2-754/1 (Senaat)
DOC 50 **1660/001 (Kamer)**

Belgische Senaat en Kamer van volksvertegenwoordigers

ZITTING 2001-2002

25 FEBRUARI 2002

Verslag over het eventuele bestaan van een netwerk voor het onderscheppen van communicaties, «Echelon» genaamd

VERSLAG

NAMENS DE COMMISSIE BELAST MET DE BEGELEIDING VAN HET VAST COMITÉ VAN TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN (SENAAT)
EN
DE BIJZONDERE COMMISSIE BELAST MET DE PARLEMENTAIRE BEGELEIDING VAN HET VAST COMITÉ VAN TOEZICHT OP DE POLITIEDIENSTEN (KAMER)
UITGEBRACHT DOOR
MEVROUW **LIZIN** (S) EN
DE HEER **VAN PARYS** (K)

Aan de werkzaamheden van de commissies hebben deelgenomen:

A. Senaat:

Leden: de heren De Decker, voorzitter; Dedecker, Hordies, mevrouw Taelman, de heer Vandenberghe en mevrouw Lizin, rapporteur.

B. Kamer van volksvertegenwoordigers:

Leden: de heren De Croo, voorzitter; Bacquelaine, Coveliers, De Man, Detremmerie, Larcier, mevrouw Pelzer-Salandra, de heren Vandenhove, Van Hoorebeke en Van Parys, rapporteur.

2-754/1 (Sénat)
DOC 50 **1660/001 (Chambre)**

Sénat et Chambre des représentants de Belgique

SESSION DE 2001-2002

25 FÉVRIER 2002

Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé «Echelon»

RAPPORT

FAIT AU NOM DE LA COMMISSION CHARGÉE DU SUIVI DU COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ (SÉNAT)
ET DE LA COMMISSION SPÉCIALE CHARGÉE DE L'ACCOMPAGNEMENT PARLEMENTAIRE DU COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE POLICE (CHAMBRE)
PAR MME **LIZIN** (S) ET
M. **VAN PARYS** (Ch)

Ont participé aux travaux des commissions:

A. Sénat:

Membres: M. De Decker, président; Dedecker, Hordies, Mme Taelman, M. Vandenberghe et Mme Lizin, rapporteuse.

B. Chambre des représentants:

Membres: MM. De Croo, président; Bacquelaine, Coveliers, De Man, Detremmerie, Larcier, Mme Pelzer-Salandra, MM. Vandenhove, Van Hoorebeke et Van Parys, rapporteur.

INHOUD

SOMMAIRE

1. INLEIDING

1.1. Aanleiding tot het opstellen van dit verslag

In de loop van 1998 werden er in het Belgisch Parlement verschillende vragen gesteld over het mogelijke bestaan van Echelon, een interceptiesysteem van de communicatiemiddelen en de bescherming die de Europese en Belgische wetgeving hiertegen bood aan burgers en bedrijven (1).

Vertrekpunt voor deze parlementaire bezorgdheid over de interceptie van communicatiestromen was een tussentijds verslag, «*An Appraisal of the Technology of Political Control*» (Une évaluation des techniques de contrôle politique) (PE 166 499), dat door de Omega Foundation uit Manchester werd voorgesteld aan het STOA Panel (2) op 18 december 1997 en aan de Commissie voor de burgerlijke vrijheden en rechten, de justitie en de binnenlandse aangelegenheden van het Europees Parlement op 27 januari 1998. Het definitieve verslag werd door STOA onder dezelfde titel officieel gepubliceerd in september 1998.

In het tussentijds verslag wordt gesteld dat vijf landen (de Verenigde Staten van Amerika, het Verenigd Koninkrijk, Canada, Australië en Nieuw Zeeland), op grond van een geheimgehouden akkoord («UK-USA-agreement»), reeds jarenlang het e-mail-, telefoon- en faxverkeer over de hele wereld onderscheppen. Het Echelon-systeem maakt het mogelijk om uit die massa onderschepte communicatie automatisch de nuttige elementen te filteren door het gebruik van krachtige computers die werken met sleutelwoorden.

Op 10 november 1998 heeft de voorzitter van de bijzondere Kamercommissie belast met de begeleiding van het Vaste Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingendiensten («Comité I»), de heer R. Delathouwer, aan het Comité I gevraagd om een toezichtsonderzoek te openen om na te gaan op welke de wijze onze inlichtingendiensten reageren op het eventuele bestaan van een Amerikaans systeem, genaamd Echelon, dat dient om het fax- en telefoonverkeer te onderscheppen. Tevens werd gevraagd om te onderzoeken of onze inlichtingendiensten proberen bewijzen te verzamelen over het bestaan van dit interceptiesysteem en op welke manier ze proberen onze burgers te beschermen tegenover dit systeem.

1.2. De verslagen van het Vast Comité van Toezicht op de Inlichtingendiensten

In het eerste verslag dat door het Comité I op 5 augustus 1999 werd goedgekeurd kwam het tot de volgende conclusies (3):

«De Belgische inlichtingendiensten beschikken niet over de technische mogelijkheden om zelf het

1. INTRODUCTION

1.1. Motif de la rédaction du présent rapport

Au cours de l'année 1998, plusieurs questions ont été posées au Parlement belge sur l'existence éventuelle d'Echelon, un système d'interception des communications, et sur la protection que la législation européenne et la législation belge offrent aux citoyens et aux entreprises contre ce système (1).

L'inquiétude des parlementaires à propos de l'interception des communications a été suscitée par une étude intérimaire intitulée «Une évaluation des techniques de contrôle politique» (PE 166 499), qui a été présentée par la Fondation Omega de Manchester au Groupe du STOA (2) lors de sa réunion du 18 décembre 1997 et à la commission des libertés et des droits des citoyens, de la justice et des Affaires intérieures le 27 janvier 1998. Le STOA a publié officiellement l'étude définitive, sous le même titre, en septembre 1998.

Selon l'étude intérimaire, cinq pays (les États-Unis d'Amérique, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande) interceptent depuis des années les communications électroniques, téléphoniques et par fax dans le monde entier, sur la base d'un accord secret («le pacte UK-USA»). Le système Échelon permet de filtrer automatiquement les éléments utiles de cette masse de communications interceptées en utilisant de puissants ordinateurs qui opèrent à l'aide de mots clés.

Le 10 novembre 1998, le président de la Commission spéciale de la Chambre chargée du suivi du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements («Comité R»), M. Delathouwer, a demandé au Comité R d'ouvrir une enquête de contrôle sur la manière dont nos services de renseignements réagissent à l'existence éventuelle d'un système américain, nommé Echelon, servant à intercepter les communications par fax et par téléphone. En outre, il a demandé au même comité d'examiner si nos services de renseignements tentent de rassembler des preuves de l'existence de ce système d'interception et de quelle manière ils s'efforcent de protéger nos citoyens contre celui-ci.

1.2. Les rapports du Comité permanent de contrôle des services de renseignements et de sécurité

Le premier rapport, qui a été approuvé par le Comité R le 5 août 1999, arrivait aux conclusions suivantes (3):

«Les services de renseignements belges n'ont pas la possibilité technique de constater eux-mêmes

bestaan van het systeem « Echelon » vast te stellen. Al wat ze over dit systeem weten, hebben ze uit open bronnen gehaald.

De Veiligheid van de Staat kon niet bewijzen of er wel degelijk sprake is van operaties waarbij telecommunicaties worden onderschept. Deze dienst verklaart dat hij kampt met een tekort aan zowel personele als materiële middelen. De onderzoeksmiddelen waarover deze dienst beschikt laten hem niet toe na te gaan of het systeem « Echelon » wel degelijk bestaat.

Van zijn kant twijfelt de Algemene Dienst Inlichting en Veiligheid (ADIV) niet aan het bestaan van een interceptiesysteem van het type « Echelon ».

...

ADIV voert echter geen actief onderzoek naar het systeem « Echelon » en steunt daarvoor enerzijds op het feit dat een dergelijk onderzoek geen deel uitmaakt van zijn bevoegdheden die beschreven staan in de wet van 30 november houdende regeling van de Inlichtingen- en Veiligheidsdiensten, en anderzijds op de wettelijke beperkingen betreffende het onderscheppen van radiocommunicaties. »

Ter zake laat het comité niet na aan te stippen dat artikel 7, 1º van de bovenvermelde wet de Veiligheid van de Staat de volgende opdracht toevertrouwt :

« ...

1º het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elk activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het ministerieel Comité, bedreigt of zou kunnen bedreigen;

... »

Artikel 11, § 1, 3º van bovenvermelde wet geeft de Algemene Dienst inlichting en veiligheid (ADIV) trouwens als opdracht :

« ...

3º het beschermen van het geheim dat, (...) verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert;

... »

In zijn aanbevelingen (4) benadrukt het Comité I dat, om ongeoorloofde COMINT-activiteiten (5)

l'existence du système « Echelon ». Leur connaissance du sujet résulte de la consultation de sources ouvertes.

La Sûreté de l'État n'a pas été en mesure de confirmer l'existence de pratiques d'interception de télécommunications. Ce service se déclare confronté à un manque de moyens, tant sur le plan du personnel que sur le plan du matériel. Ses moyens d'investigation ne lui permettent donc pas de vérifier l'existence du systéme « Echelon ».

Le Service général de renseignement et de sécurité (SGR) considère quant à lui l'existence d'un système d'interception de type « Echelon » comme un fait acquis.

...

Le SGR n'effectue cependant pas de recherche active sur le programme « Echelon », se fondant, d'une part, sur le fait qu'il ne s'agit pas d'une de ses compétences définies dans la loi organique du 30 novembre 1998 des services de renseignement et, d'autre part, sur les restrictions légales en matière de captation de radiocommunications. »

À cet égard, le comité ne manque pas de souligner que l'article 7, 1º, de la loi précitée confie à la Sûreté de l'État la mission suivante :

« ...

1º rechercher, analyser et traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État et les relations internationales, le potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel;

... »

L'article 11, § 1er, 3º, de la loi précitée charge d'ailleurs le Service général de renseignement et de sécurité (SGR) :

« ...

3º de protéger le secret qui (...) s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense nationale gère;

... »

Dans ses recommandations (4), le Comité R a souligné que, pour lutter contre le phénomène d'activités

tegen te gaan, er nog veel meer aandacht zal moeten besteed worden aan de veiligheid van de informaticasystemen.

Het Comité I treedt de ADIV bij die meent dat de overheden moeten gesensibiliseerd worden over deze problematiek.

Op vraag van de parlementaire begeleidingscommissies heeft het Comité I regelmatig tussentijdse verslagen ingediend over het dossier Echelon. In zijn laatste activiteitenverslag (6) heeft het Comité I een voorlopige synthese gemaakt van al zijn bevindingen. Uiteraard zal het Comité I dit dossier verder blijven opvolgen.

Aangestipt dient te worden dat de parlementaire begeleidingscommissies het Comité I eveneens hebben belast met het onderzoek naar een aantal nevendossiers die mogelijk verband houden met Echelon. Zo is het Comité I gevraagd om een toezichtsonderzoek te voeren naar de pogingen tot indringing in het computersysteem van een universitair onderzoekscentrum (7). Eveneens werd gevraagd om na te gaan of er in de zaak « Lernout en Hauspie » geen sprake kan zijn van een georchestreerde campagne. Het specifieke terrein waarop L&H actief is, de spraakherkenning, is een gebied waarvoor de inlichtingendiensten betrokken bij Echelon een zeer hoge belangstelling moeten koesteren.

