Cette thèse est confirmée par une simulation à grande échelle réalisée sur ses propres ordinateurs par le ministère américain de la défense. On a tenté, de façon systématique, de pénétrer de l'extérieur dans 8 932 serveurs et unités centrales. Pour 7 860 systèmes, ces essais ont été fructueux, les essais n'étant découverts que 390 cas et notifiés que dans 19. On fait la distinction entre les attaques et les incidents de sécurité. Une attaque est une tentative isolée d'obtenir un accès sans autorisation à un système. Un incident de sécurité consiste en un certain nombre d'attaques conjointes. En extrapolant pour l'ensemble du réseau internet les résultats d'études portant sur une longue période, réalisées par le Pentagone et certaines universités américaines, il est

²⁴¹ George Kurtz, Stuart McClure, Joel Scambray, *Hacking exposed*, Osborne/McGraw-Hill (2000), 94.

²⁴² Martin Kuppinger, *Internet- und Intranetsicherheit*, Microsoft Press Deutschland (1998), 60.

²⁴³ Othmar Kyas, *Sicherheit im Internet*, International Thomson Publishing (1998), 23.

possible d'estimer les incidents de sécurité et les attaques sur Internet à respectivement 20 000 et 2 millions par an.

10.10.4. Acteurs et méthodes

Les services de renseignement étrangers qui attaquent les systèmes TI visent à parvenir, si possible sans se faire remarquer, aux informations qui y sont contenues. En principe, il est possible de distinguer trois groupes d'acteurs et trois modes d'opération différents.

Acteurs internes avec droit d'accès général

Un espion introduit ou acheté qui arrive à occuper une fonction de gestionnaire de systèmes ou d'administrateur de la sécurité dans un centre informatique ne doit, pour exercer son activité d'espionnage et s'appropriier quasiment l'ensemble du savoir-faire de son employeur, qu'utiliser les pouvoirs qui lui sont officiellement conférés. Il en va de même pour un ingénieur de développement dirigeant ayant un accès illimité à toutes les bases de données techniques de l'entreprise.

L'efficacité d'un tel espion est maximale. Il est toutefois exposé, en cas de suspicion, à un risque de découverte important, dès lors que les enquêtes se concentreront immédiatement sur le petit cercle de personnes ayant un accès général aux informations. De plus, il n'existe aucun moyen permettant de mettre un espion dans une situation lui garantissant un accès général; le hasard est le seul maître en l'occurrence.

Acteurs intérieurs avec droit d'accès localisé

Par rapport au pirate informatique qui agit de l'extérieur, un espion travaillant dans l'entreprise dispose d'un net avantage: il lui faut simplement vaincre l'obstacle de la sécurité du réseau et il n'est pas confronté en outre à une cloison coupe-feu. Depuis un poste de travail isolé, il est possible d'établir l'architecture du réseau, à condition de disposer des connaissances voulues, en utilisant les techniques des pirates informatiques extérieurs et les autres techniques accessibles aux personnes travaillant dans l'entreprise, et d'obtenir des informations considérables²⁴⁴. À cela s'ajoute que l'espion peut communiquer, sans éveiller le soupçon, avec d'autres membres de l'entreprise et que ce qu'il est convenu d'appeler le "social engineering" permet d'obtenir des mots de passe.

Si elle peut être grande, l'efficacité d'un tel espion ne saurait toutefois être aussi prévisible que dans le premier cas. Le risque de découverte est réduit, en particulier dans les réseaux où l'administrateur n'attache pas une importance suffisante à la possibilité d'une attaque interne. L'infiltration d'un espion ayant une formation technique lui permettant de pénétrer les réseaux informatiques est beaucoup plus simple (stagiaires, chercheurs extérieurs, etc.).

²⁴⁴ *Anonymus*, Hacker's guide, Markt & Technik-Verlag (1999)

10.10.5. Piratage de l'extérieur

Il est connu et prouvé que des pirates informatiques ne cessent de pénétrer de l'extérieur dans les réseaux informatiques. Désormais, les services de renseignement forment également des spécialistes pour cela. L'efficacité d'une attaque par un pirate n'est ni prévisible ni planifiable; elle est fonction dans une grande mesure de la qualité de l'organisation de la défense et du fait, par exemple, que le réseau du département de recherche soit ou non matériellement connecté à Internet. Le risque pour l'espion professionnel est proche de zéro, même si l'attaque en tant que telle est découverte, car il ne doit pas être sur place pour agir.

10.11. Sous-estimation des risques

10.11.1. Conscience des risques dans les milieux économiques

La conscience du risque que représente l'espionnage économique n'est, jusqu'ici, pas très développée dans les milieux économiques. La preuve en est notamment donnée par le fait que souvent, les responsables de la sécurité font partie des cadres moyens et non de la direction de l'entreprise. La sécurité coûte cher, et les membres du comité de direction ne s'occupent la plupart du temps des questions de sécurité que lorsqu'il est trop tard.

Les grandes entreprises ont toutefois leurs propres services de sécurité ainsi que des spécialistes dans le domaine des TI. Par contre, les petites et moyennes entreprises ne disposent que très rarement d'experts en sécurité, et la plupart du temps, elles sont déjà bien contentes lorsque l'équipement informatique fonctionne tout simplement. Il n'empêche que de telles entreprises peuvent également être la cible de l'espionnage économique, dès lors qu'elles sont parfois très innovantes. De plus, les moyennes entreprises sous-traitantes sont, compte tenu de leur intégration dans le processus de production, de bonnes bases de départ pour des attaques sur les grandes entreprises.

10.11.2. Conscience du risque dans les milieux scientifiques

En règle générale, les chercheurs ne s'intéressent qu'à leur propre domaine spécialisé. Aussi sont-ils souvent une proie facile pour les services de renseignement. Votre rapporteur a appris, non sans un certain étonnement, que des instituts dont les activités s'orientent nettement sur la recherche appliquée, communiquent en clair par le courrier électronique et le réseau scientifique. C'est là de la folie pure et simple.

10.11.3. Conscience du risque dans les institutions européennes

10.11.3.1. Banque centrale européenne

Les informations concernant l'élaboration des décisions de la Banque centrale européenne pourraient revêtir une grande importance pour les services de renseignement. Que les marchés pourraient manifester un net intérêt en la matière, voilà qui se comprendrait naturellement. Au cours d'une réunion à huis clos, la commission a également entendu des représentants de la Banque centrale européenne au sujet des mesures de sécurité prises pour protéger les informations. Votre rapporteur a ainsi acquis le sentiment que la conscience du risque existait et que toutes les mesures de sécurité possibles étaient prises. Il dispose cependant d'informations²⁴⁵ selon lesquelles la conscience du risque n'est pas aussi développée dans de nombreuses banques centrales nationales.

10.11.3.2. Conseil de l'Union européenne

Avant la désignation du Haut responsable pour la politique étrangère et de sécurité, le Conseil avait essentiellement axé ses efforts en matière de confidentialité sur la volonté de cacher au public et au Parlement européen le déroulement du processus de décision et l'attitude des gouvernements des États membres. Il n'aurait jamais pu se prémunir contre une opération de renseignement menée par des professionnels²⁴⁶, dès lors, par exemple, que l'entretien des équipements techniques des cabines d'interprétation est confié à une firme israélienne. Le Conseil a désormais adopté des règles de sécurité²⁴⁷ conformes aux normes de l'OTAN.

10.11.3.3. Parlement européen

N'ayant pas jusqu'ici eu à s'occuper de documents confidentiels, le Parlement européen n'a, en matière de protection du secret, ni une expérience ni une philosophie de sécurité. La nécessité ne s'en fera sentir qu'à partir du moment où le Parlement aura accès à des documents secrets. Dans tous les autres cas, il ne convient pas qu'une représentation démocratique, qui doit être aussi transparente que possible, se dote d'une politique générale du secret. Toutefois, il conviendrait, ne serait-ce que dans l'intérêt de la protection des informateurs et pétitionnaires, de pouvoir crypter, si besoin, le courrier électronique entre les différents bureaux de députés. Jusqu'ici, ce n'est pas possible.

²⁴⁵ Communication privée, source protégée.

²⁴⁶ Communication de membres du COREPER et de fonctionnaires du Conseil, sources protégées.

²⁴⁷ Décision du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil, JO L 101 du 11.4.2001, pp. 1 et ss.

10.11.3.4. Commission européenne

À la Commission européenne, il existe des directions générales où, compte tenu de la nature des informations traitées, la confidentialité et la protection ne sont pas nécessaires. Bien au contraire, il convient qu'une transparence absolue soit la règle dans tous les domaines ayant trait avec la législation. Le Parlement européen devrait veiller à ce que, dans ces domaines, des règles de confidentialité hors de propos ne viennent inutilement masquer encore plus qu'aujourd'hui l'influence qu'exercent des firmes intéressées et d'autres tiers sur les propositions législatives.

Il existe toutefois également des secteurs de la Commission où des informations sensibles circulent. Il s'agit en particulier, outre Euratom, des relations extérieures, du commerce extérieur et de la concurrence. Sur la base des informations que la commission a obtenues des directions générales concernées à l'occasion d'une réunion à huis clos, et surtout d'autres informations en possession de votre rapporteur, il semble bien que l'on puisse véritablement douter de l'existence d'une conscience du risque que représente l'espionnage et d'une approche professionnelle de la sécurité au sein de la Commission européenne. Dans un rapport public, il ne convient pas, naturellement, de mettre en évidence les failles en matière de sécurité. Votre rapporteur estime néanmoins impérieux que le Parlement européen attache sans tarder toute l'attention voulue à cette question.

Aujourd'hui déjà, il est toutefois possible de constater que les systèmes de cryptage que la Commission utilise pour certaines parties de ses communications avec ses bureaux extérieurs sont surannés. Cela ne signifie pas que le niveau de sécurité soit mauvais. Les appareils utilisés ne sont toutefois plus produits et la moitié seulement des bureaux extérieurs disposent de possibilités de cryptage. Il est nécessaire de mettre en place d'urgence un nouveau système fonctionnant sur la base de courrier électronique crypté.

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 employées²⁴⁸.

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.

²⁴⁸ 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 qu'il est breveté. 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 **ECHELON** 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 (**brute force attack**) 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)²⁴⁹. 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.

²⁴⁹ *Otto Leiberich, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, juin 1999, pp. 26 et ss.*

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 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 mondiale²⁵⁰ 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 mathématiquement²⁵¹.

L'inconvénient du système tient au fait qu'il n'est pas facile de produire de grandes quantités de telles clés aléatoires²⁵² 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 ENIGMA²⁵³, employée par l'Allemagne durant la deuxième guerre mondiale. L'armée de spécialistes du décryptage en activité à 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.

²⁵⁰ Introduit par le major Joseph Mauborgne, chef du service cryptographique de l'armée américaine. Voir *Simon Singh, Geheime Botschaften*, Carl Hanser Verlag (1999), 151.

²⁵¹ *Simon Singh, Geheime Botschaften*, Carl Hanser Verlag (1999), 151 et ss.

²⁵² *Reinhard Wobst, Abenteuer Kryptologie²*, Adison-Wesley (1998), 60.

²⁵³ 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.

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.

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 ASCII²⁵⁴ qui s'est imposée: chaque lettre est représentée par une combinaison à 6 chiffres de 0 et de 1²⁵⁵. 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 0 ($0+0=0$ 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

²⁵⁴ American Standard Code for Information Interchange.