In zijn laatste activiteitenverslag komt het Comité I tot de volgende conclusies.

1. wat het bestaan van Echelon betreft, stelt het Comité vast dat noch het bestaan, de omvang of het gebruik van een interceptienetwerk officieel erkend wordt door de betrokken regeringen;

2. wel staat het buiten kijf dat de Verenigde Staten en het Verenigd Koninkrijk over officiële inlichtingendiensten beschikken, respectievelijk de *National Security Agency (NSA)* en de *Government Communications Headquarters (GCHQ)*, die belast zijn met het onderscheppen van telecommunicaties;

3. het bestaan van het UKUSA-verdrag en dat van een technische samenwerking tussen de interceptieorganismen van de vijf Angelsaksische landen is intussen officieel erkend;

4. de technische mogelijkheden van deze diensten zijn enorm : het systeem zou alle communicatie die via satellieten verloopt kunnen opgevangen; toch is er nog geen volledig toezicht op alle telefonische communicatie via een systeem van trefwoorden; momenteel kan enkel, via systemen van stemherkenning, de internationale communicatie van een specifiek persoon worden opgespoord;

5. de omvang van de ingezamelde gegevens doet twijfels rijzen over de beheerbaarheid van het systeem;

COMINT illégitimes (5), il faudra accorder encore beaucoup plus d'attention à la sécurité des systèmes informatiques.

Le Comité R rejoint le SGR lorsqu'il estime que les autorités doivent être sensibilisées à ce problème.

À la demande des commissions parlementaires de suivi, le Comité R a régulièrement présenté des rapports intermédiaires concernant le dossier Échelon. Dans son dernier rapport d'activités (6), le Comité R a fait une synthèse provisoire de toutes ses constatations. Il va de soi que le Comité R assurera le suivi de ce dossier.

Il convient de noter que les commissions parlementaires du suivi ont également chargé le Comité R d'examiner un certain nombre de dossiers annexes susceptibles de présenter un lien avec Echelon. Il a ainsi été demandé au comité d'effectuer une enquête de contrôle sur les tentatives d'intrusion dans le système informatique d'un centre universitaire de recherches (7). Il lui a également été demandé d'examiner si, dans l'affaire « Lernout et Hauspie », on ne pouvait pas parler d'une campagne orchestrée. Le terrain spécifique sur lequel L&H est actif, celui de la reconnaissance vocale, est un domaine auquel les services de renseignement impliqués dans Echelon doivent s'intéresser au plus haut point.

Dans son dernier rapport d'activités, le comité R arrive aux conclusions suivantes :

1. en ce qui concerne l'existence d'Echelon, le comité constate que ni l'existence, ni l'étendue, ni l'utilisation d'un réseau d'interception ne sont officiellement reconnues par les gouvernements concernés;

2. toutefois, il ne fait aucun doute que les États-Unis et le Royaume-Uni disposent de services de renseignement officiels, respectivement la *National Security Agency (NSA)* et le *Government Communications Headquarters (GCHQ)*, qui sont chargés de l'interception des télécommunications;

3. l'existence du pacte UKUSA et celle d'une collaboration technique entre les organismes d'interception des cinq pays anglo-saxons ont, entre-temps, été officiellement reconnues;

4. les ressources techniques et humaines de ces services sont énormes : le système serait en mesure de capter toutes les communications qui se font par satellites; il n'offre toutefois pas encore à l'heure actuelle, un aperçu complet de toutes les communications téléphoniques obtenues par le biais d'une grille de mots clés; il permet seulement, par des dispositifs de reconnaissance vocale, de détecter les communications internationales d'une personne spécifique;

5. l'ampleur des données récoltées amène à douter que ce système soit gérable;

6. er bestaan ernstige aanwijzingen dat het systeem wordt gebruikt voor economische spionage;

7. een dergelijk interceptiesysteem vormt ongetwijfeld een aanslag op het privé-leven van de burgers en overtreedt de Europese regels i.v.m. de interceptie van telecommunicatie.

Het Comité I doet de volgende aanbevelingen (8):

— vaststellende dat de Belgische inlichtingendiensten geen enkele taak van informatiewinning en -analysering hebben uitgevoerd met betrekking tot het mogelijk bestaan van een interceptienetwerk voor telecommunicaties, genaamd Echelon, dat gestuurd zou worden door de Verenigde Staten en Groot-Brittannië;

— in overweging nemende dat dit netwerk hoogstwaarschijnlijk bestaat, zonder daarvoor een sluitend bewijs te hebben;

— in overweging nemende dat algemeen gezien de huidige technologieën de mogelijkheden bieden aan zowel landen als criminele organisaties om op grote schaal telecommunicaties te onderscheppen;

— in overweging nemende dat deze handelswijze een geschikte manier is om vertrouwelijke informaties te vergaren betreffende de veiligheid of het wetenschappelijk en economisch potentieel van een land door een buitenlandse macht of door een criminele organisatie;

— ...

herhaalt het Vast Comité I de aanbevelingen die het formuleerde naar aanleiding van het samenvatten van de voorgaande verslagen aangaande dit onderwerp:

— om bijgevolg als opdracht te geven aan de Belgische inlichtingendiensten om samen te werken teneinde elke beschikbare informatie (van open bronnen of andere) aangaande elke bestaande dreiging van interceptie van communicaties die gericht is tegen België;

— om aan de inlichtingendiensten de technische en menselijke middelen te verlenen die noodzakelijk zijn om deze opdracht te vervullen;

— om wettelijk toegelaten technische middelen te verlenen, dit wil zeggen, een wettelijk kader te verstrekken teneinde op een selectieve en strikt gecontroleerde wijze opsporingen te verrichten en communicaties te onderscheppen en af te luisteren;

— om de nodige menselijke middelen toe te kennen, dit wil zeggen, het gebruik van externe experten, informaticaspecialisten, ingenieurs in telecommunicatie, specialisten in cryptografie, analisten, etc.;

— om als algemeen principe de voorzichtigheid voorop te stellen in de uitwerking van een globaal en gecentraliseerd beleid inzake informatieveiligheid;

6. il existe de sérieux indices selon lesquels le système serait utilisé à des fins d'espionnage économique;

7. pareil système d'interception constitue indubitablement une atteinte à la vie privée des citoyens et enfreint les règles européennes en matière d'interception des télécommunications.

Le Comité R fait les recommandations suivantes (8):

— constatant que les services de renseignement belges n'ont entrepris aucun travail de recueil et d'analyse d'informations à propos de l'existence éventuelle d'un réseau d'interception des communications, appelé « Echelon », et piloté notamment par les États-Unis et la Grande Bretagne;

— considérant l'existence de ce réseau comme hautement vraisemblable, à défaut d'être prouvée;

— considérant de manière plus générale que les possibilités technologiques actuelles permettent, tant aux États qu'aux organisations criminelles, d'intercepter des communications à grande échelle;

— considérant qu'une telle pratique est un moyen adéquat pour une puissance étrangère ou une organisation criminelle, de se procurer des informations confidentielles sur la sécurité, le potentiel scientifique et économique du pays;

— ...

le Comité permanent R réitère les recommandations qu'il a formulées à la suite de l'ensemble de ses rapports précédents sur la question, à savoir:

— donner comme mission à la Sûreté de l'État et au SGR de collaborer en vue de recueillir toute information disponible (de sources ouvertes ou autres) sur toutes menaces d'interception de communications dirigées contre la Belgique;

— donner à ces services de renseignement les moyens légaux, techniques et humains nécessaires pour accomplir cette mission:

— les moyens légaux techniques, c'est-à-dire un cadre légal pour procéder de manière sélective et strictement contrôlée à des repérages, à des écoutes et à des interceptions de communications;

— les moyens humains, c'est-à-dire des experts externes, des informaticiens, des ingénieurs en télécommunications, des spécialistes en cryptographie, des analystes, etc.;

— mettre en œuvre le principe général de précaution dans l'élaboration d'une politique globale et centralisée de sécurisation de l'information;

— om de oprichting van een dienst te overwegen, die belast wordt met het aanbrengen van een oplossing voor het geheel van de problematiek van de beveiliging van de informatie.

1.3. De beslissing om zelf verslag uit te brengen

Gelet op de bevindingen van het tussen tijds verslag «An Appraisal of the Technology of Political Control» dat op 18 december 1997 aan het STOA-panel werd voorgelegd;

Gelet op de elementen en de analyse van het STOA-verslag «Development of surveillance technology and risk of abuse of economic information» (9);

Gelet op de vaststellingen en aanbevelingen van het Comité I in zijn verslagen over het onderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België;

Gelet op de elementen die de begeleidingscommissies zelf via open bronnen over het al dan niet bestaan van een dergelijk interceptiesysteem heeft kunnen verzamelen;

Gelet op de antwoorden die door de Eerste minister, de minister van Justitie en de minister van Landsverdediging werden verstrekt aan de begeleidingscommissies;

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;

Gelet op de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en telecommunicatie;

Gelet op de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens;

Gelet op het Europees Verdrag van de Rechten van de Mens en artikel 8 in het bijzonder dat de bescherming van het privé-leven waarborgt en de verschillende internationale verdragen die dit recht waarborgen;

Gelet op de door verschillende internationale verdragen gewaarborgde vrije handel;

Overwegende dat het eventuele bestaan van een internationaal interceptiesysteem van communicaties fundamentele vragen oproept die betrekking hebben op:

— de onafhankelijkheid, het zelfbeschikkingsrecht en de veiligheid van soevereine Staten,

— envisager la mise en place d'un service chargé d'apporter une solution à l'ensemble de la problématique de la sécurisation de l'information.

1.3. La décision des commissions de rédiger elles-mêmes un rapport

Vu les constatations de l'étude intérimaire intitulée «Une évaluation des techniques de contrôle politique», qui a été présentée le 18 décembre 1997 au groupe du STOA;

Vu les éléments et l'analyse qui figurent dans l'étude du STOA intitulée «Le développement des techniques de surveillance et les risques d'utilisation abusive d'informations économiques (9);

Vu les constatations et les recommandations du Comité R dans ses rapports sur la manière dont «les services belges de renseignements réagissent face à l'éventualité d'un système américain «Echelon» d'interception des communications téléphoniques et par fax en Belgique;

Vu les éléments que les commissions chargées du suivi parlementaire ont pu recueillir elles-mêmes à des sources publiques sur l'existence éventuelle d'un tel système d'interception;

Vu les réponses que le premier ministre, le ministre de la Justice et le ministre de la Défense ont fournies aux commissions du suivi;

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;

Vu la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées;

Vu la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données;

Vu la Convention européenne des droits de l'homme, en particulier son article 8, qui garantit le droit à la protection de la vie privée, et les diverses conventions internationales qui garantissent ce droit;

Vu les diverses conventions qui garantissent la liberté des échanges commerciaux;

Considérant que l'existence éventuelle d'un système international d'interception des communications soulève des questions fondamentales sur:

— l'indépendance, le droit à l'autodétermination et la sécurité des États souverains,

— het respect voor het privé-leven van de burgers,

— de internationaal gewaarborgde vrije handel,

— de bescherming van het wetenschappelijk en industrieel patrimonium van een land;

Overwegende dat deze intercepties, indien ze bestaan, in elk geval gebeuren buiten het medeweten van België, door landen waarmee ons land traditioneel zeer diepe vriendschapsbanden onderhoudt en waarmee het, door internationale verdragen, een militaire alliantie heeft afgesloten;

Overwegende dat deze intercepties, buiten het medeweten van België, mogelijk worden uitgevoerd door een lidstaat van de Europese Unie terwijl zij duidelijk in strijd zijn met de in verschillende verdragen vastgelegde noodzakelijke Europese loyauteit, de gewaarborgde rechten van de Europese burgers en de gewaarborgde vrije handel;

Overwegende dat deze intercepties, indien ze bestaan, de fundamentele belangen, de veiligheid, de handel en de industriële en wetenschappelijke belangen, enerzijds, van België in gevaar kunnen brengen en, anderzijds, van de Europese Unie of van bepaalde lidstaten;

Overwegende dat deze intercepties, indien ze bestaan, door ons land mogen beschouwd als een blijk van wantrouwen in het land en zijn instellingen door landen die het als bevriende naties beschouwt;

Overwegende dat het eventuele bestaan van een dergelijk interceptiesysteem, voor zover het gebeurt buiten het medeweten van ons land en zonder de mogelijkheid van een door ons land uitgeoefende politieke of juridische controle onaanvaardbaar is;

Overwegende dat noch de Belgische inlichtingendiensten, noch het Vast Comité van toezicht enige zekerheid kunnen verschaffen over het al dan niet bestaan van dit systeem;

Overwegende dat het niet tot de wettelijke opdracht van het Comité I behoot om een onderzoek uit te voeren naar de activiteiten van buitenlandse inlichtingen;

Overwegende dat het alleen aan het Parlement toekomt om een afweging te maken van de waarachtigheid van bepaalde gegevens die zeer vergaande gevolgen kunnen hebben voor onze verhouding met andere landen, om een juridische kwalificatie te geven aan deze feiten en om hieraan bepaalde politieke gevolgen aan te verlenen,

meenden de begeleidingscommissies dat zij zelf verslag moesten uitbrengen over het interceptiesysteem dat bekend is geworden onder de naam Echelon en over eventueel andere gelijkaardige systemen die zouden kunnen worden gebruikt door andere landen.

— le respect de la vie privée des citoyens,

— la liberté du commerce, qui est garantie sur le plan international,

— la protection du patrimoine scientifique et industriel d'un pays;

Considérant que ces interceptions, si elles existent, sont pratiquées en tout cas à l'insu de la Belgique, par des pays avec lesquels notre pays entretient traditionnellement des liens d'amitié très étroits et avec lesquels il a conclu une alliance militaire par l'intermédiaire de conventions internationales;

Considérant que ces interceptions pourraient être pratiquées à l'insu de la Belgique par un État membre de l'Union européenne, alors qu'elles sont clairement contraires à l'indispensable loyauté européenne, stipulée dans plusieurs traités, ainsi qu'aux droits garantis aux citoyens européens et à la liberté des échanges commerciaux, elle aussi garantie;

Considérant que ces interceptions, si elles existent, peuvent menacer les intérêts fondamentaux, la sécurité, les échanges commerciaux, ainsi que les intérêts industriels et scientifiques de la Belgique, d'une part, et de l'Union européenne ou de certains de ses États membres, d'autre part;

Considérant que ces interceptions, si elles existent, peuvent être considérées par notre pays comme une preuve de méfiance à son égard et à l'égard de ses institutions, de la part de pays qu'il considère comme des nations amies;

Considérant que l'existence éventuelle de pareil système d'interception est inacceptable, dans la mesure où notre pays n'en a pas connaissance et qu'il ne peut donc exercer aucun contrôle politique ou juridique;

Considérant que ni les services de renseignements belges, ni le Comité permanent de contrôle ne peuvent apporter la moindre certitude quant à l'existence ou non de ce système;

Considérant qu'enquêter sur les activités des services de renseignements étrangers ne fait pas partie des missions légales du Comité R;

Considérant que c'est au seul Parlement qu'il appartient de juger de la véracité de certaines données qui pourraient avoir des répercussions très lourdes sur nos relations avec des pays tiers, de qualifier juridiquement les faits en question et d'en tirer des conclusions politiques;

les commissions du suivi ont estimé qu'elles doivent faire elles-mêmes rapport sur le système d'interception aujourd'hui connu sous l'appellation «Echelon» et éventuellement sur d'autres systèmes analogues qui pourraient être utilisés par d'autres pays.

1.4. Werkwijze van de begeleidingscommissies

Tijdens deze legislatuur werd het interceptiesysteem Echelon een eerste keer besproken door de begeleidingscommissies op 31 januari 2000 bij het onderzoek van het activiteitenverslag 1999 van het Comité I(10) waarin het toezichtsonderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België was opgenomen. Het toezichtsonderzoek dat in het activiteitenverslag is opgenomen was reeds op 8 augustus 1999 goedgekeurd. Aangezien er na die datum nog heel veel bijkomende informatie aan het licht is gekomen bevat het slechts de eerste bevindingen van het Comité I en wordt het later regelmatig aangevuld.

Van deze bespreking van het activiteitenverslag van het Comité I is door de begeleidingscommissies een parlementair verslag opgesteld(11) waarin de bezorgdheid van het Parlement duidelijk tot uitdrukking komt(12). De begeleidingscommissies hebben het Comité dan ook gevraagd om verder informatie in te winnen om meer zekerheid te krijgen over het bestaan ervan.

Tevens werd gevraagd om meer informatie in te winnen over de *International Law Enforcement Telecommunications Seminars* (ILETS) waarvan in het STOA-verslag(13) beweerd wordt dat het sedert 1993, zonder dat de parlementsleden van de betrokken landen dat weten, deelnemers van politie- en inlichtingendiensten van verschillende landen verenigt die zich buigen over het op punt stellen van technische richtlijnen om toegang te krijgen tot computersystemen.

Tijdens hun vergadering van 12 mei 2000 hebben de begeleidingscommissies formeel de beslissing genomen om zelf een verslag op te stellen over het Echelonінterceptiesysteem en hebben mevrouw Lizin (Senaat) en de heer Tony Van Parijs (Kamer) als rapporteurs aangewezen.

Op 19 mei 2000 werd de heer Marc Verwilghen, als minister van Justitie bevoegd voor de Veiligheid van de Staat, gehoord over het standpunt van de Belgische regering over het Echelonsysteem en de juridische middelen die er eventueel tegen kunnen worden ingebracht.

Op de vergadering van 30 juni 2000 werd het aanvullend activiteitenverslag 1999 van het Comité I besproken en ook over de bespreking van dit verslag werd door de begeleidingscommissies een verslag uitgebracht(14).

Op 14 juni 2000 heeft senator Lizin een onderhoud gehad met de heer Arthur Paecht, député van de Franse Assemblée Nationale die rapporteur was van

1.4. Méthode de travail des commissions du suivi

Au cours de la législature actuelle, les commissions du suivi ont discuté une première fois du système d'interception Echelon le 31 janvier 2000, à l'occasion de l'examen du rapport d'activités 1999 du Comité R(10) dans lequel figurait le rapport d'enquête sur la manière dont les services belges de renseignements réagissent face à l'éventualité d'un système américain «Echelon» d'interception des communications téléphoniques et fax en Belgique. Le rapport concernant l'enquête de contrôle qui figure dans le rapport d'activités avait été approuvé dès le 8 août 1999. Comme de nombreuses informations supplémentaires ont encore été découvertes après cette date, il ne contient que les premières constatations du Comité R et sera régulièrement complété par la suite.

Cette discussion du rapport d'activités du Comité R a fait l'objet d'un rapport parlementaire des commissions du suivi(11) dans lequel transparaît clairement l'inquiétude du Parlement(12). Les commissions du suivi ont dès lors demandé au comité de continuer à rassembler des informations afin d'avoir plus de certitude quant à l'existence du système.

Il lui a aussi été demandé de recueillir davantage d'informations sur les *International Law Enforcement Telecommunications Seminars* (ILETS), dont le rapport STOA(13) affirme qu'ils rassemblent depuis 1993, à l'insu des parlementaires des pays concernés, des participants des services de police et de renseignements de divers pays pour étudier la mise au point de directives techniques en vue d'avoir accès aux systèmes informatiques.

Au cours de leur réunion du 12 mai 2000, les commissions du suivi ont pris la décision formelle de faire elles-mêmes rapport sur le système d'interception «Echelon» et désigné comme rapporteurs Mme Lizin (Sénat) et M. Tony Van Parijs (Chambre).

Le 19 mai 2000, M. Marc Verwilghen, qui, en tant que ministre de la Justice, a la Sûreté de l'État dans ses compétences, a été entendu sur le point de vue du gouvernement belge concernant le système Echelon et sur les moyens juridiques que l'on peut éventuellement lui opposer.

Au cours de la réunion du 30 juin 2000, on a examiné le rapport d'activités 1999 complémentaire du Comité R, dont la discussion a, elle aussi, fait l'objet d'un rapport des commissions du suivi(14).

Le 14 juin 2000, Mme Lizin a eu un entretien avec M. Arthur Paecht, député de l'Assemblée nationale française, qui a été rapporteur d'information à la

een informatierapport van de « Commission de la défense nationale et des forces armées » (15) over Echelon.

Tijdens de vergadering van 19 juli 2000 werd de heer Guy Verhofstadt, eerste minister, gehoord om te overleggen over de stappen die de regering en het Parlement kunnen ondernemen.

Na deze vergaderingen werden er nog verschillende vergaderingen gehouden met het Comité I om op de hoogte te blijven van de verschillende aanvullende verslagen die door het Comité aan de begeleidingscommissies werden overgemaakt.

Op 7 en 17 november 2000 werden hoorzittingen gehouden met mevrouw Godelieve Timmermans, administrateur-generaal van de Veiligheid van de Staat over Echelon en de deelname van de Veiligheid van de Staat aan ILETS.

Tijdens de vergaderingen van 18 april, 21 april en 6 juni 2001 werden het activiteitenverslag 2000 van het Comité I besproken waarbij opnieuw ruime aandacht werd geschonken aan de opvolging van het dossier Echelon.

Op 6 juni 2001 hebben de begeleidingscommissies een hoorzitting gehouden met de heer Duncan Campbell, onderzoeksjournalist, die een belangrijke bijdrage heeft geleverd over het aan het licht komen van het Echelon-interceptiesysteem en auteur van verschillende verslagen voor het STOA-panel.

Op 26 juni 2001 heeft de begeleidingscommissie een hoorzitting gehouden met de heer Dimitri Yernault, assistent van de ULB, en de heer Paul Thomas, voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer, over de juridische gevolgen van het Echelon-systeem.

In het kader van dit verslag hebben de begeleidingscommissies zelf zoveel mogelijk informatie over Echelon verzameld. Ook is regelmatig contact gehouden met de tijdelijke onderzoekscommissie van het Europees Parlement over het interceptiesysteem Echelon. Aangestipt kan worden dat zowel de voorzitter van de parlementaire begeleidingscommissie van de Senaat, de heer Armand De Decker, voorzitter van de Senaat, als senator Lizin, rapporteur, werkvergaderingen hebben bijgewoond van de tijdelijke commissie van het Europees Parlement.