²⁵⁵ A = 1000001, B = 1000010, C = 1000011, D = 1000100, E = 1000101, etc.

nombre des clés possibles à 100 000 000 000 000 000²⁵⁶. 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 américaine²⁵⁷. 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 européenne²⁵⁸, conçue sous le nom Rijndael à Louvain, 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.

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 transmise²⁵⁹. 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'ouvrir²⁶⁰. 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

²⁵⁶ Ce nombre, sous forme binaire, compte 56 zéros et uns. Singh, *Geheime Botschaften*, Carl Hanser Verlag (1999), 303.

²⁵⁷ *Simon Singh*, *Geheime Botschaften*, Carl Hanser Verlag (1999), pp. 302 et ss.

²⁵⁸ Définie par deux cryptographes belges de l'Université catholique de Louvain, Joan Daemen et Vincent Rijmen.

²⁵⁹ L'idée du cryptage asymétrique (public–key) est due à Whitfield Diffie et Martin Hellmann.

²⁶⁰ *Simon Singh*, *Geheime Botschaften*, Carl Hanser Verlag (1999), p. 327.

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 massifs²⁶¹. Nombreux sont ceux qui affirment au contraire que le problème est impossible à résoudre, mais cela n'a pas encore été prouvé²⁶².

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 particuliers²⁶³. 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.

²⁶¹ Johannes Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2 1999, pp. 6 et ss.

²⁶² Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 335 et ss.

²⁶³ Pour des informations sur le logiciel: voir www.pgpi.com.

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 succès²⁶⁴.

11.4 Sécurité des produits de cryptage

Dans le débat sur la sécurité réelle du cryptage, est sans cesse soulevé le problème que les 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 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.

²⁶⁴ Voir *Reinhard Wobst*, *Abenteuer Kryptographie²*, Addison-Wesley (1998), pp.234 et ss.

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 actuelle²⁶⁵

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

²⁶⁵ Charles Grant, *Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence?* 4.2000, Centre for European Reform

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 pratiques

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 financiers

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 UKUSA) 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. Conclusions

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

L'existence d'un système mondial d'écoutes 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 peut être admis, eu égard aux indices disponibles et aux nombreuses déclarations concordantes émanant de milieux très divers, parmi lesquels des sources américaines, que pendant un certain temps du moins, le système - ou des parties de celui-ci - a porté le nom de code ECHELON. Ce qui compte, c'est qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires.

L'analyse a montré que les possibilités techniques de ce système ne sont pas aussi grandes que ce que nombre de médias supposent. Néanmoins, il est inquiétant de constater que de nombreux responsables de la Communauté qui ont été entendus - notamment des membres de la Commission - ont déclaré n'avoir aucune connaissance de ce système.

Limites du système

Le système de surveillance repose principalement sur l'interception mondiale 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 UKUSA n'ont accès qu'à une partie très restreinte des communications par câble ou par radio et qu'en raison du personnel nécessaire, une partie plus limitée encore des communications peut être exploitée. Quelle que puisse être l'ampleur des moyens et capacités d'interception des communications disponibles, il est établi que le nombre extrêmement important des communications empêche, dans la pratique, un contrôle total et minutieux de l'ensemble des communications.

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. Possédant des territoires outre mer, la France serait le seul État membre de l'UE, en mesure, géographiquement et techniquement, d'exploiter à elle seule un système d'écoute mondial. Il ressort de nombreux indices que la Russie exploite également 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.

Lors de sa réunion du 30 mars 2000, le Conseil a clairement déclaré qu'il ne saurait accepter la création ou l'existence d'un système d'interception qui ne respecte pas les règles de droit des États membres et qui viole les principes fondamentaux visant à préserver la dignité humaine.

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, et qu'elles définissent 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, en sorte qu'il ne suffît pas qu'elles soient simplement opportunes ou souhaitables.

Un système de renseignements qui intercepterait, sans distinction et en permanence, les communications constituerait une violation du principe de proportionnalité et serait, partant, contraire à la CEDH. 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 énoncés dans la CEDH. Même si les États-Unis ne sont pas partie à la convention, 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.

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 et autorités policières dans le cadre de la CJAI, 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. Les services de renseignement des États-Unis ne se contentent toutefois pas de s'occuper de problèmes économiques généraux. Au motif de lutter contre les tentatives de corruption, ils interceptent également les communications des entreprises, et ce précisément dans le contexte de la passation des marchés. Une telle interception circonstanciée ne va cependant pas sans faire naître le risque de voir les informations détenues être utilisées aux fins non pas de la lutte contre la corruption mais bien de l'espionnage de concurrence, même si les États-Unis et le Royaume-Uni affirment qu'ils n'agissent pas ainsi. Dans ce contexte, il convient de faire observer que le rôle de l'Advocacy Center du ministère américain du commerce n'est toujours pas entièrement clair et qu'une rencontre convenue avec lui, qui aurait servi à clarifier les choses, a été décommandée par lui. Il y a également lieu de rappeler qu'en 1997 a été adoptée, dans le cadre de l'OCDE, une convention relative à la lutte contre la corruption des agents publics qui érige, à l'échelle internationale, les faits de corruption en infractions pénales. Ainsi, la corruption dans des cas d'espèce ne saurait-elle davantage justifier l'interception des communications.

En tout état de cause, il faut dire clairement qu'il n'est pas possible de tolérer une situation dans laquelle des services de renseignement sont utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales. Il n'existe toutefois aucun cas dans lequel il est prouvé que le système d'interception mondial faisant l'objet du présent rapport est utilisé à cette fin, contrairement à ce qui est souvent avancé.

En fait, les données sensibles se trouvent principalement à l'intérieur des entreprises de sorte que l'espionnage de concurrence consiste principalement à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées et de plus en plus souvent 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 surveillance des communications peut être utilisé pour espionner. Trois cas se présentent:

- 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, infrastructures de télécommunications, construction de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place.

Dans les petites et moyennes entreprises, la conscience du risque et du besoin de sécurité est malheureusement souvent insuffisante, et il est fréquent que le risque d'espionnage économique et d'interception des communications ne soit pas perçu. Dès lors qu'au sein des institutions européennes (à l'exception de la Banque centrale européenne et des directions générales "Relations extérieures" du Conseil et de la Commission), le sens de la sécurité n'est pas toujours très développé, il convient d'agir sans tarder.

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

En décembre 1999, le Conseil européen a décidé, à Helsinki, de se doter d'une capacité militaire européenne plus efficace afin de pouvoir s'acquitter de l'ensemble des missions de Petersberg dans le contexte de la PESC. Pour atteindre cet objectif, l'Union européenne devra être en mesure, d'ici 2003, de déployer rapidement des forces militaires d'environ 50 000 à 60 000 personnes, qui seraient autonomes, disposant des capacités de commandement, de contrôle et de renseignement nécessaires. Les premiers pas dans la voie de la mise en place de telles capacités de renseignement ont déjà été franchis dans le cadre de l'UEO et du comité politique et de sécurité permanent.

Une coopération entre services de renseignements de l'UE apparaît indispensable 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 naturellement être assuré. Le Parlement européen est sur le point de transposer le règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, et d'adapter son règlement en ce qui concerne l'accès aux documents sensibles.

13.2. Recommandations

Lutte contre l'espionnage économique

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

1. le Secrétaire général du Conseil de l'Europe est invité à soumettre au comité des ministres une proposition d'adaptation de la protection de la vie privée 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 de l'Union européenne sont invités à mettre en place une plateforme européenne composée de représentants des organismes nationaux chargés de contrôler le bilan des États membres en matière de droits fondamentaux et de droits des citoyens afin de vérifier si les dispositions nationales régissant les services de renseignement sont compatibles avec la CEDH et avec la charte des droits fondamentaux de l'UE, plateforme qui serait également appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications. De plus, les États membres devraient se voir soumettre une recommandation relative à l'élaboration d'un code de conduite 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. les États membres sont invités à adopter, lors de la prochaine conférence intergouvernementale, la Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux, notamment en ce qui concerne la vie privée; les institutions européennes sont invitées, dans le cadre de leur sphère de compétence et d'action respective, à mettre en application les droits fondamentaux établis par la Charte;
5. l'Union européenne et les États-Unis sont invités à conclure une convention établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises;

6. les États membres sont invités à conclure avec les pays tiers une convention visant à renforcer la protection de la vie privée des citoyens de l'Union, convention dans laquelle toutes les parties s'engagent à ce que, en cas d'interception pratiquée par l'une d'entre elles dans un autre pays signataire, la première informe ce dernier des actions envisagées;
7. 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;
8. 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;
9. le Conseil et les États membres sont instamment invités à se doter d'un système de contrôle démocratique de la capacité de renseignement européenne autonome ainsi que des autres activités de renseignement connexes au niveau européen, étant entendu que le Parlement européen doit jouer un rôle important dans ce système de contrôle;

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

10. les États membres sont instamment invités à vérifier la conformité aux droits fondamentaux, tels qu'ils sont définis dans la convention relative aux droits de l'homme et dans la jurisprudence de la Cour des droits de l'homme, de leur législation relative aux activités des services de renseignements et, au besoin, à lui apporter les adaptations nécessaires, ainsi qu'à reconnaître à tous les citoyens européens les mêmes garanties légales en ce qui concerne la protection de la vie privée et la confidentialité de la correspondance, étant entendu que si leurs lois relatives au pouvoir d'interception des services secrets établissent des discriminations, celles-ci doivent être supprimées;
11. les États membres sont invités à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements et à élaborer à cet effet un code de conduite qui se fonde sur le 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, un code de conduite analogue devant également être négocié avec les États-Unis;
12. les États membres sont invités à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission;

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

13. 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; les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande sont invités à se joindre à cette initiative;
14. les États membres sont invités à s'engager, sans réserve, à ne pas pratiquer, directement ou sous couvert, l'espionnage économique à l'encontre d'une puissance étrangère sur leur territoire et à ne pas autoriser, une puissance étrangère à le faire sur leur territoire, afin de respecter l'esprit et la lettre du traité CE;
15. les États membres et le gouvernement des États-Unis sont invités à nouer un dialogue franc sur la collecte de renseignements économiques;
16. les autorités du Royaume-Uni sont invitées à faire la lumière sur leur rôle dans l'alliance UKUSA étant donné que sont établies l'existence d'un système de type Échelon et son utilisation aux fins de collecte de renseignements économiques;
17. les États membres sont invités à s'assurer que leurs dispositifs de renseignements ne sont pas utilisés abusivement pour collecter des renseignements dans le cadre de la concurrence, au mépris de l'obligation de loyauté des États membres ainsi que de l'idée d'un marché unique fondé sur la libre concurrence;

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

18. les États membres sont invités à garantir un contrôle parlementaire et judiciaire approprié de leurs services secrets; les parlements nationaux qui ne disposeraient pas d'organe de contrôle parlementaire des services de renseignements sont invités à se doter d'un tel organe;
19. 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;
20. 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;
21. 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