2. BEWAKINGSTECHNOLOGIE (16)

2.1. Enkele begrippen

Hoewel over het interceptiesysteem dat bekend is geworden onder de naam « Echelon » in de media veel inkt is gevloeid wordt meestal verwezen naar dezelfde originele bronnen (17) die het bestaan van Echelon

Commission de la défense nationale et des forces armées (15) sur la question d'Echelon.

Au cours de la réunion du 19 juillet 2000, le premier ministre, M. Guy Verhofstadt, a été entendu en vue d'une concertation sur les mesures que peuvent prendre le gouvernement et le Parlement.

Par la suite, plusieurs autres réunions ont encore eu lieu avec le Comité R en vue de prendre connaissance des différents rapports complémentaires que le Comité a transmis aux commissions du suivi.

Les 7 et 17 novembre 2000 ont eu lieu des auditions de Mme Godelieve Timmermans, administrateur général de la Sûreté de l'État, sur Echelon et la participation de la Sûreté de l'État à des ILETS.

Au cours des réunions des 18 avril, 21 avril et 6 juin 2001, on a examiné le rapport d'activités 2000 du Comité R, en accordant à nouveau une grande attention au suivi du dossier Echelon.

Le 6 juin 2001, les commissions du suivi ont entendu M. Duncan Campbell, journaliste d'investigation, qui a largement contribué à faire connaître l'existence du système d'interception Échelon, et par ailleurs auteur de plusieurs rapports pour le groupe du STOA.

Le 26 juin 2001, la commission du suivi a entendu M. Dimitri Yernault, assistant à l'ULB, et M. Paul Thomas, président de la Commission de la protection de la vie privée, sur les conséquences juridiques du système Echelon.

Dans le cadre du présent rapport, les commissions du suivi ont elles-mêmes rassemblé le plus d'informations possible au sujet d'Echelon. Elles ont en outre été régulièrement en contact avec la commission d'enquête temporaire du Parlement européen sur le système d'interception Echelon. On peut noter que tant le président de la commission parlementaire du suivi du Sénat, M. Armand De Decker, président du Sénat, que la sénatrice et la rapporteuse de la commission, Mme Lizin, ont assisté à des réunions de travail de la commission du Parlement européen.

2. TECHNOLOGIE DE SURVEILLANCE (16)

2.1. Notions

Bien que les médias aient abondamment parlé du système d'interception aujourd'hui connu sous l'appellation « Echelon », on se réfère le plus souvent aux mêmes sources (17) d'origine qui en ont dévoilé l'exis-

aan het licht hebben gebracht zonder dat iemand die heeft gelezen, laat staan dat de bronnen waarnaar in die teksten verwezen wordt kritisch worden doorgenomen.

Op die manier is het begrip Echelon in de media een eigen leven gaan leiden en worden de technische mogelijkheden om telecommunicatie te onderscheppen tot bijna mythische proporties opgeblazen.

In elk geval is duidelijk dat het werk van inlichtingendiensten mee is geëvolueerd met de technologische ontwikkeling op het vlak van communicatie. De ontwikkeling van radioverbindingen, satellieten, glasvezelkabels en de steeds ruimere mogelijkheden die hierdoor geboden werden om op internationaal vlak steeds meer informatie uit te wisselen via telefoon, fax en e-mail is op de voet gevolgd door de «bewakingstechnologie».

De ontwikkeling van steeds krachtiger computers heeft het bovendien mogelijk gemaakt om de grote hoeveelheden onderschepte informatie automatisch te filteren via sleutelwoorden.

Om het overzicht te behouden in het geheel van het jargon dat in de wereld van de inlichtingendiensten gebruikt wordt lijkt het nuttig om een aantal begrippen te definiëren. Het meest aangewezen is om hierbij gebruik te maken van de definities die komen van een wel bijzonder welingelichte bron: het Amerikaanse ministerie van Defensie (18) zelf.

In richtlijn nr. S-5100.20 van het Amerikaans ministerie van Defensie wordt de bevoegdheid, de functies en de verantwoordelijkheden vastgelegd van de National Security Agency (NSA) en de Central Security Service (CSS). De NSA wordt omschreven als de structuur die de opdracht inzake Signals Intelligence (SIGINT) moet verzekeren en die moet zorgen voor veilige communicatiesystemen voor alle overheidsorganen (19). De CSS wordt belast met de uitvoering van deze SIGINT-operaties.

Deze richtlijn definieert Signals Intelligence (SIGINT) als het onderdeel van het inlichtingenwerk dat zowel Communications Intelligence (COMINT), Electronic Intelligence (ELINT) als Telemetry Intelligence (TELINT) omvat.

COMINT omvat de technische informatie en inlichtingen verkregen van buitenlandse communicatie door personen die niet de bedoelde bestemmelingen van die communicatie zijn (20). COMINT betreft dus het onderscheppen van buitenlandse elektromagnetisch verstuurde communicatie die al dan niet versleuteld is.

ELINT omvat de technische informatie en inlichtingen die worden afgeleid uit buitenlandse, niet op communicatie gerichte, elektromagnetische straling

tence, sans que personne les ait lues, et moins encore soumises à une analyse critique.

Du coup, la notion de système Echelon s'est mise à mener une existence propre dans les médias, et les possibilités techniques d'interception des télécommunications ont été gonflées jusqu'à prendre des proportions quasi mythiques.

Quoi qu'il en soit, il est clair que le travail des services de renseignements a suivi l'évolution technologique dans le domaine des télécommunications. Le développement des liaisons radio, des satellites, des câbles en fibre de verre et l'éventail de plus en plus large des possibilités ainsi offertes pour échanger toujours plus d'informations via le téléphone, le fax et le courrier électronique, est suivi de près par la «technologie de surveillance».

Le développement d'ordinateurs de plus en plus puissants a en outre permis de filtrer automatiquement, à l'aide de mots-clés, les quantités énormes d'informations interceptées.

Afin d'éviter de se perdre dans le jargon utilisé par le monde du renseignement, il semble utile de définir certaines notions. Le plus indiqué est d'emprunter ces définitions à une source particulièrement bien informée, à savoir le ministère américain de la Défense lui-même (18).

La directive n° S-5100.20 du ministère américain de la Défense fixe la compétence, les fonctions et les responsabilités de la *National Security Agency* (NSA) et du *Central Security Service* (CSS). La NSA est définie comme la structure responsable de missions en matière de *Signals Intelligence* (SIGINT) et devant veiller à fournir des systèmes de communications sûrs à tous les organismes publics (19). Le CSS est chargé de l'exécution de ces opérations SIGINT.

Dans la directive, la notion de *Signals Intelligence* (SIGINT) est définie comme la branche du travail de renseignements couvrant ce qui relève tant de la *Communications Intelligence* (COMINT) et de l'*Electronic Intelligence* (ELINT) que de la *Telemetry Intelligence* (TELINT).

COMINT regroupe les informations techniques et les renseignements obtenus à partir des communications avec l'étranger par des personnes qui ne sont pas les destinataires de ces communications (20). COMINT concerne donc l'interception des communications avec l'étranger transmises par voie électromagnétique, sous forme cryptée ou non.

ELINT regroupe les informations techniques et les renseignements tirés des émissions électromagnétiques étrangères dont l'objet n'est pas la communica-

en TELINT omvat de informatie afgeleid uit buitenlandse telemetrie.

In mensentaal samengevat betekent dit dat SIGINT moet begrepen worden als de activiteit gericht op het verzamelen van informatie die voorvloeit uit het opvangen van elektromagnetische golven terwijl COMINT enkel betrekking heeft op het verzamelen van inlichtingen door interceptie van elektromagnetisch verstuurde communicatie. COMINT is dus een onderdeel van SIGINT.

Op grond van richtlijnen als die waarnaar in *supra* werd verwezen is in de Verenigde Staten dus door NSA en CSS het United States Signals Intelligence System uitgebouwd (21).

Globaal genomen kan men stellen dat vele landen, afhankelijk van hun financiële middelen, beschikbare technologie en de wettelijke beperkingen, op een of andere manier aan SIGINT doen.

In het Verenigd Koninkrijk is het Government Communications Headquarters (GCHQ) de bevoegde overheidsdienst (22), in Australië en Nieuw-Zeeland zijn dat respectievelijk, het Defence Signals Directorate en het Government Communications Security Bureau (GCSB) (23).

Artikel 44 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten voorziet dat zelfs onze eigen militaire inlichtingendienst, de Algemene Dienst Inlichtingen en Veiligheid, militaire radioverbindingen mag onderscheppen «om redenen van militaire aard» uitgezonden in het buitenland.

2.2. Werking van COMINT (24)

De manier waarop de COMINT-activiteit wordt ontwikkeld is nauw verweven met de technologische ontwikkelingen van de communicatiedragers.

De inlichtingencyclus bestaat uit drie fases: planning, verzameling en exploitatie.

In de fase van de planning wordt bepaald welke de behoeften zijn inzake inlichtingen. Nadat de doelen zijn bepaald wordt de inwinningscapaciteit ontwikkeld. Daarbij is het van het grootste belang om toegang te krijgen tot een specifiek communicatiemedium zodat de boodschappen kunnen onderschept worden. Uiteraard hangt dit van de aard van het medium af en sommige communicatiedragers zijn gemakkelijker toegankelijk dan andere.

De berichten die worden onderschept worden dan verzameld. Vele onderschepte communicaties zullen niet worden behandeld. Wanneer een nieuwe satelliet wordt gelanceerd zal eerst worden nagegaan welke satellietsignalen televisiebeelden of communicatie die van geen enkel belang is dragen zodat deze kanalen

tion et TELINT concerne les informations tirées de la télémétrie étrangère.

En langage courant, cela signifie que SIGINT est l'activité orientée sur la collecte d'informations provenant de l'interception d'ondes électromagnétiques tandis que COMINT concerne uniquement la collecte de renseignements provenant de l'interception de communications électromagnétiques. COMINT est donc un élément de SIGINT.

Sur la base de directives telles que celles auxquelles il a été fait référence plus haut, la NSA et le CSS ont donc créé, aux États-Unis, le *United States Signals Intelligence System* (21).

D'une manière générale, on peut dire qu'un grand nombre de pays, en fonction de leurs moyens financiers, de la technologie dont ils disposent et des restrictions légales, pratiquent d'une manière ou d'une autre, le SIGINT.

Au Royaume-Uni, le service compétent s'appelle *Government Communications Headquarters* (GCHQ) (22); en Australie et en Nouvelle-Zélande, il s'agit respectivement du *Defence Signals Directorate* et du *Government Communications Security Bureau* (GCSB) (23).

L'article 44 de la loi organique des services de renseignements et de sécurité du 30 novembre 1998 prévoit que notre propre service de renseignements militaire, le Service général du renseignement et de la sécurité, est autorisé à intercepter «à des fins militaires» les radiocommunications militaires émises à l'étranger.

2.2. Fonctionnement du COMINT (24)

La manière dont l'activité COMINT se développe est étroitement liée à l'évoution technologique des supports de communication.

Le cycle du renseignement se compose de trois phases: la planification, la collecte et l'exploitation.

La phase de planification sert à déterminer les besoins en matière de renseignement. Une fois les objectifs fixés, on développe la capacité de collecte des informations. À cet égard, il est capital d'avoir accès à un canal de communication spécifique afin de pouvoir intercepter les messages. Cette interception dépendra évidemment du média utilisé, certains supports de communication étant plus facilement accessibles que d'autres.

Les messages interceptés sont ensuite rassemblés. Nombre de messages interceptés ne seront pas examinés plus avant. Lors du lancement d'un nouveau satellite, on vérifie d'abord quels signaux transmis par ce satellite contiennent des images de télévision ou des communications sans aucun intérêt, afin que ces

niet langer worden onderschept. Het selecteren van berichten voor verdere verzameling en behandeling gebeurt in moderne onderscheppingssystemen automatisch door middel van on-line gegevensbanken die informatie bevatten over de interessante doelen.

Bij de behandeling (processing) van de ingewonnen gegevens wordt deze in een vorm gegoten die analyse mogelijk maakt of die relevante inlichtingen produceert (eenvormige notitie, vermelding van de bron, aard van de gegevens, technische gegevens).

De productie van eigenlijke COMINT impliceert daarna de analyse, evaluatie, vertaling en interpretatie van ruwe gegevens tot afgewerkte bruikbare informatie.

In het laatste stadium van de cyclus worden de ingewonnen inlichtingen verspreid. Dit is een belangrijk element voor de COMINT-activiteit en onderworpen aan strikte regels inzake geheimhouding omdat kennis over de verwerving van de inlichtingen en de manier waarop ze werden ingewonnen er toe kan leiden dat het doel zijn communicatiemiddel verandert om toekomstige onderscheppingen te voorkomen.

COMINT kan enkel gebeuren als de inlichtingendienst toegang krijgt tot het communicatiekanaal. Welke middelen hiertoe worden aangewend behoort tot de best bewaarde geheimen van COMINT-organisaties. De toegangsverschaffing gebeurt al dan niet met medewerking van de operatoren van de communicatiedragers.

De COMINT-organisaties hebben voor de verschillende communicatiemiddelen telkens de aangepaste onderscheppingstechnologie ontwikkeld.

Zo heeft, bijvoorbeeld, het NSA, of zijn voorgangers, sinds 1945 systematisch toegang gekregen tot de communicatie die via de kabel verliep vanwege de belangrijkste kabelmaatschappijen. Deze activiteit, die de codenaam Shamrock droeg, is 30 jaar lang geheim gebleven tot onderzoek in het kader van de Watergate-affaire dit aan het licht bracht.

Zo worden, bijvoorbeeld, op telefoonkabels die over de zeebodem lopen door Amerikaanse duikboten *«pods»* geplaatst die de signalen opvangen.

Voor een bondige en bevattelijke beschrijving van de technische voorwaarden voor het afluisteren van telecommunicatie en de techniek voor satellietcommunicatie verwijzen de commissies naar het uitmuntend verslag van de tijdelijke Commissie over het Echelon-interceptiesysteem van het Europees Parlement (25).

In hoofdstuk 3 van dit verslag («Technische randvoorwaarden voor het afluisteren van telecommunicatie») worden de mogelijkheden van onderschepping van de verschillende communicatiedragers uitvoerig besproken.

canaux ne soient plus interceptés. Dans les systèmes d'interception modernes, la sélection des messages en vue de leur collecte et de leur traitement ultérieur s'effectue automatiquement au moyen de banques de données en ligne contenant des informations sur les objectifs intéressants.

Lors du traitement (processing) des données récoltées, celles-ci sont coulées dans un format permettant de les analyser ou de produire des informations pertinentes (notation uniforme, mention de la source, nature des données, données techniques).

La production de COMINT proprement dit passe ensuite par l'analyse, l'évaluation, la traduction et l'interprétation des données brutes pour obtenir des informations prétraitées utilisables.

Le dernier stade du cycle est celui de la diffusion des informations recueillies. Cet élément essentiel de l'activité COMINT est soumis à des règles strictes de confidentialité parce que si la cible vient à connaître les procédures d'acquisition du renseignement et la manière de collecter l'information, elle peut être amenée à changer de moyen de communication pour prévenir des interceptions futures.

Le COMINT ne peut avoir lieu que si le service de renseignement a accès au canal de communication. Les moyens utilisés pour y arriver font partie des secrets les mieux gardés des organisations COMINT. L'accès aux canaux de communication s'obtient avec ou sans l'aide des opérateurs de ceux-ci.

Les organisations COMINT ont développé une technologie d'interception appropriée à chaque moyen de communication.

C'est ainsi que depuis 1945, la NSA ou ses prédécesseurs ont eu systématiquement accès aux communications par câble et ce, grâce au concours des principaux opérateurs du secteur. Cette activité, qui portait le nom de code *Shamrock*, est restée secrète pendant 30 ans jusqu'à ce que l'enquête menée dans le cadre de l'affaire du *Watergate* dévoile le pot aux roses.

C'est ainsi par exemple que des sous-marins américains placent sur les câbles téléphoniques sous-marins des *«pods»* qui servent à intercepter les signaux.

Pour une description claire et sommaire des conditions techniques des écoutes de télécommunications et de la technique utilisée pour les communications par satellite, les commissions renvoient à l'excellent rapport de la Commission temporaire sur le système d'interception Echelon du Parlement européen (25).

Le chapitre 3 de ce rapport (intitulé «Conditions techniques minimales requises pour l'interception des télécommunications») examine en détail les possibilités d'interception des différents moyens de communication.

Daaruit kan vooral worden geconcludeerd dat de toegang tot moderne optische glasvezelkabels alleen redelijk gemakkelijk is als de eindpunten van de onderzeese kabels op het grondgebied van de onderschepper liggen.

Wat de onderschepping van communicatie via geostationaire satellieten betreft, volstaat het om afluisterstations te plaatsen binnen de *«footprints»* (het gebied dat door de satelliet bestreken wordt) van een bepaalde satelliet.

3. HET ECHELON-INTERCEPTIESYSTEEM

3.1. Het UKUSA agreement

Om van deze theoretische situering van de verschillende vormen van SIGINT-activiteit tot Echelon te komen moeten we terug naar de tweede helft van de jaren veertig waar, in de naloop van de Tweede Wereldoorlog en in de aanloop naar de koude oorlog tussen de Angelsaksische landen een samenwerkingsakkoord werd afgesloten op het vlak van SIGINT.

Dit akkoord dat bekend is als het «UKUSA agreement» maar volgens Hager officieel het UK-USA Security Agreement heet, dateert vermoedelijk van 1948(26) maar is gewoon de verderzetting van een samenwerking die reeds tijdens de Tweede Wereldoorlog was ontstaan tussen de Verenigde Staten, Groot-Brittannië en drie landen van het Commonwealth: Canada, Nieuw-Zeeland en Australië(27).

Volgens de bronnen geciteerd in Hager's boek zou het eigenlijke akkoord enkel door Groot-Brittannië en de Verenigde Staten ondertekend zijn en zijn de drie andere Commonwealth landen veeleer toegetreden als een soort «junior-partners».

Alhoewel de inhoud van het UKUSA-akkoord nooit is bekend geraakt gaat het wel degelijk om een samenwerking inzake SIGINT(28).

3.2. Over het bestaan van interceptie van internationale communicatie

Het ultieme en onomstotelijke bewijs leveren van een inlichtingenactiviteit die door de overheid van de betrokken landen geheim wordt gehouden is een bijna onmogelijke taak. De begeleidingscommissies zijn bovendien geen academische instelling die enkel tot conclusies komt op grond van een wetenschappelijk bewijs. Op grond van de documenten die zij heeft onderzocht en de personen die zij heeft gehoord gaan zij ervan uit dat het Echelon-interceptiesysteem wel degelijk bestaat.

De door verschillende onderzoekers aangebrachte elementen voor het bestaan van Echelon weerstaan de toets van de redelijke twijfel.

On peut surtout en conclure que pour avoir assez facilement accès aux câbles modernes en fibre optique, il faut que les extrémités des câbles sous-marins se trouvent sur le territoire de l'intercepteur.

En ce qui concerne l'interception de communications transmises par des satellites en orbite géostationnaire, il suffit d'installer les stations d'écoute dans la zone de couverture terrestre (*«footprints»*) du satellite en question.

3. LE SYSTÈME D'INTERCEPTION ECHELON

3.1. Le Pacte UKUSA

Pour faire le lien entre cette présentation théorique des différentes formes d'activités SIGINT et Echelon, il faut remonter à la deuxième moitié des années quarante, lorsque, dans la foulée de la Seconde Guerre mondiale et à l'aube de la guerre froide, un pacte de coopération en matière de SIGINT a été conclu entre les pays anglo-saxons.

Ce pacte, connu sous le nom de «*UKUSA agreement*», mais qui, selon Hager, s'appelle officiellement «*UK-USA Security Agreement*», date probablement de 1948(26), mais n'est que le prolongement d'une coopération qui s'était déjà fait jour au cours de la Seconde Guerre mondiale entre les États-Unis, la Grande-Bretagne et trois pays du *Commonwealth*: le Canada, la Nouvelle-Zélande et l'Australie(27).

Selon les sources citées dans le livre de Hager, le pacte proprement dit n'aurait été signé que par la Grande-Bretagne et les États-Unis et les trois autres pays du *Commonwealth* y auraient plutôt adhéré en quelque sorte en qualité d'«associés en second».

Bien que le contenu du Pacte UKUSA n'ait jamais été révélé, il s'agit bel et bien d'une coopération en matière de SIGINT(28).

3.2. Sur l'existence d'une interception des communications internationales

Fournir la preuve ultime et irréfutable d'une activité de renseignement tenue secrète par les autorités des pays concernés confine à l'impossible. En outre, les commissions du suivi ne sont pas une institution académique qui n'arrive à des conclusions que sur la base d'une preuve scientifique. Se fondant sur les documents qu'elles ont examinés et les personnes qu'elles ont entendues, elles partent du principe que le système d'interception Echelon existe bel et bien.

Les éléments avancés par les différents enquêteurs concernant l'existence d'Echelon résistent à l'épreuve du doute raisonnable.

Om precies het domein af te bakenen waarover de discussie gaat dient een onderscheid te worden gemaakt tussen SIGINT-activiteit enerzijds en Echelon anderzijds.

Vele landen ontwikkelen, afhankelijk van hun financiële middelen, SIGINT-activiteit dit wil zeggen onderscheppen buitenlandse elektromagnetische signalen met het oog op het inwinnen van inlichtingen.

Zowel de Verenigde Staten als het Verenigd Koninkrijk hebben officiële overheidsinstellingen die SIGINT activiteit als wettelijke opdracht hebben. Het uitoefenen van deze activiteit is in detail geregeld (29) en over de activiteit van deze overheidsinstellingen wordt parlementair toezicht uitgeoefend (30) waarover regelmatig verslag wordt uitgebracht, tenminste in democratische landen. In een brief aan de tweede kamer en een bijgevoegde notitie van de Nederlandse minister van Defensie van 19 januari 2001 (31) wordt hierover het volgende gezegd: « De feitelijke uitvoering van de interceptie en selectie van de niet-kabelgebonden telecommunicatie ten behoeve van de Militaire Inlichtingendienst en de Binnenlandse Veiligheidsdienst gebeurt bij de Afdeling Verbindingsinlichtingen van de MID. Opsporingsinstanties en de BVD zijn binnen de daartoe door de wet gestelde grenzen bevoegd tot het aftappen van kabelgebonden telecommunicatie ».