22. la Commission et les États membres sont invités à informer les citoyens et les entreprises qu'il est possible que leurs communications internationales soient, dans certaines circonstances, interceptées, cette information devant être assortie d'une assistance pratique en matière de conception et de mise en œuvre de mesures de protection globales, incluant la sécurité des techniques d'information;
23. la Commission, le Conseil et les États membres sont invités à élaborer et à appliquer une politique efficace et active en matière de sécurité de la société de l'information, étant entendu qu'une attention particulière doit être accordée à la sensibilisation de tous les utilisateurs des systèmes de communication modernes en ce qui concerne la protection des informations confidentielles, et qu'un réseau européen coordonné d'organismes capables de fournir une assistance pratique en matière de conception et de mise en œuvre de stratégies de protection globale doit être mis en place ;
24. 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;
25. 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"); la Commission est invitée à définir une norme du niveau de sécurité des logiciels destinés à l'échange de correspondances électroniques en plaçant les logiciels dont le code source n'est pas publié dans la catégorie la moins fiable;
26. 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 les mesures de renforcement de la sécurité dans les institutions

27. les institutions communautaires et les administrations publiques des États membres sont invitées à prévoir la formation de leur personnel et la familiarisation de celui-ci avec les nouvelles techniques de cryptage en organisant les stages et les cours de formation nécessaires;
28. la Commission est invitée à faire réaliser une analyse de sécurité destinée à préciser ce qui doit être protégé et à faire élaborer un schéma de protection;
29. la Commission est invitée à actualiser son système de cryptage, une modernisation s'imposant d'urgence, et l'autorité budgétaire (Conseil et Parlement) est invitée à prévoir les moyens financiers à cette fin;

30. la commission compétente est invitée à élaborer un rapport d'initiative sur la sécurité et la protection du secret dans les institutions européennes;
31. la Commission est invitée à assurer la protection des données dans le contexte du traitement interne et à renforcer la protection des documents non accessibles au public;
32. la Commission et les États membres sont invités à investir, dans le cadre du sixième programme cadre de recherche, dans les nouvelles techniques de cryptage et dans la recherche dans le domaine de la protection contre les tentatives de décryptage;

en ce qui concerne d'autres démarches

33. 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;
34. la Commission est invitée à proposer la création, en coopération étroite avec les entreprises et les États membres, d'un réseau européen et coordonné de centres de conseil, notamment dans les États membres qui ne possèdent pas de tels organes, en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;
35. la Commission est invitée à attacher une attention particulière à la situation des pays candidats en matière de sécurité, étant entendu que ceux-ci devraient être aidés s'ils ne sont pas en mesure de se doter des moyens de protection nécessaires faute d'indépendance technologique;
36. 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.

PARLEMENT EUROPÉEN

1999



2004

Document de séance

FINAL
A5-0264/2001
Par2

11 juillet 2001

RAPPORT

sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)
(2001/2098(INI))

Partie 2: Avis minoritaires
Annexes

Commission temporaire sur le système d'interception ECHELON

Rapporteur: Gerhard Schmid

SOMMAIRE

	Page
AVIS MINORITAIRE de Giuseppe Di Lello Finuoli, Pernille Frahm et Alain Krivine	4
AVIS MINORITAIRE de Patricia McKenna et Ilka Schröder	5
AVIS MINORITAIRE de Jean-Charles Marchiani	6
AVIS MINORITAIRE de Maurizio Turco	7
Annexe I: Liste des experts qui ont fourni des informations en commission	8
Annexe II: Sources documentaires	11
Annexe III: Interception des communications aux fins de poursuites pénales: définitions et commentaires	17
1. Remarques liminaires	17
2. Délimitation: interception des communications à des fins pénales/ à des fins de renseignement	17
3. Interception des communications à des fins pénales: travaux dans l'Union européenne	18
3.1 Généralités	18
3.2 Limitation de la compétence de l'UE aux réglementations techniques	18
3.3 Travaux et actes juridiques dans le domaine de l'interception des télécommunications	19
4. Travaux transfrontières dans le domaine de l'interception des télécommunications: définitions et commentaires	21
Annexe IV:	23

**AVIS MINORITAIRE de Giuseppe Di Lello Finuoli, Pernille Frahm
et Alain Krivine**

Le rapport de la Commission affirme l'existence du système d'interception Echelon géré par différents Etats, parmi lesquels le Royaume Uni, Etat membre de l'Union européenne, avec la collaboration de l'Allemagne.

Un tel système d'interception indifférencié de communications, de données et documents viole le droit fondamental au respect de la vie privée garanti par les articles 8 de la Convention européenne des droits de l'Homme, et 6 du Traité de l'Union européenne.

Ce système viole donc de manière flagrante les libertés des citoyens européens, la logique du libre marché et la sécurité de l'Union ; quelle que soit notre appréciation ou opposition à ces logiques et à ces Traités, ces violations sont inacceptables.

Dans ses conclusions, le rapport aurait dû demander au Royaume Uni de se dissocier du système Echelon et à l'Allemagne de fermer la base d'écoutes située sur son territoire. On ne peut que regretter que l'Union européenne soit plus préoccupée par l'espionnage industriel que par les écoutes individuelles.

AVIS MINORITAIRE de Patricia McKenna et Ilka Schröder

En soulignant qu'ECHELON existe bel et bien, le présent rapport fait mouche. Mais il s'arrête au moment d'en tirer les conséquences politiques. Critiquer les interceptions pratiquées dans le cadre d'ECHELON, tout en participant à des projets visant à la création d'un service secret européen, voilà qui, de la part du Parlement européen, est bien hypocrite.

À l'échelle mondiale, il n'existe aucun mécanisme efficace de contrôle public des services secrets et de leurs pratiques antidémocratiques. Par nature, les services secrets ne peuvent être contrôlés. Ils doivent donc être supprimés. Le présent rapport sert à légitimer un service secret européen qui portera atteinte aux droits fondamentaux, tout comme le fait ECHELON.

La majorité du Parlement voit surtout une industrie dont l'espionnage industriel menacerait les profits. Or, la question vitale, c'est que les communications confidentielles sur longue distance sont devenues chose impossible. L'espionnage politique est une menace autrement plus grave que l'espionnage économique.

Outre qu'il minimise constamment les dangers qu'ECHELON présente à cet égard, le présent rapport passe sous silence les projets ENFOPOL d'interception dans l'Union européenne. Toute société est confrontée à ce choix fondamental: accepter ou refuser un contrôle permanent. En adoptant le présent rapport, le Parlement européen démontre qu'il ne se préoccupe pas de la sauvegarde des droits de l'homme et des libertés des citoyens.

AVIS MINORITAIRE de Jean-Charles Marchiani

C'est sans surprise que le groupe UEN a pris acte des résultats du vote sur le rapport de Monsieur Schmid, initialement censé concerner le système d'espionnage anglo-saxon Echelon.

La majorité de ce Parlement avait dès l'origine indiqué clairement ses intentions, en préférant cette commission ad hoc à l'instauration d'une véritable commission d'enquête. Elle n'avait alors plus rien à craindre de travaux où l'efficacité du rapporteur à faire systématiquement diversion n'était en rien menacée par un cartel de mécontents aux motivations trop disparates.

Notre message, lui, est limpide : les efforts de Monsieur Schmid n'ont pu occulter l'évidence de l'existence du système ECHELON, ni celle de l'implication active ou passive de plusieurs Etats membres.

Dès lors est constituée une sérieuse infraction aux principes des Traités qui aurait dû appeler à des sanctions ou, à tout le moins, à des mesures susceptibles d'éviter la subordination de la solidarité intra-européenne aux impératifs de la solidarité anglo-saxonne.

Le lourd rapport de Monsieur Schmid est riche d'informations, mais hors sujet. Nous tenions donc à nous en démarquer, et à rejeter un fonctionnement qui permet à la fois à ce Parlement de prendre des sanctions « préventives » contre un gouvernement démocratiquement élu, et de s'en abstenir en pareille circonstance...

AVIS MINORITAIRE de Maurizio Turco

A. Alors même que l'on met en évidence l'existence probable d'un système anglo-américain "d'interceptions systématiques et généralisées à l'aide de moteurs de recherche", on omet de dire que cette capacité technologique est certainement utilisée par l'Allemagne et les Pays-Bas ainsi que, probablement, par la France. Il s'ensuit que – puisque les services secrets interceptent, au nom de la sécurité nationale et sans autorisation, des communications provenant de l'extérieur – certains États membres interceptent les communications d'institutions, de citoyens et d'entreprises d'autres États membres.

B. S'il favorise la protection de la vie privée, le renforcement du chiffage suppose, par ailleurs, le renforcement des moyens de déchiffrement techniques et légaux, et cela en raison du lien indissoluble entre développement de systèmes cryptographiques, développement de systèmes de déchiffrement et développement de techniques d'interception.

C. Les solutions sont donc recherchées à l'échelon politique:

- contrôle juridictionnel et parlementaire des activités d'interception et surveillance des services de police, de sécurité et d'espionnage;
- empêcher la multiplication des autorités de contrôle qui appliquent des normes disparates en matière de protection des données, en l'absence d'un véritable contrôle démocratique et juridictionnel;
- arrêter des règles – dans le sens de la norme la plus élevée et sur la base de la jurisprudence de la CJCE – en matière de protection de la vie privée des citoyens européens contre les intrusions préventives des autorités publiques et éliminer les discriminations qui existent, dans l'Union, entre citoyens des États membres.

Annexe I: Liste des experts qui ont fourni des informations en commission

1. Membres de parlements nationaux

M. Arthur PAECHT, Assemblée nationale française
M. Armand De DECKER, président du Sénat belge
M^{me} Anne-Marie LIZIN, Sénat belge
M. Hans VAN HEVELE, secrétariat du Sénat belge
M. Guilherme SILVA, Parlement portugais
M. Ludwig STIEGLER, Bundestag, Allemagne
M. Dieter ANTONI, Parlement autrichien
M. Desmond O'MALLEY, Parlement irlandais

2. Représentants du secteur des services secrets

M. Ernst UHRLAU, coordinateur des services secrets à la Chancellerie fédérale d'Allemagne
M. Harald WOLL, Office du Bade-Wurtemberg pour la protection de la constitution, Allemagne

3. Experts en matière de télécommunications, de sécurité des réseaux et de sécurité informatique

M. José Manuel MENDES ESTEVES SERRA VERA, directeur technique, Banco Espirito Santo, Portugal
M. Clive FEATHER, directeur du développement "Logiciel", Demon Internet Ltd, Royaume-Uni
M. Jacques VINCENT-CARREFOUR, ancien chef de la division "Sécurité des réseaux", France Télécom
M. Bruno PELLERO, consultant spécialisé en matière d'écoute des télécommunications, Italie
MM. Erhard MÖLLER, Lutz BERNSTEIN et Bernd SCHINKEN, École technique supérieure, Aix-la-Chapelle, Allemagne

4. Auteurs et journalistes spécialistes d'ECHELON

M. Duncan CAMPBELL, Royaume-Uni
M. Bo ELKJAER, Danemark
M. Kenan SEEBERG, Danemark
M. James BAMFORD, Washington DC
M. Nicky HAGER, Nouvelle-Zélande

5. Experts en matière de cryptage

M. Reinhard WOBST, Unix Software, Allemagne
M. Bernd ROELLEN, Ciphers GmbH, Allemagne
M. Peter BAHR, Ciphers GmbH, Allemagne
M. Johan KEMPENERS, KBC Bank, Belgique

M. Leo VERHOEVEN, KBC Bank, Belgique
M. Bart PRENEEL, professeur de cryptologie, Université catholique de Louvain, Belgique
M. Danny de TEMMERMAN, Commission européenne
M. Desmond PERKINS, Commission européenne