Bovendien vergt deze SIGINT-activiteit het gebruik van onderscheppingsinstallaties die weliswaar met de nodige discretie worden omgeven maar waarvan het bestaan moeilijk kan ontkend worden (32).

De verschillende interceptieinstrumenten (radars, antennes, satellieten, ...) worden uitvoerig beschreven in de reeds geciteerde bronnen.

Samenvattend kan men stellen dat in democratische rechtsstaten inlichtingendiensten werken binnen een wettelijk kader en op een of andere manier onderworpen zijn aan een toezicht door de uitvoerende, wetgevende en de rechterlijke macht. Deze doorzichtigheid maakt het bijzonder moeilijk om te ontkennen dat een land een SIGINT-activiteit heeft.

Het feit dat voor deze SIGINT-activiteit op intern vlak een wettelijke regeling getroffen is betekent niet dat deze activiteit niet onwettig kan zijn op grond van het internationaal recht of op grond van de wetgeving van een ander land. SIGINT heeft immers per definitie betrekking op internationale communicatie.

3.3. Situering van « Echelon » in het geheel van SIGINT

Over de aard van het interceptiesysteem dat bekend is geworden onder de benaming « Echelon », zijn door

Si l'on veut délimiter précisément le domaine qui fait l'objet de la discussion, il convient de faire une distinction entre l'activité SIGINT, d'une part, et Echelon, d'autre part.

De nombreux pays développent, en fonction de leurs moyens financiers, des activités SIGINT, c'est-à-dire qu'ils interceptent des signaux électromagnétiques étrangers en vue de récolter des renseignements.

Tant les États-Unis que le Royaume-Uni ont des organismes officiels dont les activités SIGINT constituent la mission légale. L'exercice de ces activités est réglé en détail (29) et les activités de ces organismes publics sont soumises à un contrôle parlementaire (30) qui fait régulièrement l'objet d'un rapport, du moins dans les pays démocratiques. Dans une lettre du 19 janvier 2001 adressé à la *Tweede Kamer* néerlandaise et une note jointe du ministre néerlandais de la Défense (31), on peut lire à ce sujet ce qui suit : (trad.) « L'exécution effective de l'interception et de la sélection des télécommunications non câblodiffusées à l'intention du *Militaire Inlichtingendienst* et du *Binnenlandse Veiligheidsdienst* est assurée par la *Afdeling Verbindingsinlichtingen* du MID. Les instances de détection et le BVD sont habilités, dans les limites fixées par la loi, à écouter les télécommunications câblodiffusées. »

En outre, ces activités SIGINT nécessitent l'utilisation d'installations d'interception qui sont certes entourées de la discrétion voulue mais dont l'existence peut difficilement être niée (32).

Les sources déjà citées décrivent amplement les différents instruments d'interception (radars, antennes, satellites, ...).

En résumé, on peut dire que dans les États de droit démocratiques, les services de renseignements travaillent dans un cadre légal et sont soumis d'une manière ou d'une autre à un contrôle exercé par les pouvoirs exécutif, législatif et judiciaire. Du fait de cette transparence, il est particulièrement difficile de nier qu'un pays exerce une activité SIGINT.

Le fait qu'une réglementation légale ait été adoptée sur le plan interne pour cette activité SIGINT ne signifie pas que cette activité ne puisse pas être illégale au regard du droit international ou de la législation d'un autre pays. SIGINT concerne en effet, par définition, des communications internationales.

3.3. Le système « Echelon » dans l'activité SIGINT globale

Du fait de l'attention soutenue que les médias ont accordée au système d'interception aujourd'hui

de uitgebreide media-aandacht de meest uiteenlopende opvattingen ontstaan.

In de context van dit verslag wordt met Echelon echter het interceptiesysteem bedoeld dat, in het kader van het UKUSA agreement over samenwerking inzake SIGINT, gericht is op het onderscheppen van communicatie die verloopt via satellieten (COMSAT).

Het Echelon-systeem is een geïntegreerd internationaal netwerk waarvan de verschillende stations worden bediend door de vijf landen die deel uitmaken van het UKUSA. De benaming «Echelon» is echter geen benaming die door alle UKUSA-landen gebruikt wordt.

Het systeem maakt gebruik van op de grond geplaatste antennes om de neerwaarts gerichte stralenbundel van commerciële satellieten op te vangen («downlinks») en de signalen te bewerken met het oog op het vergaren van inlichtingen (33).

Daarbij mag niet over het hoofd worden gezien dat COMSAT-interceptie niet het enige middel is dat door de UKUSA-landen wordt ingezet voor de onderschepping van communicaties (34) en dat de Verenigde Staten zeker over een SIGINT-capaciteit beschikken buiten het UKUSA-akkoord.

Kortom, Echelon is gericht op COMSAT-interceptie in het kader van het UKUSA-akkoord en is slechts een onderdeel van de SIGINT-activiteit binnen UKUSA. Het is bovendien slechts een onderdeel van een ruimere SIGINT-activiteit van de Verenigde Staten en (eventueel ook) van de andere UKUSA-landen.

Tenslotte mag niet over het hoofd gezien worden dat nog ongeveer veertigtal andere landen over een belangrijke SIGINT-capaciteit beschikken (zie hoofdstuk 5).

3.4. Over het gebruik en de betekenis van het woord «Echelon»

Dat het woord «Echelon» in elk geval binnen het UKUSA gebruikt wordt staat buiten kijf.

In de omschrijving van de opdracht, functies en taken van de «*Naval Security Group Activity* (NAVSECGRUACT)» die gelegerd is in Sugar Grove, West Virginia (35) wordt vermeld «*Maintain and operate an Echelon site*». In zijn commentaar bij deze instructie wijst Jeffrey Richelson er op dat, alhoewel het NSA de Amerikaanse SIGINT-activiteiten leidt en beheert, het eigenlijke verzamelen van inlichtingen meestal gebeurt door het leger — in dit geval de *Naval Security Group Command*. De rol van de basis in Sugar Grove inzake het onderscheppen van communicatie die via de Intelsat-satellieten verloopt

connu sous l'appellation «Echelon», les conceptions les plus diverses circulent au sujet de la nature du système.

Dans le contexte du présent rapport, on entend par «Echelon» le système d'interception qui, dans le cadre du pacte UKUSA relatif à la collaboration en matière de SIGINT, vise à intercepter les communications par satellite (COMSAT).

Le système Echelon est un réseau international intégré dont les différentes stations sont gérées par les cinq pays du pacte UKUSA. Toutefois, tous les pays parties n'utilisent pas l'appellation «Echelon».

Le système utilise des antennes basées au sol pour capter les faisceaux d'ondes que les satellites commerciaux envoient vers la terre («*downlinks*») et traiter les signaux en vue de réunir des renseignements (33).

À ce sujet, il ne faut pas perdre de vue que la captation COMSAT n'est pas le seul moyen mis en œuvre par les pays UKUSA pour intercepter les communications (34) et que les États-Unis disposent certainement d'une capacité SIGINT extérieure à l'accord UKUSA.

En résumé, Echelon est axé sur l'interception COMSAT dans le cadre du pacte UKUSA et il ne représente qu'une partie de l'activité SIGINT au sein de ce pacte. De plus, Echelon ne représente qu'une partie de l'activité SIGINT globale des États-Unis et (peut-être) aussi de celle des autres pays UKUSA.

Enfin, il faut se rappeler qu'une trentaine d'autres pays possèdent également une capacité SIGINT importante (voir le chapitre 5).

3.4. Concernant l'utilisation et la signification du mot «Echelon»

Le mot «Echelon» est indéniablement utilisé au sein de l'UKUSA.

Dans la définition de la mission, des fonctions et des tâches du «*Naval Security Group Activity* (NAVSECGRUACT)» basé à Sugar Grove en Virginie occidentale (35), on peut lire «*Maintain and operate an Echelon site*». Dans son commentaire sur cette instruction, Jeffrey Richelson souligne que si la NSA dirige et administre les activités SIGINT des États-Unis, la collecte des renseignements proprement dite est généralement effectuée par l'armée — en l'occurrence le *Naval Security Group Command*. Le rôle joué par la base de Sugar Grove dans l'interception des communications transmises par les satelli-

werd voor het eerst onthuld door James Bamford (36).

Ook in «*History of the Air Intelligence Agency, 1 January-31 December 1994, Volume I*» van de *Air Intelligence Agency* (AIA) wordt vermeld «*Activation of Echelon Units*» (37). In zijn commentaar bij deze tekst vermeldt Richelson dat hier uit kan worden afgeleid dat, naast de eenheden van *Naval Security Group*, ook onderdelen van de AIA met ingang van 1 januari 1995 deel gaan uitmaken van de Echelon-eenheden.

Alhoewel uit deze vrijgegeven documenten duidelijk blijkt dat het Amerikaans leger over Echelon-eenheden beschikt wordt niet vermeld met welke opdrachten deze eenheden precies belast zijn. Het Amerikaans leger omschrijft op het internet de opdracht van de *Air Intelligence Agency* als volgt (38): «*The AIA mission is to gain, exploit, defend and attack information to ensure superiority in the air, space and information domains. The Agency's people worldwide deliver flexible collection, tailored air and space intelligence, ...*». Over de 544th IG waarvan detachementen met Echelon-opdrachten worden belast meldt de site van het Amerikaans leger: «*The 544th IG, ..., directs, manages and supports units worldwide in the collection, refinement and delivery of wholesale Intelligence. Personnel operate C41 systems, providing space surveillance ...The 544th was activated on Sep. 7, to provide a single focal point for AIA involvement in worldwide space issues and to posture AIA to better support national agencies.*»

Op de eigen website van de AIA wordt het volgende vermeld (39):

«*Detachment 3, 544th Intelligence Group is fully integrated with Naval Security Group Activity, located at Sugar Grove, W. Va. Its mission is to direct satellite communications equipment supporting research and development for multi-service national missions. It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations. This achieved by embedding personnel into field station operations and by providing a trained cadre of collection system operators, analysts and managers for AIA.*

Det. 3's vision is to provide AIA a highly trained cadre of people to capitalize on emerging technologies to meet consumer requirements and to establish itself as a leader in the COMSAT environment ...»

Hieruit blijkt in elk geval duidelijk dat de Amerikaanse militaire eenheden die met een Echelon-opdracht worden belast bezig zijn met Comsat-interceptie.

In zijn «*Interception Capabilities 2000*» verslag (40) heeft Duncan Campbell bovendien een kopie

tes Intelsat a été dévoilé pour la première fois par James Bamford (36).

Dans l'«*History of the Air Intelligence Agency, 1 January-31 December 1994, Volume I*», publiée par l'*Air Intelligence Agency* (AIA), on trouve aussi la mention «*Activation of Echelon units*» (37). Dans son commentaire de ce texte, Richelson déclare qu'on peut en déduire qu'en sus des unités du *Naval Security Group*, des éléments de l'AIA seront également incorporés dans les unités Echelon à partir du 1er janvier 1995.