6. Experts en matière d'espionnage économique et questions connexes

M. Sorbas VON COESTER, directeur de Salamandre (bureau de consultants), France
M. Christian HARBULOT, École de guerre économique, France
M. Thierry LA FRAGETTE, Circé, France
M. Ralf NEMEYER, Articon-Integralis, Allemagne

7. Droits de l'homme et protection de la vie privée

M. Dimitri YERNAULT, Université libre de Bruxelles
M. Simon DAVIES, Privacy International, Royaume-Uni
M. Jérôme THOREL, Privacy International, France
M. Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds, Royaume-Uni
MM. David NATAF et Alexandre COSTE, Millet-Sala-Nataf (bureau d'avocats), Paris
M. Rüdiger DOSSOW, Conseil de l'Europe, Strasbourg

8. Représentants d'institutions européennes

Commission européenne

Commissaire Christopher PATTEN (relations extérieures)
Commissaire António VITORINO (justice et affaires intérieures)
Commissaire Erki LIKKANEN (entreprises et société de l'information)
M. Lodewijk BRIET, direction générale des relations extérieures
M. Jacques DE BAENST, chef du protocole et de la sécurité
M^{me} Françoise DE BAIL, direction générale du commerce
M^{me} Susan BINNS, direction générale du marché intérieur

Conseil de l'Union européenne

M. Brian CROWE, directeur général des relations extérieures
M. Roland GENSON, représentation permanente du Luxembourg, justice et affaires intérieures
M. Hervé MASUREL, représentant de la présidence française en exercice
M. Gunnar LUND, ambassadeur, représentant de la présidence suédoise en exercice

Banque centrale européenne

MM. Christoph BOERSCH, Wolfgang SCHUSTER et Dominique DUBOIS, Banque centrale européenne

9. Interlocuteurs rencontrés lors de déplacements

Déplacement du président et du rapporteur à Paris, les 18 et 19 janvier 2001

M. Jean-Claude MALLET, secrétaire général, SGDN
M. Bertrand DUMONT, général de corps aérien, secrétaire général adjoint, SGDN

M^{me} Claude-France ARNOULD, directeur des affaires internationales et stratégiques, SGDN
M. Henri SERRES, directeur chargé de la sécurité des systèmes d'information, SGDN
M. Stéphane VERCLYTTE, conseiller pour les affaires juridiques et européennes, SGDN
M. Philippe DULUC, conseiller pour les affaires scientifiques et techniques, SGDN
M. Gérard ARAUD, directeur des affaires stratégiques, ministère des affaires étrangères
M. Olivier MOREAU, directeur de la sécurité, ministère des affaires étrangères
M. Eric PERRAUDAU, conseiller, ministère de la défense
M. Jean-Pierre MILLET, avocat

Déplacement du président et du rapporteur à Londres, 24-26 janvier 2001

M. Tom KING, Chairman of the Intelligence & Security Committee, House of Commons
M. Alistair CORBETT, Head of the Secretariat of the ISC, House of Commons
M. Donald ANDERSON, Chairman of the Foreign Affairs Committee, House of Commons
M. Bruce GEORGE, Chairman of the Defence Committee, House of Commons
M. Jack STRAW, Secretary of State at the Home Office
M. Michael GILLESPIE, Security Service Coordinator
M. Charles GRANT, Director, Centre for European Reform
M. Casper BOWDEN, Director of FIPR

Déplacement du bureau de la commission, des coordinateurs et du rapporteur à Washington D.C., 6-12 mai 2001

H.E. Günter BURGHARDT, chef de la délégation de la Commission à Washington D.C.
M. James WOOLSEY, former Director CIA
M. Jeffrey RICHELSON, Director, National Security Archive, George Washington University
M. Marc ROTENBERG, Electronic Information Privacy Centre
M. Wayne MADSEN, Electronic Information Privacy Centre
M. David SOBEL, Electronic Information Privacy Centre
M. Barry STEINHARDT, Associate Director, American Civil Liberties Union
M. Porter J. GOSS, chairman House Permanent Select Committee on Intelligence
M^{me} Nancy PELOSI, vice-chair House Permanent Select Committee on Intelligence
M. Robert DAVIS, Deputy Counsel for the office of Intelligence Policy Review, US Department of Justice

ANNEXE II: Sources documentaires

SOURCES CITÉES

Advocacy Center, Homepage, <http://www.ita.doc.gov/td/advocacy/>

Andrew, Christopher, The growth of the Australian Intelligence Community and the Anglo-American Connection, 223-224 in *E. Hayden, H. Peake and S. Halpern* eds, In the Name of Intelligence. Essays in honor of *Washington Pforzheimer* (Washington NIBC Press 1995), 95-109

Andrew, Christopher, The making of the Anglo-American SIGINT Alliance, in: *Hayden B. Peake, Halpern, Samuel*. (Eds.): In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, NIBC Press (1995), 95 -109

Andronov, Major A., Zarubezhnoye voyennoye obozreniye, Nr.12, 1993, 37-43

Anonymus, Hacker's guide, Markt & Technik-Verlag (1999)

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001)

Bamford, James, The Puzzle Palace. Inside the National Security Agency, America's most secret intelligence organization, Penguin Books (1983)

Benett, Gordon, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, <http://www.csrc.ac.uk/pdfs/c105.pdf>

Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werdenn Handelsblatt, 29.8.1996

Brady, Martin, Direktor der DSD, Brief vom 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

Bronskill, Jim, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, <http://www.ottawacitizen.com/national/990522/2630510.html>

Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computerspionage, Dokumentation Nr. 44, Juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmietleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung, Band 2/5, in: STOA (Ed), die Entwicklung der Überwachungstechnologie und die Risiken des Missbrauchs von Wirtschaftsinformationen (Oktober 1999), PE 168.184

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000,
<http://www.heise.de/tp/deutsch/special/ech/6928/1.html>

Comité permanent de contrôle des service de renseignement, Rapport d'enquête sur la manière dont les services belges de renseignement reagissent face à l'éventualité d'un système américain "echelon" d'interception des communications téléphoniques et fax en Belgique,
<http://www.droit.fundp.ac.be/textes/echelonfr.pdf>

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, (1996)
<http://www.gpo.gov/int/report.html>

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet (Neuseeland), "Securing our Nation's Safety", Dezember 2000,
<http://www.dpmc.govt.nz/dess/securingoursafety/index.html>

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999),

Elkjaer, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

Federation of American Scientists (FAS), Homepage, <http://www.fas.org/>

Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattoni, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000.

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Freyer, Ulrich, Nachrichten-Übertragungstechnik, Hanser Verlag (2000)

Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention², N. P. Engel Verlag (1996)

Frost, Mike in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000,
<http://cryptome.org/echelon-60min.htm>

Frost, Mike in Interview des australischen Senders Channel 9 vom 23.3.1999
<http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm>

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

Guisnel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealand's Role in the international Spy Network, Craig Potton Publishing (1996)

Hager, Nicky, Exposing the global surveillance system, <http://www.ncoic.com/echelon1.htm>

Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, April 2001

Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)

Intelligence and Security Committee (UK), Annual Report 1999-2000

Jacobs, Francis G, White, Robin C.A., The European Convention on Human Rights², Clarendon Press (1996)

Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001

Kuppinger, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

Kurtz, George, McClure, Stuart, Scambray, Joel, Hacking exposed, Osborne/McGraw-Hill (2000)

Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23

Landesamt für Verfassungsschutz Baden Württemberg, Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 10/1998

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, Bericht an den amerikanischen Congress Ende Februar 2000, <http://www.fas.org/irp/nsa/standards.html>

Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999

Lyle Robert, Radio Liberty/Radio free Europe, 10. Februar 1999

National Security Councils (NSC), Homepage, <http://www.whitehouse.gov/nsc>

Madsen, Wayne in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, <http://cryptome.org/echelon-60min.htm>

Paecht, Arthur, 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.

Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999

Porter, Michael E., Competitive Strategy, Simon & Schuster (1998)

Richelson, Jeffrey T., Desperately seeking Signals, The Bulletin of the Atomic Scientists Vol. 56, No. 2/2000, pp. 47-51, <http://www.bullatombci.org/issues/2000/ma00/ma00richelson.html>

Richelson, Jeffrey T., The U.S. Intelligence Community⁴, Westview Press, 1999

Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University
<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html>

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzer, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.02.2000,
http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, (1999)

Schütze, Arno, Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? P.M. Magazin, Die Moderne Welt des Wissens (1998)

Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)

Smith, Bradley F., The Ultra-Magic Deals and the Most Secret Special Relationship 1940-1946, Presidio (1993)

Sorti, Francesco, Dossier esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998

State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, Oktober 1996

Thaller, Georg Erwin, Satelliten im Erdorbit. Nachrichten, Fernsehen und Telefonate aus dem Weltall, Franzis Verlag, München (1999)

Weißes Haus, Archive,
<http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html>

Wessely, Wolfgang, Das Fernmeldgeheimnis - ein unbekanntes Grundrecht?, ÖJZ 1999, 491 ff

Wirtschaftswoche "Antennen gedreht", Nr. 46/9, November 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, Oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)

Woolsey, James, Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000

Woolsey, James, Remarks at the Foreign Press Center, Transskript, 7.3.2000,
<http://cryptome.org/echelon-cia.htm>

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998) PE 166.499/INT.ST.

Yernaut, Dimitri, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, S. 187 ff.

AUTRES SOURCES

Air Intelligence Agency (AIA), Homepage, <http://www.aia.af.mil>

America's Military Community, Homepage, <http://www.military.com>

Barr, Bob, Barr moves to expose "project ECHELON", 9.11.1999,
http://www.house.gov/barr/p_110999.html

Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000,
<http://www.bundesnachrichtendienst.de/diensteb.htm>

Bundesamt für Verfassungsschutz, Spionage gefährdet die Sicherheit und die Interessen
unseres Landes, 2001, <http://www.verfassungsschutz.de/arbeitsfelder/spion/page.html>

Campbell, Duncan, Somebody's listening, They've got it taped, 12.8.1988, New Statesman,
<http://jya.com/echelon-dc.htm>

Central Intelligence Agency (CIA), Homepage <http://www.odci.gov/index.html>

Commander Submarine Force, U.S. Atlantic Fleet - Surveillance and Intelligence,
<http://www.sublant.navy.mil/roles.htm#survintel>

Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room
<http://www.fbi.gov/>

Ecole de Guerre Economique, Homepage, <http://www.ege.eslsca.fr/>

Federal Bureau of Investigation (FBI), Homepage, <http://www.fbi.gov>

Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftsspionage, 19.4.2000

Frankfurter Allgemeine Zeitung, Wirtschaftsspionage, 3.2.2001

Freeh, J. Louis, Wirtschaftsspionage, 28.2.1996, Ansprache vor dem Senat,
<http://www.fbi.gov>

General Dynamics, Seawolf Class, <http://www.gdeb.com/programs/seawolf/>

Göbel, Jürgen, Kommunikationstechnik, Grundlagen und Anwendungen, Hüthig (1999)

Goss, J. Porter, Additional views of chairman Porter J. Goss, 2000,
<http://www.aclu.org/echelonwatch/goss.htm>

Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt
und Technik (1999)

Hager, Nicky, Wie ich Echelon erforscht habe, 11.04.2000,
<http://www.heise.de/tp/deutsch/special/ech/6728/1.html>

Hayden, Michael, Statement for the record of House Permanent Select Committee on
intelligence, 12.04.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML

Innenministerium Brandenburg, Abwehr von Wirtschaftsspionage, 1999

Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000,
<http://www.fbi.gov>

Kerr, M. Donald, Congressional Statement on Internet and data Interception Capabilities
Developed by FBI, 24.7.2000, <http://www.fbi.gov>

Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger,
Franzis Verlag, Funkschau Telekom, Poing 1998

Mathiesen, Thomas, On Globalisation of Control: Towards an Integrated Surveillance System
in Europe, Statewatch Publication, 11.1999

Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media
Verlag Ingelheim

National Security Agency (NSA), Homepage, <http://www.nsa.gov/>

Preneel, Bart, Relative Security of Cryptographic, 18.11.1998, Presentation on Conference on
Problems of Global Security

Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communication in the UK, Juni
1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d'activités 1999 du
Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, Statement by Director of Central Intelligence before the House Permanent
Select Committee on Intelligence, 12.4.2000,
http://sun00781.dn.net/irp/congress/2000_hr/tenet.html

The United States Navy, Homepage, <http://www.navy.mil>

The US Army Intelligence and Security Command (INSCOM), Homepage
<http://www.vulcan.belvoir.army.mil>

The White House, Defending America's Cyberspace, National Plan for Information systems
protection Version 1.0, 2000, The White House 2000

Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen
ausplündert und ruiniert. Bertelsmann Verlag, München (1999)

V. Bülow, Andreas, Im Namen des Staates. CIA, BND und die kriminellen Machenschaften
der Geheimdienste. Piper Verlag, München (1998)

Verfassungsschutz Brandenburg, Abwehr von Wirtschaftsspionage - eine Aufgabe des
Verfassungsschutzes, 1999, <http://www.brandenburg.de/land/mi/vschutz/wispion.htm>

Wall, Stephen, Ständiger Vertreter des Vereinigten Königreichs bei der Europäischen Union,
Brief an Kommissar Liikanen zu GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard

Annexe III: Interception des communications aux fins de poursuites pénales: définitions et commentaires

1. Remarques liminaires

Dans le cadre des travaux de la commission, lors du débat sur l'admissibilité, les incidences et les dangers des systèmes d'interception mondiaux utilisés à des fins de renseignements, on a évoqué de façon répétée l'existence, dans l'Union européenne, de mesures et d'activités qui, certes, touchent à la question de l'interception des communications, mais qui relèvent du domaine de la coopération judiciaire en matière pénale.

Dans la partie principale du rapport, le rapporteur n'évoque pas ces mesures, car la question de la légitimité de l'interception des communications à des fins pénales ne doit pas être amalgamée avec la question de la légitimité de l'interception des communications à des fins de renseignement. Même si, dans les deux cas, il s'agit d'atteintes à la vie privée qui se justifient par des considérations de sécurité (au sens le plus large), ces deux types d'interceptions présentent cependant, par les méthodes et les objectifs, des différences telles que des réglementations qui pourraient sembler rationnelles et équilibrées pour un domaine ne le seraient pas forcément pour l'autre. L'opportunité et la proportionnalité des mesures pénales ne doivent donc pas être examinées dans le contexte de l'appréciation politique des opérations de renseignement.

Pour éviter tout malentendu, il convient ici de revenir sur certaines questions qui ont été soulevées et de définir certaines notions. Dans les paragraphes qui suivent, on commencera par indiquer les différences entre interception des communications aux fins de poursuites pénales et interception des communications aux fins de renseignement (2); ensuite, compte tenu des compétences de l'UE, on en présentera les actes juridiques qui touchent à l'interception des communications à des fins pénales (3); et, enfin, on explicitera encore d'autres notions qui ont été utilisées de façon répétée au sein de la commission à propos de travaux transfrontaliers dans le domaine de l'interception des communications (4).

2. Délimitation: interception des communications à des fins pénales / à des fins de renseignement

Si les services de renseignements étrangers interceptent les communications (comme dans le cas du système ECHELON), c'est non pour surveiller telle ou telle personne, mais pour surveiller de façon générale les activités déployées à l'étranger, et cela afin d'obtenir des informations importantes sous le rapport de la sécurité. Cette surveillance est exercée secrètement et n'est pas censée être un jour portée à la connaissance de l'opinion publique. En faisant valoir que seul le secret peut garantir la sécurité et que l'on n'a pas affaire à des sujets de droit au sens propre, on permet souvent à des services secrets d'opérer dans une zone grise du droit dans laquelle les réglementations sont peu claires et les contrôles lacunaires.

En revanche, l'interception des communications à des fins pénales vise à empêcher, en cas de soupçon, la personne de passer à l'acte, ou à sanctionner des délits. Ce sont les autorités nationales qui mettent en place les mesures d'interception. Si des mesures d'interception

doivent être mises en place à l'étranger, elles le sont par les autorités du pays en question, dans le cadre de l'entraide judiciaire. Comme ces interventions visent les sujets de droit proprement dits, il existe, depuis la chute des États policiers, des réglementations très précises et des mécanismes de contrôle efficaces qui assurent l'équilibre entre les intérêts en cause. Des mesures d'interception ne peuvent donc être mises en place, en cas de soupçon fondé, que dans des cas particuliers. Dans de nombreux États membres, il est nécessaire d'obtenir l'autorisation d'un juge. Même lorsqu'elle est secrète, l'interception vise à permettre l'utilisation des matériaux dans le cadre d'une procédure pénale publique, de sorte que l'autorité elle-même a intérêt à obtenir de façon légale les preuves recherchées.

3. Interception des communications à des fins pénales: travaux dans l'Union européenne

3.1 Généralités

En insérant dans le traité UE un titre "Politique étrangère et de sécurité commune", on a créé la possibilité d'une coopération entre services de renseignements à l'échelon européen. Mais il n'a pas encore été fait usage de cette possibilité. Dans la mesure où il en existe dans le cadre de l'Union européenne, réglementations et travaux dans le domaine de l'interception des communications portent exclusivement sur le volet pénal, c'est-à-dire sur la coopération dans les domaines de la justice et des affaires intérieures.

3.2 Limitation de la compétence de l'UE aux réglementations techniques

À l'heure actuelle, la question de la recevabilité de mesures d'interception relève exclusivement de la compétence nationale des États membres. En vertu du principe d'autorisation limitée, l'UE ne peut intervenir que là où des compétences lui sont reconnues conformément aux traités. Or, le titre VI du TUE "dispositions relatives à la coopération policière et judiciaire en matière pénale" ne prévoit pas une telle compétence. Dans le domaine de la coopération policière (article 30, paragraphe 1 du traité UE), une action en commun est exclusivement prévue pour des aspects opérationnels, c'est-à-dire ceux qui concernent la manière d'exécuter le travail de la police. En matière de coopération judiciaire, l'article 31 c) prévoit dans le cadre de l'action en commun "d'assurer la compatibilité des règles applicables dans les États membres", ce qui n'est recevable que si cela est "nécessaire à l'amélioration de cette coopération" et vise donc les dispositions spécifiques à la coopération. Et le "rapprochement des règles de droit pénal des États membres" visé à l'article 29, dernier tiret, se limite à la fixation de règles minimales relatives aux éléments constitutifs (article 31, lettre e). En résumé, on peut constater que la question des conditions de l'opportunité des mesures d'interception continue de relever du droit national. Le rapporteur n'a connaissance d'aucune tentative d'un État membre visant à toucher à cette compétence exclusivement nationale.

Les États membres ne peuvent donc coopérer sur la base des traités UE que sur la question de l'exécution des mesures d'interception recevables au titre du droit national, c'est-à-dire à un niveau inférieur. Dans les cas où les régimes juridiques nationaux autorisent une interception des télécommunications, l'État membre concerné doit pouvoir solliciter l'aide des autres États membres en vue de l'exécution technique de celle-ci. Quant à savoir si l'on considère comme positive ou négative la simplification technique recherchée qui apportera sans doute une plus

grande efficacité dans l'interception transfrontalière en vue des poursuites pénales précisément dans le domaine de la criminalité organisée, cela dépend sans doute beaucoup de la confiance dans son propre État de droit. Soulignons une fois encore que – quand bien même l'harmonisation technique simplifierait-elle l'interception transfrontalière et sachant qu'un abus ne peut pas toujours être évité – les conditions de la recevabilité d'une interception, qui sont régies par un droit purement national, ne sont pas affectées.

3.3 Travaux et actes juridiques dans le domaine de l'interception des télécommunications

Dans le domaine de l'interception des télécommunications, deux actes juridiques ont été jusqu'à présent arrêtés dans le cadre de l'UE: la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, dont le contenu devait être étendu aux États tiers par le biais d'un mémorandum et pour lequel une proposition de "up-date" était prévue (les deux sont préparés dans "des documents ENFOPOL") et la Convention relative à l'entraide judiciaire en matière pénale.

Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications²⁶⁶

Cette résolution résulte, semble-t-il, de la coopération des experts au sein des séminaires ILET (voir plus bas); elle est conforme pour l'essentiel aux IUR (international user requirements).

Cette résolution a pour but de faire en sorte que tous les États membres créent les conditions techniques pour que les autorités puissent accéder aux données dans le cadre de leur autorisation nationale et, donc, exercer techniquement les pouvoirs que leur confère le droit national.

À cet effet, une annexe énumère des "spécifications" très détaillées des États membres dont le Conseil "prend acte", du fait qu'elles constituent "un condensé important des besoins des autorités compétentes pour la réalisation technique des mesures d'interception légale dans les systèmes modernes de télécommunications". Ces spécifications sont, par exemple, les possibilités de surveillance en temps réel ou la capacité de transmettre les communications interceptées à l'installation de surveillance par l'opérateur de réseaux. Dans la résolution, le Conseil se déclare favorable à ce que les spécifications soient prises en considération lors "de la définition et de l'exécution des mesures et demande aux États membres et aux ministres responsables de coopérer afin d'appliquer ces spécifications en ce qui concerne les opérateurs de réseaux et les fournisseurs de services".

Il convient de souligner ici que la forme de l'acte juridique choisie, la résolution, ne revêt aucun caractère contraignant et n'engage donc aucunement les États membres. L'émotion que cette résolution et les documents qui s'y rapportent ont suscitée est moins imputable au contenu qu'aux circonstances dans lesquelles ils ont été élaborés, en particulier au manque de transparence.

²⁶⁶ JO C 329 du 4.11.1996.

Memorandum of Understanding

Dans le "Mémorandum of Understanding"²⁶⁷ qui a suivi, certains États tiers ont été invités à transposer les spécifications techniques citées dans la résolution du Conseil du 17 janvier 1995. Il fallait en outre obtenir que les innovations techniques et les nouvelles spécifications qui en découlent soient communiquées au FBI ainsi qu'au secrétariat du Conseil, ce qui a été fait sachant que la production des techniques d'information est souvent aux mains d'entreprises multinationales, rendant ainsi indispensable la coopération avec les autorités de surveillance des États tiers dans lesquels sont implantés des sites de production importants.

Le mémorandum a été signé le 23 novembre 1995 par les États membres de l'UE et par la Norvège mais il ne l'a pas été par d'autres États tiers. Les États-Unis, l'Australie et le Canada ont seulement fait savoir par écrit qu'ils encourageront la transposition nationale dans leur pays²⁶⁸.

Le texte, qui n'a malheureusement pas été publié à ce jour, a donné lieu à de nombreuses spéculations dans la presse.