Si ces documents établissent clairement que l'armée américaine dispose d'unités «Echelon», ils ne disent pas quelles sont exactement les missions qui ont été confiées à ces unités. Sur son site internet, l'armée américaine définit les missions de l'*Air Intelligence Agency* comme suit (38): «*The AIA mission is to gain, exploit, defend and attack information to ensure superiority in the air, space and information domains. The Agency's people worldwide deliver flexible collection, tailored air and space intelligence, ...*» Au sujet du 544e IG, dont certains détachements sont chargés de missions «Echelon», le site de l'armée américaine indique: «*The 544th IG, ..., directs, manages and supports units worldwide in the collection, refinement and delivery of wholesale Intelligence. Personnel operate C41 systems, providing space surveillance ... The 544th was activated on Sep. 7, to provide a single focal point for AIA involvement in worldwide space issues and to posture AIA to better support national agencies.*»

Sur le site même de l'AIA, on peut lire (39):

«*Detachment 3, 544th Intelligence Group is fully integrated with Naval Security Group Activity, located at Sugar Grove, W. Va. Its mission is to direct satellite communications equipment supporting research and development for multi-service national missions. It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navycommanded field stations. This is achieved by embedding personnel into field station operations and by providing a trained cadre of collection system operators, analysts and managers for AIA.*

Det. 3's vision is to provide AIA a highly trained cadre of people to capitalize on emerging technologies, to meet consumer requirements and to establish itself as a leader in the COMSAT environment ...»

Il ressort, en tout cas, clairement de ces textes que les unités militaires américaines qui sont chargées d'une mission «Echelon» effectuent des interceptions Comsat.

Dans son rapport intitulé «*Interception capabilities 2000*» (40), Duncan Campbell a, en outre, repro-

opgenomen van een document dat een lijst bevat van de databanken die in 1979 in Menwith Hill (Verenigd Koninkrijk) in gebruik waren. Het document vermeldt duidelijk «Echelon 2». In zijn opvolgingsverslag dat hij aan de tijdelijke Onderzoekscommissie van het Europees Parlement heeft voorgesteld (41) onthult Campbell dat hij deze informatie heeft verkregen van Margaret Newsham die zowel in Menwith Hill als in Californië heeft gewerkt aan een aantal projecten om het Echelon-systeem drastisch uit te breiden.

In zijn boek over de betrokkenheid van Nieuw Zeeland omschrijft Hager (42) Echelon als een systeem dat computers van verschillende UKUSA-grondstations, die bekend zijn als «dictionaries», met elkaar verbindt. Deze computers bevatten voor elk van de betrokken inlichtingendiensten van de UKUSA-landen een lijst met trefwoorden (= *the dictionary*) waarvan de aanwezigheid in een onderschept bericht maakt dat het bericht interessant is voor die dienst. De computers filteren automatisch uit miljoenen onderschepte berichten degene die de voorgeprogrammeerde sleutelwoorden bevatten en verzenden ze naar de computers van de vragende dienst.

Alhoewel in het gebruik van het woord «Echelon» door de verschillende diensten enige nuanceverschillen lijken te bestaan besluiten de begeleidingscommissies dat het woord verwijst naar het gebruik van krachtige computers die onderschepte Comsat-berichten automatisch filteren en versturen naar de betrokken diensten van de vijf UKUSA-landen en dit op grond van op voorhand geprogrammeerde trefwoordenlijsten die worden opgesteld door elke dienst afzonderlijk (= *the dictionaries*).

3.5. Wat doet het Echelon-netwerk?

Reeds 20 jaar geleden onthulde Bamford (43) dat het NSA in Sugar Grove (West-Virginia) en Yakima (Washington) Intelsat-communicatiesatellieten onderschepte.

Alhoewel de UKUSA-partners niet in staat zijn om eenzelfde hoeveelheid middelen in te zetten voor SIGINT-operaties nemen ze, onder de benaming Echelon, deel aan COMSAT-intercepties. Jeffrey Richelson (44) somt de volgende grondstations op:

— Waihopai (Nieuw Zeeland);
— Geraldton (Australië);
— Leitrim (Canada);
— Morwenstow (Verenigd Koninkrijk).

Door deze geografische spreiding kan Echelon ongeveer alle communicatie die via satellieten verloopt over de hele wereld onderscheppen en automatisch filteren in functie van de door de UKUSA opgestelde sleutelwoorden.

duit une copie d'un document contenant une liste des banques de données qui étaient opérationnelles à Menwith Hill (Royaume-Uni) en 1979. Ce document mentionne clairement «Echelon 2». Dans le rapport du suivi qu'il a présenté à la Commission d'enquête temporaire du Parlement européen (41), Campbell dévoile qu'il tient ces informations de Margaret Newsham, qui a travaillé à Menwith Hill et en Californie sur des projets visant à élargir considérablement le système Echelon.

Dans son ouvrage sur l'implication de la Nouvelle-Zélande, Hager (42) décrit Echelon comme un système reliant les ordinateurs de différentes stations terrestres d'UKUSA, appelées «dictionnaires». Ces ordinateurs contiennent, pour chacun des services de renseignements concernés des pays UKUSA, une liste de mots clés (= le dictionnaire) dont la présence dans un message intercepté rend celui-ci intéressant pour le service concerné. Les ordinateurs filtrent automatiquement dans les millions de messages interceptés, ceux qui contiennent un des mots clés préprogrammés et les transmettent vers les ordinateurs du service demandeur.

Bien qu'il semble y avoir des nuances dans l'emploi du mot «Echelon» par les différents services, les commissions du suivi concluent que le mot fait référence à l'utilisation d'ordinateurs puissants qui filtrent automatiquement les messages Comsat captés et transmettent le résultat du filtrage aux services concernés des cinq pays UKUSA, le filtrage étant effectué sur la base de listes de mots clés préprogrammés qui sont établies indépendamment par chaque service (les dictionnaires).

3.5. Que fait le réseau Echelon?

Il y a 20 ans déjà, Bamford (43) dévoilait qu'à Sugar Grove (Virginie occidentale) et à Yakima (Washington), la NSA interceptait les transmissions des satellites Intelsat.

Les partenaires d'UKUSA ne sont pas tous capables d'affecter les mêmes moyens aux opérations SIGINT, mais ils prennent part, sous le vocable «Echelon» aux interceptions COMSAT. Jeffrey Richelson (44) énumère les stations terrestres suivantes:

— Waihopai (Nouvelle-Zélande);
— Geraldton (Australie);
— Leitrim (Canada);
— Morwenstow (Royaume-Uni).

Grâce à cette dispersion géographique, Echelon est en mesure d'intercepter pratiquement toutes les communications transmises par satellite dans le monde entier et de les filtrer automatiquement en fonction de mots clés établis par l'UKUSA.

Zowat alle auteurs relativeren echter de capaciteiten van het interceptiesysteem. De omvang van het aantal communicaties, de kost van het systeem verplichten de Echelon-landen om prioriteiten te bepalen. Ook is er een nadeel dat het systeem nog steeds geen oplossing heeft gevonden voor verbale communicatie (45).

Terwijl fax-, telex-, e-mail- and computerverkeer dus het voorwerp zijn van automatische behandeling en analyse gebeurt dit niet met telefoongesprekken. Wel kunnen de telefoons van de gesprekspartners automatisch worden geïdentificeerd en kunnen *voice-prints* worden gebruikt om te weten wie er aan het woord is.

De Amerikaanse parlementaire toezichtorganen van de inlichtingendiensten hebben het NSA in het recente verleden trouwens hevig bekritiseerd omdat het agentschap niet in staat is gelijke tred te houden met de stormachtige ontwikkelingen inzake commerciële communicatie- en computertechnologie (46).

Verschillende ontwikkelingen hebben het onderscheppen van communicaties ernstig bemoeilijkt:

1. het toenemend gebruik van glasvezelkabels;

2. de enorme sprong inzake de ontwikkeling van encryptiesystemen;

3. de explosieve groei van het volume van de internationale communicaties (GSM, fax, internet, ...); hoe groter het aantal internationale communicaties, hoe lager het percentage van interessante onderscheppingen;

3.6. Evaluatie van het Echelon-systeem

Alhoewel de mogelijkheden van het Echelon-systeem niet onbeperkt zijn doet het ernstige vragen rijzen over de aantasting van het privé-leven van mensen over de hele wereld, van de soevereiniteit van de landen die geen deel uitmaken van het UKUSA-akkoord en van de waarborgen inzake vrijhandel.

Ondanks het feit dat het Echelon-systeem een erfenis is van de Koude Oorlog is het systeem ongebreideld gehandhaafd en zelfs uitgebreid door de automatisering van de onderschepping van communicatie. Deze evolutie werd in de jaren negentig nog versterkt in de Verenigde Staten door een heroriëntering van de opdrachten van de militaire en inlichtingendiensten om de budgetten te verrechtvaardigen. De elektronische bewaking werd overgeheveld naar politieopdrachten vooral in de strijd tegen de drugs en het terrorisme. Daarnaast proberen de computer- en electronicabedrijven nieuwe afzetgebieden te vinden voor hun producten.

De meeste vragen die in het Europees en de verschillende Europese nationale parlementen werden

Presque tous les auteurs relativisent cependant les capacités du système d'interception. Le nombre des communications concernées et le coût du système obligent les pays d'Echelon à fixer des priorités. Le système a aussi un inconvénient: on n'a toujours pas trouvé de solution pour la communication verbale (45).

Alors que les transmissions par fax, par télex, par e-mail ou par ordinateur font l'objet d'un traitement et d'une analyse automatisés, tel n'est donc pas le cas pour les conversations téléphoniques. On peut cependant identifier automatiquement les téléphones des interlocuteurs et utiliser des empreintes vocales pour savoir qui est en train de parler.

Dans un passé récent, les organes américains de contrôle parlementaire des services de renseignements ont d'ailleurs vivement critiqué la NSA parce que l'agence s'avère incapable de suivre l'évolution fulgurante des communications commerciales et des technologies informatiques (46).

Plusieurs développements ont considérablement compliqué la captation des communications:

1. l'utilisation croissante des câbles en fibre de verre;

2. les progrès énormes réalisés dans l'évolution des systèmes de cryptage;

3. la croissance explosive du volume des communications internationales (GSM, fax, internet, ...); plus grand est le nombre des communications internationales, plus faible est le pourcentage des captations intéressantes;

3.6. Évaluation du système Echelon

Bien que ses potentialités ne soient pas illimitées, le système Echelon soulève de graves questions quant à la violation de la vie privée des personnes dans le monde entier, à la souveraineté des pays qui ne sont pas parties au pacte UKUSA et aux garanties en matière de libre-échange.

Quoique le système Echelon soit un héritage de la Guerre froide, on l'a conservé sans restriction et on l'a même développé en automatisant l'interception des communications. Cette évolution s'est encore vue renforcée dans les années nonante aux États-Unis par une réorientation des missions des services de renseignements militaires et civils visant à justifier les budgets. La surveillance électronique est devenue une mission de police, principalement dans le cadre de la lutte contre la drogue et le terrorisme. Par ailleurs, les entreprises spécialisées en informatique et en électronique s'efforcent de trouver de nouveaux marchés pour leurs produits.

La plupart des questions qui ont été posées au Parlement européen et dans les divers parlements

gesteld betroffen het ogenschijnlijk gemak waarmee de Amerikaanse inlichtingendiensten economische inlichtingen verzamelen, hierin bijgestaan door een land dat lid is van de Europese Unie. Het inzetten van deze technologie geschiedt buiten elk internationaal wettelijk kader.