Le projet de résolution du Conseil relative à l'interception légale des télécommunications dans le domaine des nouvelles technologies

Comme le rapporteur l'a déjà indiqué dans son rapport du 23 avril 1999²⁶⁹, le projet de résolution du Conseil relative à l'interception légale des télécommunications dans le domaine des nouvelles technologies est un "up-date" de la résolution de 1995. La nouvelle résolution du Conseil précise que les "spécifications" de la résolution du Conseil de 1995, auxquelles viennent s'ajouter plusieurs spécifications nouvelles, sont également valables pour les nouvelles technologies de communication, par exemple par satellite et Internet, et que les termes techniques utilisés jusqu'à présent doivent être interprétés conformément à la nouvelle technologie (par exemple, identification d'un numéro de téléphone dans Internet). Le projet a été adopté par le Parlement européen²⁷⁰, mais provisoirement gelé par le Conseil.

La Convention relative à l'entraide judiciaire en matière pénale²⁷¹

Le second acte juridique est la Convention relative à l'entraide judiciaire en matière pénale. Dans ses articles 17 et suivants, elle traite de la question des conditions et de la nature de

²⁶⁷ N° 10037/95 ENFOPOL, 112, non publié.

Voir la réponse écrite, du 16 décembre 1998, de M. Karl Schlögel, ministre autrichien de l'intérieur, à la question parlementaire du député Alexander Van der Bellen (4739/AB XX. GP).
http://www.parlament.gv.at/pd/pm/XX/AB/his/047/AB04739_.html

²⁶⁸ C'est ce qu'a expressément déclaré M. Karl Schlögel, ministre autrichien de l'intérieur (cf. note précédente); répondant, le 14 mai 1997, lors de l'heure des questions, à la question orale H-0330/97 de Jonas Sjöstedt, Michiel Patijn, en sa qualité de président en exercice du Conseil, a indiqué, de façon quelque peu obscure, que les États-Unis, le Canada, l'Australie et la Norvège avaient également souscrit à "ces dispositions" (il se référait aux spécifications visées dans la résolution du Conseil du 17 janvier 1995).

²⁶⁹ A4-0243/1999.

²⁷⁰ Résolution législative portant avis du Parlement européen du 7 mai 1999, JO C 279 du 1.10.1999, p. 498.

²⁷¹ 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 2000, p. 1, articles 17 et suivants.

l'entraide judiciaire en matière pénale qui doit être possible en ce qui concerne l'interception des télécommunications. Sans entrer dans les détails des réglementations, constatons seulement que la Convention ne porte aucunement atteinte aux droits de la cible, puisque l'État membre dans lequel celle-ci se trouve peut toujours refuser l'entraide judiciaire lorsque celle-ci n'est pas admissible en vertu du droit national.

4. Travaux transfrontières dans le domaine de l'interception des télécommunications: définitions et commentaires

En plus des multiples actes communautaires, les différents groupes de travail qui existent ou ont existé dans le domaine de la politique de sécurité ont souvent suscité la confusion. Dans les paragraphes qui suivent, on s'efforcera donc d'explicitier certaines des notions en question.

ILETS (International Law Enforcement Telecommunications Seminar)

Les séminaires ILET sont dus à une initiative du FBI. En 1993, le FBI a invité des autorités chargées de poursuites pénales et des services d'information d'États amis à assister, à Quantico, à une séance sur le thème de l'interception des télécommunications. Une grande partie des États de l'UE ainsi que l'Australie et le Canada y ont participé²⁷². Depuis lors, des rencontres ont régulièrement lieu en vue d'examiner les impératifs d'une surveillance efficace des communications à l'échelon international.

Au cours d'une rencontre à Bonn, en 1994, les membres des ILETS se sont mis d'accord sur un document comportant des orientations politiques dans l'annexe duquel figure une liste de "International user requirements" (IUR 1.0 ou IUR 95). Celle-ci contenait des critères qui devaient être imposés aux différents opérateurs de télécommunications en vue de simplifier le processus d'interception. Ces IUR 1.0 servaient – fût-ce de manière informelle – de base à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications. Par la suite, d'autres réunions d'experts sur le thème des IUR et leur éventuelle transposition et adaptation aux nouvelles télécommunications ont été organisées.

Groupe TREVI

Dans le cadre du groupe TREVI, les ministres de la justice et des affaires intérieures des États membres de la CE ont examiné certaines questions de sécurité intérieure avant l'entrée en vigueur du traité de Maastricht (qui a introduit les dispositions relatives à la coopération dans le domaine de la justice et des affaires intérieures). Le groupe TREVI ne fonctionne plus, étant donné que les sujets sont traités entre temps au sein des groupes de travail spécifiques du Conseil.

Dans le domaine à l'examen, mentionnons essentiellement deux groupes de travail: le groupe "Entraide judiciaire en matière pénale", qui a examiné la Convention relative à l'entraide judiciaire en matière pénale dans le cadre de la coopération "justice et affaires intérieures", et le groupe de travail "Coopération policière" qui se penche sur les questions de l'interception légale des télécommunications, y compris celle des nouveaux systèmes de communication

²⁷² Voir la réponse écrite de M. Schlögel, ministre autrichien de l'intérieur, à la question parlementaire du député Van der Bellen 4014/AB XX.GP). http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html.

(téléphones mobiles, Internet, e-Mail); ce groupe s'est également penché sur le rapprochement des normes des spécifications imposées par les autorités d'interception agréées aux exploitants de réseaux et aux prestataires de services.

"ENFOPOL"

Contrairement à ce que croient de nombreux auteurs, ENFOPOL n'est ni un groupe de travail ni une organisation, mais une abréviation qualifiant des documents de travail en matière de poursuites pénales et d'affaires policières, comme le groupe de travail "Coopération policière"²⁷³. Ces documents ne portent pas l'entête ENFOPOL, mais sont classés en fonction de celui-ci.

²⁷³ Réponse écrite de M. Schlögels, ministre autrichien de l'intérieur à la question parlementaire du député Van der Bellen (4014/AB XX.GP) http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html.

TABLEAU SYNOPTIQUE

DES SERVICES DE RENSEIGNEMENT ET DES ORGANES
DE CONTRÔLE PARLEMENTAIRE

DES ÉTATS MEMBRES

ET DES ÉTATS UKUSA

Pays	Service de renseignement	Base juridique	Missions	Rensei- gnement électro- magnétique	Organe de contrôle	B
AUTRICHE	<p>Heeresnachrichtenamt (HnA)</p> <p>Abwehramt (AbwA)</p> <p>service de renseignement militaire</p> <p>sous l'autorité du ministre de la défense</p>	<p>§ 20 Abs 3 <i>Militärbefugnisgesetz (MBG) BGBl I 86/2000</i></p>	<p>collecte de renseignements militaires; protection contre les activités étrangères constituant des menaces pour la sécurité</p>		<p>sous-commission parlementaire:</p> <p><i>Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung (14 membres; chaque parti représenté au Parlement doit être représenté au sein de la sous-commission).</i></p> <p><i>1 commissaire à la protection des droits.</i></p>	<p>Ar Be ge</p> <p>§§ G 19</p>
AUTRICHE	<p>Sondereinheit für Observation (SEO)</p> <p>service de renseignement civil</p> <p>sous l'autorité du ministre de l'intérieur</p>	<p>§§ 6, 14, 15 <i>Sicherheitspolizeigesetz (SPG, BGBl 566/1991 idgF)</i></p> <p><i>Sondereinheiten-Verordnung (BGBl II 207/1998)</i></p>	<p>préservation de la sécurité publique; contre-espionnage sur le territoire national; protection des principes faisant l'objet d'une garantie de la Constitution; lutte contre les mouvements extrémistes, le terrorisme et la criminalité organisée</p>		<p>sous-commission parlementaire:</p> <p><i>ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (14 membres; chaque parti représenté au Parlement doit être représenté au sein de la sous-commission).</i></p> <p><i>1 commissaire à la protection des droits.</i></p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
BELGIQUE	<p>Service Général du Renseignement et de la Sécurité des Forces armées (S.G.R.)</p> <p>service militaire de renseignement et de sécurité</p> <p>sous l'autorité du ministre de la défense nationale</p>	<p><i>Loi du 30 novembre 1998 organique des services de renseignement et de sécurité</i></p>	<p>collecte d'informations et de données dans les domaines militaire, politique, économique et technico-scientifique; protection de la sécurité des installations et du personnel militaires.</p>		<p><i>Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R),</i></p> <p>composé de trois membres nommés par le Sénat, qui n'ont pas le droit d'exercer un mandat électif ou une autre activité de nature à compromettre leur indépendance.</p>	<p><i>Loi</i> <i>(V</i> <i>cc</i> <i>de</i> <i>re</i></p>
BELGIQUE	<p>Sûreté de l'État (V.S.)</p> <p>service civil de renseignement et de sécurité sous l'autorité du ministre de la justice</p>	<p><i>Loi du 30 novembre 1998 organique des services de renseignement et de sécurité</i></p>	<p>Sécurité intérieure et extérieure, contre-espionnage, observation des mouvements politiques extrémistes</p>		<p><i>Service d'enquêtes des services de renseignements</i></p> <p>subordonné au Comité permanent R; ses membres sont désignés par le Comité R.</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
DANEMARK	<p>Forsvarets Efterretningstjeneste (FE(T))</p> <p>"Service secret de la défense"</p> <p>sous l'autorité du ministère de la défense</p>	<p><i>Lov om forsvarets formål, opgaver og organisation m.v.</i></p> <p>Lov 909 af 8/12/1993</p> <p>["loi-cadre", sauf mention du FE(T)]</p> <p>[FET et PET feront prochainement l'objet d'une nouvelle loi]</p>	<p>collecte et analyse, aux fins de la défense, d'informations secrètes sur la CEI et l'Europe centrale et orientale dans les domaines militaire, politique, économique et technico-scientifique; renseignement électro-magnétique; chiffre; effectif et budget: informations classées</p>	oui	<p>2 commissions de contrôle:</p> <p><i>Kontroludvalget vedrørende Politiets og Forsvarets efterretningstjenester (Wamberg-udvalget) (composée de fonctionnaires et d'avocats)</i> membres désignés par le ministre de la justice</p>	pa sp
DANEMARK	<p>Politiets Efterretningstjeneste (PET)</p> <p>"Service secret de la police"</p> <p>sous l'autorité du ministère de la justice</p>	<p>aucune législation spécifique</p> <p>[FET et PET feront prochainement l'objet d'une nouvelle loi]</p>	<p>contre-espionnage, prévention des activités de nature à mettre en danger la sécurité du pays et lutte contre ces activités: espionnage, terrorisme, etc.; sécurité du gouvernement et de la famille royale</p> <p>effectif: 370 personnes environ (1998) budget: informations classées.</p>		<p><i>Udvalget vedrørende efterretningstjenesterne</i></p> <p>commission parlementaire (composée de 5 membres du Folketing)</p>	Lo et fo ef lo

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
FINLANDE	<p>Pääesikunnan tiedusteluosasto "Section du renseignement militaire du personnel de défense de la Finlande"</p> <p>sous l'autorité du ministère de la défense</p>	<p><i>Laki puolustusvoimista</i> N:o 402/1974 2§</p> <p>"Loi relative aux forces de défense" (qui ne mentionne pas la section du renseignement)</p>	surveillance du territoire et de l'espace aérien du pays en collaboration avec d'autres organes de surveillance en vue d'assurer l'intégrité territoriale du pays	oui	<p>aucun organe spécifique de contrôle</p> <p>le ministère de la défense présente chaque année au médiateur parlementaire un rapport sur les interceptions</p>	<p>Pe §3 "L po La m 40 "L m cc [s m m pa cc in m cc</p>
FINLANDE	<p>Suojelupoliisi (SUPO) "La police de sécurité finlandaise"</p> <p>sous l'autorité du ministère de l'intérieur</p>	<p><i>Laki poliisin hallinnosta</i> N:o 110/1992, 1§, 10§ 1. ja 2. momentti <i>Asetus poliisin hallinnosta</i> N:o 158/1996 8§</p> <p><i>Laki poliisin henkilökäytöstä</i> N:o 509/1995 23§, 9§</p> <p>"Loi et décret sur l'administration de la police" et "loi relative au traitement par la police des données à caractère personnel "</p>	contre-espionnage; prévention des activités de nature à mettre en danger la sécurité intérieure du pays et les relations internationales; lutte contre le terrorisme; action préventive pour la sécurité		<p>aucun organe spécifique de contrôle;</p> <p>la police est tenue de rendre compte de tous les cas d'interception au ministère de l'intérieur, qui présente un rapport annuel au médiateur parlementaire</p>	
FINLANDE	<p>Tullin tiedusteluyksikkö "Section de renseignement des douanes finlandaises"</p> <p>ministère des finances</p>	<p><i>Tullilaki</i> N:o 1466/1994 "Loi relative aux douanes"</p>	collecte et analyse de données en vue de la prévention et de la découverte des infractions douanières et transmission de ces données aux services compétents pour suites à donner		<p>aucun organe spécifique de contrôle</p> <p>l'administration des douanes est tenue de rendre compte de tous les cas d'interception à l'office national des douanes et au ministère de l'intérieur, qui présente un rapport annuel au médiateur parlementaire</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
FRANCE	<p>Direction générale de la sécurité extérieure (DGSE)</p> <p>sous l'autorité du ministère de la défense</p>	<p>décret n°82-306 du 2 avril 1982</p>	<p>collecte de renseignements d'intérêt politique, militaire, économique et technico-scientifique</p> <p>recherche et exploite des renseignements intéressants la sécurité de la France; contre-espionnage (hors du territoire national)</p> <p>Effectif: 4100 personnes; budget: FRF 1,7 milliards</p>	<p>oui</p>	<p>aucun organe parlementaire spécifique de contrôle (projet en discussion; la commission de la défense de l'Assemblée nationale a proposé, à deux reprises, la création d'un comité de surveillance; n^{os} 1951 et 2270)</p> <p>Commission nationale de contrôle des interceptions de sécurité (exclusivement le contrôle des écoutes sur câbles)</p> <p>composée, entre autres, d'un député et d'un sénateur.</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
	Direction du renseignement militaire (DRM) ministère de la défense	<i>décret n°92-523 du 16 juin 1992</i>	Fournit les renseignements militaires nécessaires aux armées Effectif: 1700 personnes; budget: FRF 90 millions; sécurité militaire intérieure, soutien de l'armée			
FRANCE	Direction de la surveillance du territoire (DST) service de renseignement civil sous l'autorité du ministre de l'intérieur	<i>décret n°82-1100 du 22 décembre 1982</i>	contre-espionnage sur le sol français effectif: 1500 personnes; préservation de la sécurité publique, contre-espionnage sur le territoire national			

Pays	service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle	B
ALLEMAGNE	Bundesnachrichtendienst (BND) sous l'autorité du chancelier fédéral	<i>Gesetz über den Bundesnachrichtendienst (BNDG)</i> , BGBl 1990 I 2954 idgF	collecte et exploitation d'informations sur les pays étrangers qui présentent un intérêt pour la sécurité et la politique extérieure	oui	<i>Parlamentarisches Kontrollgremium (PKGR)</i> organe de contrôle parlementaire des trois services secrets; composé de 9 membres du Bundestag	G K di de (F 19 id
ALLEMAGNE	Bundesamt für Verfassungsschutz (BfV) sous l'autorité du ministre de l'intérieur	<i>Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für den Verfassungsschutz (BVerfSchG)</i> , BGBl 1090 I 2954)	collecte et exploitation d'informations sur les activités mettant la sécurité en danger et sur les activités des services de renseignement hostiles sur le territoire national		<i>G 10-Kommission</i> indépendante; peut, mais ne doit pas nécessairement, être composée de députés;	§ G G (G A 94 (l re du pa té
ALLEMAGNE	Militärischer Abschirmdienst (MAD) sous l'autorité du ministre de la défense	<i>Gesetz über den militärischen Abschirmdienst (MADG)</i> BGBl 1990 I 2954 idgF	assurer le fonctionnement efficace de l'armée fédérale ainsi que la sécurité des installations et du personnel militaires.		4 membres nommés par le PKGR.	

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
GRÈCE	<p>Ethniki Ypiresia Pliroforion (EYP)</p> <p>"Service national de renseignement"</p> <p>sous l'autorité du KYSEA (Conseil national de la sécurité: Premier ministre + ministres des affaires étrangères et de la défense nationale)</p>	<p><i>loi 1645/86 relative au Service national de renseignement (Ethniki Ypiresia Pliroforion)</i></p>	<p>- collecte et traitement d'informations en rapport avec la sécurité nationale (sur la criminalité organisée et le terrorisme) et de renseignements militaires, économiques et politiques;</p> <p>transmission aux autorités compétentes</p> <p>- contre-espionnage, observation des activités des agents de renseignements étrangers agissant contre le pays</p>		<p>commission parlementaire spéciale pour la protection du secret des communications et de la vie privée. Pas de droit de contrôle particulier. Composition: 1 vice-président du Parlement, 1 député par groupe politique, 1 spécialiste des communications.</p> <p>Office pour la protection des données à caractère personnel</p>	<p>lo A e, (s cc</p> <p>lo Pr ep de pr (F tra de pe</p>

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
IRLANDE	<p>Garda Síochána (police nationale) chargée des questions relevant de la sécurité nationale</p> <p>La police est responsable devant le ministre de la justice</p>	<p>pouvoir d'interception en vertu de l'<i>Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993</i></p>	<p>interceptions autorisées dans l'intérêt de la sûreté de l'État</p>		<p><i>le Joint Committee on Justice, Equality and Women's Rights</i> a compétence pour tout le champ des droits civils</p>	
IRLANDE	<p>Intelligence Staff</p>		<p>protection de la sécurité du pays (principalement à l'égard de l'IRA), sécurité des forces armées nationales, évolutions technologiques des armées étrangères</p>		<p>Pas d'autorité de contrôle spéciale.</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
ITALIE	Servizio per le informazioni e la sicurezza militare (SISMI) Servizio informazione Operative Segrete (SIOS) soumis au ministre de la défense, qui désigne le directeur du Service et les hauts fonctionnaires	<i>L. 24 ottobre 1977, n. 801, art. 4 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato</i>	tâches d'information et de sécurité pour la défense, au niveau militaire, de l'indépendance et de l'intégrité de l'État; contre-espionnage; collecte d'informations étrangères sur des thèmes politiques, militaires, économiques et technico-scientifiques		Commission parlementaire (4 députés +4 sénateurs)	L. 801/77
ITALIE	Servizio per le informazioni e la sicurezza democratica (SISDE) Direzione investigazioni anti-mafia (DIA) soumis au ministre de l'intérieur, qui désigne le directeur du Service et les hauts fonctionnaires	<i>L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato</i>	tâches d'information et de sécurité pour la défense de l'État démocratique et de ses institutions informations sur les activités mettant la sécurité en danger sur le territoire national; contre-espionnage, lutte contre le terrorisme et la criminalité organisée		Le gouvernement soumet au Parlement un rapport semestriel sur la politique d'information et de sécurité.	L. 801/77

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
LUXEMBOURG	<p>Service de renseignement</p> <p>service national d'information et de sécurité</p> <p>sous l'autorité du ministre d'État (=président du gouvernement)</p>	<p><i>Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État</i> du 30 juillet 1960</p>	<p>assurer la protection des secrets visés à l'art. 120 octies du Code pénal* et rechercher les informations que requiert la sauvegarde de la sécurité extérieure du Grand-Duché de Luxembourg et des États avec lesquels il est uni par un accord régional en vue d'une défense commune</p> <p>* "infractions commises envers le Grand-Duché de Luxembourg."</p>		<p>pas de contrôle parlementaire</p> <p>(la surveillance de toutes les formes de communications aux fins de rechercher des infractions contre la sûreté de l'État requiert l'assentiment d'une commission composée du président de la Cour supérieure de Justice, du président du Comité du contentieux du Conseil d'État et du président de la Chambre des comptes)</p>	(L 19 in d' de 2,

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	B
PAYS-BAS	<p>Militaire Inlichtingendienst MID, ou bien MIVD plus récemment</p> <p>sous l'autorité du ministère de la défense</p>	<p><i>Wet op de inlichtingen- en veiligheidsdiensten</i> Loi 635/87 du 3 décembre 1987, dernier amendement loi 194/1999 du 19 avril 1999.</p>	<p>service de renseignement militaire; collecte d'informations sur les armées étrangères</p>	<p>oui</p>	<p><i>Tweede-Kamercommissie voor de Inlichtingen- en veiligheidsdienst</i> "Commission auprès de la 2e Chambre des services de renseignements et de sécurité intérieure"</p> <p>Commission parlementaire</p> <p>(4 membres: présidents des 4 partis les plus grands)</p>	<p>17 or Ka G "F Cl Ar po d' S</p>
PAYS-BAS	<p>Binnenlandse Veiligheidsdienst (BVD) ou bien le AIVD plus récemment)</p> <p>sous l'autorité du ministère de l'intérieur</p>	<p>[Actuellement en discussion une toute nouvelle loi]</p>	<p>service de renseignement intérieur; lutte contre l'extrémisme de droite et de gauche; contre-espionnage</p>			

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
PORTUGAL	<p>Serviço de Informações Estratégicas de Defesa e Militares (SIEDM)</p> <p>dépend du ministre de la défense</p>	<p>Loi 30/84 du 5 septembre 1984, modifiée par la loi 4/95 du 21 février 1995; loi 15/96 du 30 avril 1996; et loi 75-A/97 du 22 juillet 1997</p>	<p>service de renseignement pour l'étranger; service de renseignements stratégiques sur les questions politiques, militaires et économiques</p>		<p><i>Conselho de Fiscalização dos Serviços de Informações (CFSI)</i>. organe composé de trois citoyens élus par l'Assemblée de la République (parlement) pour un mandat de quatre ans</p>	l'in de da pr m
PORTUGAL	<p>Serviço de Informações de Segurança (SIS)</p> <p>dépend du ministère de l'intérieur</p>		<p>service de sécurité pour les affaires intérieures; sauvegarde de la Constitution (sans compétences exécutives); collecte et analyse d'informations sur les activités criminelles et subversives</p>		<p>une commission parlementaire de l'Assemblée de la République peut auditionner les directeurs du SIS et du SIEDM</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseigne- ment électro- magnétique	Organe de contrôle	B
ESPAGNE	<p>Centro Superior de Información de la Defensa (CESID)</p> <p>sous l'autorité du ministère de la défense</p>	<p><i>R.D. 2632/1985 de 27.12.1985 (BOE 20.01.1986) Estructura interna y relaciones del Centro Superior de la Defensa;</i> <i>modif. par R.D. 266/1996 de 16.02.1996 Modif. de la estructura organica del CESID</i></p>	<p>service de renseignement pour l'étranger et le territoire national; recherche d'informations politiques, économiques, technico-scientifiques et militaires; surveillance des services étrangers de renseignement; contre-espionnage dans le pays et à l'étranger</p>	<p>oui</p>	<p>aucun organe spécifique de contrôle; contrôle parlementaire général sous la forme de l'audition d'organes gouvernementaux par des commissions parlementaires</p>	
ESPAGNE	<p>Dirección General de la Guardia Civil (GC)</p> <p>sous l'autorité du ministère de la défense et du ministère de l'intérieur</p>	<p><i>L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad</i></p>	<p>autorité centrale de police paramilitaire comportant un service de renseignement de police; lutte contre la prolifération de la criminalité organisée sur le territoire espagnol</p>			

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle	B
ESPAGNE	<p>Dirección General de la Policia</p> <p>sous l'autorité du ministère de l'intérieur</p>		<p>autorité centrale de police comportant un service de renseignement de police;</p> <p>activités de renseignement sur le territoire national et à l'étranger;</p> <p>lutte contre les structures terroristes et le fondamentalisme islamiste au Moyen-Orient et en Afrique du Nord</p>			

Pays	Service de renseignement	Base juridique	Missions	Renseignement électro-magnétique	Organe de contrôle
SUÈDE	<p>Säkerhetspolisen (SÄPO) service civil de renseignement et de sécurité</p> <p>dépend du ministre de la justice</p>	<p><i>Polislag (1984:387)</i> <i>Förordning (1989:773) med instruktion för Rikspolisstyrelsen</i></p> <p>"loi (1984/387) relative aux services de police, ordonnance (1989/773) portant application de la directive relative à l'Office national de police" (NPB)</p>	<ul style="list-style-type: none"> - contrôle de la sécurité - contre-espionnage - lutte contre le terrorisme - "protection de la Constitution" <p>effectif en 1999: 800 personnes environ</p> <p>budget en 1995: SEK 475 millions (€ 55,7 millions)</p>		<p>conseil exécutif de l'Office national de police, composé de cinq parlementaires, de deux agents et du directeur général de la police nationale</p> <p><i>Registernämnd</i>, composé de huit membres au maximum; siègent actuellement deux "magistrats", deux parlementaires, un avocat et un expert</p> <p>ces deux organes rendent compte au gouvernement</p>
SUÈDE	<p>Militära Underrättelse och Säkerhetstjänsten (MUST)</p> <p>"direction du renseignement et de la sécurité militaires, placée auprès de l'État major suédois</p> <p>Service de renseignement et de sécurité militaire</p> <p>sous l'autorité du ministre de la défense</p>	<p>Loi 2000/130 et ordonnance 2000/131 relatives aux services de renseignement militaire</p>	<p>Collecte et analyse d'informations militaires et politiques secrètes; contre-espionnage; lutte contre la subversion, le sabotage et les émeutes; protection des forces armées et de l'industrie de l'armement</p>		<p><i>Försvarets underrättelsenämnd</i></p> <p>commission de contrôle du service de renseignement de défense; composée, pour partie, de parlementaires</p>

Pays	Service de renseignement	Base juridique	Missions	Renseignem- ent électro- magnétique	Organe de contrôle
SUÈDE	Försvarets Radioanstalt (FRA) Unité spéciale autonome (station radio)		renseignements militaires ou autres; déchiffrement des communications; surveillance radar	oui	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	B
ROYAUME-UNI	<p>Government's Communication Headquarters (GCHQ)</p> <p>sous l'autorité du ministre des affaires étrangères</p>	<i>Intelligence Services Act 1994</i>	espionnage à l'étranger/collecte d'informations à l'étranger; renseignement électromagnétique dans les domaines politique, économique, technico-scientifique et militaire	oui	<p>Le <i>Security Service Commissioner</i> est nommé par le premier ministre; haut juge en exercice ou honoraire.</p> <p><i>The Investigatory Powers Tribunal</i></p>	
	<p>Secret intelligence Service (SIS) = MI6</p> <p>sous l'autorité du ministre des affaires étrangères</p>	<i>Intelligence Services Act 1994</i>	collecte d'informations sur les activités de renseignement et les événements politiques à l'étranger		<p><i>The Intelligence and Security Committee (ISC)</i></p> <p>La commission se compose de 9 membres (Chambre des Communes +Chambre des Lords; aucun membre ne peut être ministre), nommés par le premier ministre</p>	

Pays	Service de renseignement	Base juridique	Missions	Renseignements électromagnétique	Organe de contrôle	B
ROYAUME-UNI	Defense Intelligence Staff (DIS) sous l'autorité du ministre de la défense		soutien de la sécurité militaire; évaluation et analyse d'informations militaires, politiques et technico-scientifiques et de certaines informations économiques			

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
ÉTATS-UNIS	Central Intelligence Agency (CIA)	<i>National Security Act 1947</i>	collecte de renseignements à l'échelon mondial; contre-espionnage à l'étranger; compétences centrales pour toutes les affaires relatives aux services de renseignement aux États-Unis.		Senate: Senate Select Committee on Intelligence (SSCI) House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)
ÉTATS-UNIS	Defense Intelligence Agency (DIA)	créée par la <i>Directive 5105.21</i> de 1961, par le ministre de la défense <i>Executive Order 11905</i> de 1976 <i>DoD Directive 5105.21</i> <i>1978 Executive Order 12036</i> <i>1981 Executive Order 12333</i>	compétente pour fournir des renseignements militaires aux troupes d'assaut et aux décideurs du ministère de la défense et du gouvernement.		Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)
ÉTATS-UNIS	National Security Agency (NSA)	<i>Executive Order 12333 of 4 December 1981</i>	compétente pour la sécurité des systèmes d'information américains, en particulier pour le cryptage; compétente pour la surveillance des communications à l'étranger.	oui	Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)
ÉTATS-UNIS	National Imagery and Mapping Agency (NIMA)	<i>National Imagery and Mapping Agency Act of 1996.</i>	compétente pour fournir images et cartes et les exploiter.		Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)
ÉTATS-UNIS	National Reconnaissance Office (NRO)		compétente pour développer et mettre en œuvre des systèmes de satellites		Senate Select Committee on Intelligence (SSCI) House Permanent

Pays	Service de renseignement	Base juridique	Missions	Rensei- gnement électro- magnétique	Organe de contrôle
			d'espionnage (SIGINT, image)		<i>Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	US Army Intelligence (p. ex. Deputy Chief of Staff for Intelligence, Intelligence and Security command (INSCOM))	<i>Executive Order 12333</i> (4 décembre 1981)	collecte d'informations et analyse en matière militaire; mise au point de concepts et de systèmes de renseignement militaires et guerre électronique.	oui	<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	Marine Corps Intelligence Activity (MCIA) National Maritime Intelligence Center (NMIC)	<i>Executive Order 12333</i> (4 décembre 1981)	renseignements destinés à la Marine; renseignements militaires et mise au point de cryptage et d'auxiliaires électroniques à la guerre.	oui	<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	Office of Naval Intelligence (ONI)	<i>Executive Order 12333</i> (4 décembre 1981)	renseignements à l'intention de la Navy, questions maritimes; analyse des flottes étrangères; collecte de renseignements sur les systèmes de surveillance des océans, les plates-formes sous-marines et les systèmes d'armement.	oui	<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	Air Intelligence Agency (AIA)	<i>Executive Order 12333</i> (4 décembre 1981)	renseignement à destination de l'Airforce; renseignement militaire	oui	<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	Federal Bureau of Investigation (FBI)	<i>Title 28, United States Code (U.S. Code), Section 533</i> créé en 1908; son nom existe depuis 1935.	contre-espionnage; police fédérale		<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on Intelligence (HPSCI)</i>
ÉTATS-UNIS	Drug Enforcement Administration	<i>Executive Order du 1^{er} juillet 1973</i>	collecte d'informations sur la drogue et le blanchiment d'argent sur le territoire		<i>Senate Select Committee on Intelligence (SSCI)</i> <i>House Permanent Select Committee on</i>

Pays	Service de renseignement	Base juridique	Missions	Rensei- gnement électro- magnétique	Organe de contrôle
			national et à l'étranger		<i>Select Committee on Intelligence (HPSCI)</i>
CANADA	Communication Security Establishment (CSE); assistée par le Canadian Forces Supplementary Radio System (CFSRS)	le mandat formel est classifié; il est vraisemblablement fixé avec l'accord du cabinet.	conseiller le gouvernement et les milieux économiques sur les questions de sécurité relatives à la transmission et au traitement des données (Infosec); mettre au point des systèmes de cryptage.	oui	pas d'autorité de contrôle indépendante (uniquement un contrôle par l'Auditor General et le ministre de la défense, lequel est responsable devant le parlement)
CANADA	Canadian Security Intelligence Service (CSIS) sous l'autorité du ministre de l'intérieur	<i>Canadian Security Intelligence Service Act (CSIS Act)</i> de 1984	contre-espionnage, lutte contre le sabotage et le terrorisme international sur le territoire national.		The Security Intelligence Review Committee (SIRC) organe indépendant, composé de 5 membres, qui ne sont pas des parlementaires
CANADA	Director General Intelligence Division (membre du <i>Deputy Chief of the Defence Staff</i>) sous l'autorité du ministre de la défense		renseignement militaire		
AUSTRALIE	Defence Signals Directorate (DSD) sous l'autorité du ministre de la défense		collecter et traiter les renseignements électromagnétiques; fournir au gouvernement et aux forces militaires des produits de sécurité de l'information (Infosec).		<i>Inspector General of Intelligence and Security (IGIS)</i> (nommé par le premier ministre)
AUSTRALIE	Defence Intelligence Organisation (DIO) sous l'autorité du ministre de la défense		collecter et évaluer informations et renseignements stratégiques et militaires		<i>Inspector-General of Intelligence and Security (IGIS)</i>
AUSTRALIE	Australian Secret Intelligence Service (ASIS) service d'espionnage sous l'autorité du		collecter des informations concernant l'étranger, en particulier le sud-est asiatique, dans l'intérêt de la sécurité nationale, de		<i>Inspector-General of Intelligence and Security (IGIS)</i>

Pays	Service de renseignement	Base juridique	Missions	Rensei- gnement électro- magnétique	Organe de contrôle
	ministre des affaires étrangères		l'économie et des relations extérieures.		
AUSTRALIE	Australian Security Intelligence Organisation (ASIO)	<i>The Australian Security Intelligence Organisation Act 1979 (the ASIO Act)</i>	protection contre la violence à motivation politique; sécurité des personnes et des biens; lutte contre le terrorisme international et le transfert illégal de technologies.		<i>Parliamentary Joint Committee on the Australian Security Intelligence Organization</i> <i>Inspector-General of Intelligence and Security (IGIS)</i>
AUSTRALIE	Office of National Assessments organe indépendant	<i>Office of National Assessments Act 1977</i>	fait rapport au premier ministre		<i>Inspector-General of Intelligence and Security (IGIS)</i>

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
	militaire sous l'autorité du ministre de la défense		plan militaire, notamment dans l'espace Asie-Pacifique; analyse d'informations tactiques et stratégiques.		