Sinds het verschijnen van het STOA-verslag is in de pers veel inkt gevloeid en gespeculeerd over de mogelijke economische schade die Europese en Japanse bedrijven is toegebracht door de inlichtingen die via Echelon aan het Amerikaanse bedrijfsleven werden doorgespeeld.

Als Echelon moet dienen om zowel inlichtingen- en politiediensten als beleidsverantwoordelijken een wapen te geven in de strijd tegen georganiseerde misdaad, terrorisme en «schurkenstaten» (rogue States) dan kan het in elk geval geen alibi zijn om blind alle communicatie te onderscheppen van onschuldige burgers, bevriende landen, niet-gouvernementele organisaties of ondernemingen. Door het onderscheppen van COMSAT wint men echter informatie in over het politiek beleid van andere landen, concurrerende ondernemingen en politieke opponenten die het niet noodzakelijk eens zijn met de Amerikaanse opvattingen over «wereldorde».

Zowel de Verenigde Staten als de andere UKUSA-landen verzekeren dat de rechten van de eigen burgers van hun land niet geschonden worden. Nu lijkt dit aannemelijk gelet op de bescherming van het privéleven die door de wetten in de betrokken landen aan de eigen onderdanen wordt gewaarborgd. Dit belet niet dat met de rechten van de burgers van andere landen wel degelijk een loopje wordt genomen.

Tenslotte is het ook duidelijk dat zowel telecommunicatie- als computerbedrijven mee betrokken zijn bij de uitbouw van het Echelon-netwerk als bij het eigenlijke onderscheppingwerk. Geen enkele van die bedrijven heeft haar klanten (bedrijven, overheden, burgers) laten weten dat hun communicaties wetens en willens onderschept werden.

Wat er van dit alles ook zij, het bestaan van een dergelijk systeem roept allerlei vragen op.

In de eerste plaats rijst de vraag wat de gevolgen zijn voor de Atlantische Alliantie. Een deel van de geallieerde landen bespioneert andere geallieerde landen, zonder dat deze hiervan op de hoogte worden gebracht en zonder dat deze hierop enige democratische controle kunnen uitoefenen. Een deel van de Atlantische Alliantie behandelt met andere woorden een ander deel op dezelfde manier als de voormalige vijand uit het Oostblok, of als landen als Irak en Libië.

Tevens kan men vragen stellen over de rol van het Verenigd Koninkrijk in het Echelon-systeem en de verenigbaarheid ervan met tot wat het zich heeft ver-

nationaux concernaient l'aisance apparente avec laquelle les services de renseignements américains, assistés par un État membre de l'Union européenne, ont pu recueillir des informations de nature économique. Le recours à cette technologie a lieu en dehors de tout cadre international légal.

Depuis la parution du rapport du STOA, la presse a beaucoup écrit et spéculé sur les dommages économiques qui ont pu être infligés aux entreprises européennes et japonaises suite à des informations qui auraient été fournies aux entreprises américaines grâce à Échelon.

Si Echelon doit servir d'arme aux services de police et de renseignements comme aux responsables politiques dans la lutte contre le crime organisé, le terrorisme et les États parias (rogue States), il ne saurait en aucun cas justifier l'interception aveugle de toutes les communications de citoyens innocents, de pays amis, d'organisations non gouvernementales ou d'entreprises. Or, l'interception de communications par satellite permet de recueillir des informations sur la politique des pays tiers, des entreprises concurrentes et des opposants politiques, qui ne partagent pas nécessairement les opinions américaines sur l'«ordre mondial».

Les États-Unis comme les autres pays UKUSA assurent qu'ils ne violent pas les droits de leurs citoyens. Cela semble plausible au vu des garanties en matière de protection de la vie privée que les lois de ces pays offrent à leurs citoyens. Il n'empêche qu'on prend bel et bien quelques libertés avec les droits des citoyens d'autres pays.

Enfin, il est clair que des entreprises spécialisées dans les télécommunications comme dans l'informatique ont participé au développement du réseau Echelon et au travail d'interception proprement dit. Aucune de ces entreprises n'a fait savoir à ses clients (des entreprises, des pouvoirs publics, des citoyens) que leurs communications étaient sciemment interceptées.

Quoi qu'il en soit, l'existence d'un tel système soulève toute une série de questions.

Tout d'abord, force est de se demander quelles sont les répercussions pour l'Alliance atlantique. Une partie des pays alliés espionne d'autres pays alliés sans les en informer et sans que ces derniers puissent exercer un quelconque contrôle démocratique. En d'autres termes, une partie de l'Alliance atlantique traite l'autre partie de la même manière qu'elle traitait l'ancien ennemi du bloc de l'Est ou comme elle traite des pays tels que l'Irak ou la Libye.

En outre, on peut s'interroger sur le rôle du Royaume-Uni dans le système Echelon et sur la compatibilité de ce rôle avec les engagements de ce

bonden binnen de Europese Unie, en dit zowel op het niveau van de lidstaten als wat betreft het respect voor de elementaire rechten van de burgers van de andere lidstaten.

Op deze juridische maar vooral politieke vragen proberen de begeleidingscommissies in dit verslag een antwoord te geven.

3.7. Wordt Echelon gebruikt voor economische spionnage?

Voor het mogelijke gebruik van het systeem Echelon voor het inwinnen van inlichtingen van economische aard rijst in elk geval op technisch vlak geen enkel probleem: het volstaat om bepaalde bedrijven of sectoren in de sleutelwoorden van het «woordenboek» (dictionary) op te nemen om het systeem COMSAT-communicatie dat die termen bevat automatisch te filteren en te selecteren.

Vraag is of de UKUSA-landen ook daadwerkelijk economische inlichtingen inwinnen.

In het Verenigd Koninkrijk voorziet de *Intelligence Security Act* in elk geval dat de *Secret Intelligence Service* inlichtingen moet inwinnen met het oog op de economische belangen van het land(47). GCHQ, de dienst die is belast met het onderscheppen van communicaties, voert zijn opdracht onder meer uit met het oog op de economische belangen van het land(48).

De directeur van de *Central Intelligence Agency* van de Verenigde Staten, George Tenet, heeft in een verklaring voor het *House Permanent Select Committee on Intelligence* weliswaar verklaard dat de inlichtingendienst steunt op SIGINT-activiteit(49) maar hij ontkende ten stelligste dat de inlichtingendiensten aan industriële spionage zouden doen(50): wel geeft het systeem nuttige economische informatie. Deze kan de beleidsmakers bijstaan in tijden van economische crisis.

Wanneer er informatie wordt ingewonnen over de plannen van buitenlandse bedrijven om Amerikaanse wetten of sancties te schenden of om de kansen van Amerikaanse bedrijven te belemmeren wordt ze doorgespeeld aan het ministerie van Financiën, het ministerie van Economische Zaken of andere met de controle op de toepassing van de Amerikaanse wet belaste bestuursorganen.

Alhoewel de heer Tenet dus ontkent dat de Amerikaanse inlichtingendiensten aan economische of industriële spionage doen geeft hij wel degelijk toe dat er dus ook economische inlichtingen worden ingewonnen die zowel van macro- als micro-economische aard zijn.

pays au sein de l'Union européenne, tant au niveau des États membres qu'en ce qui concerne les droits élémentaires des citoyens des autres États membres.

Les commissions du suivi vont tenter, dans le présent rapport, d'apporter une réponse à ces problèmes juridiques, mais surtout politiques.

3.7. Utilise-t-on Echelon pour l'espionnage économique?

L'utilisation éventuelle du système Echelon pour recueillir des informations de nature économique ne pose en tout cas aucun problème sur le plan technique: il suffit d'inclure certaines entreprises ou certains secteurs parmi les mots clés du dictionnaire pour que le système filtre et sélectionne automatiquement les communications COMSAT qui contiennent ces termes.

La question est de savoir si les pays UKUSA recueillent effectivement des informations économiques.

Au Royaume-Uni, l'*Intelligence Security Act* prévoit en tout cas que le *Secret Intelligence Service* doit recueillir des informations pour préserver les intérêts économiques du pays(47). Le GCHQ, le service chargé de l'interception des communications, exerce ses missions, notamment, dans l'intérêt de la prospérité économique du pays(48).

Le directeur de la *Central Intelligence Agency* des États-Unis, George Tenet, a certes déclaré devant le *House Permanent Select Committee on Intelligence* que le service du renseignement reposait sur l'activité SIGINT(49), mais il a formellement nié que les services de renseignements se livrent à l'espionnage industriel(50). Il est toutefois exact que le système fournit des informations économiques utiles.

Ces informations peuvent aider les décideurs politiques en période de crise économique. Quand on recueille des informations sur les intentions des entreprises étrangères de violer les lois ou les sanctions américaines ou d'entraver les perspectives de marchés des entreprises américaines, ces informations sont transmises au ministère des Finances, au ministère des Affaires économiques ou à d'autres organes administratifs chargés du contrôle et de l'application de la loi américaine.

Bien que M. Tenet refuse donc d'admettre que les services de renseignements américains se livrent à l'espionnage économique ou industriel, il reconnaît que ces services recueillent des informations économiques de nature macro- ou microéconomique.

De precisering dat het gaat om bedrijven die Amerikaanse wetten of sancties schenden is veelbetekenend. Er blijkt uit dat om onderschepping van internationale economische communicatie te verantwoorden de Amerikaanse diensten alleen de eigen wet inroepen. Nu zal iedereen zich nog de geschillen herinneren die op internationaal vlak zijn gerezen naar aanleiding van de Amerikaanse wetten D'Amato en Helms-Burton die beide extraterritoriale effecten hadden.

De interceptie van internationale COMSAT moet niet alleen aan de eigen nationale wet getoetst worden maar ook aan het internationale recht en de wetten inzake internationale handel en telecommunicatie.

Men kan dus enkel besluiten dat het antwoord van de CIA hoogstens nuttig is voor binnenlands gebruik maar geen enkele verantwoording geeft voor de schending van de meest elementaire beginselen van het internationale recht.

Een zelfde verantwoording wordt ook gegeven door de voormalige CIA-directeur James Woolsey in een intussen bekend artikel in the *«Wall Street Journal»* van 17 maart 2000 onder de titel *«Why we spy on our allies»* (zie bijlage 3). In een artikel, dat niet bepaald van veel takt getuigt, stelt Woolsey onomwonden: *«Yes, my continental friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?»*

Het is in elk geval niet omwille van onze technologie: *«My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology isn't worth our stealing.»*

De reden waarom de Amerikanen spioneren zou de corruptie zijn van onze bedrijven bij het verwerven van grote, internationale contracten: *«That's right, my European friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot.»*

Daarna zet Woolsey uiteen dat als een Europees bedrijf op corruptie wordt betrapt de Amerikaanse overheid contact opneemt met de overheid van het land dat een contract wenst te sluiten om dit te melden. Verder meent Woolsey te weten dat de Europese bedrijven wel moeten tot corruptie overgaan wegens de inferioriteit van hun economisch systeem (Colbert) tegenover het Amerikaanse (Adam Smith).

De Amerikaanse diensten doen ook economische spionage, aldus nog steeds Woolsey, om te controleren of er geen technologie wordt verkocht die voor dubbel gebruik geschikt is, die met andere woorden

La précision selon laquelle il s'agit d'entreprises qui violent les lois ou les sanctions américaines est significative. Elle montre que pour justifier l'interception des communications économiques internationales, les services américains se basent uniquement sur leur propre législation. Or, chacun se souviendra des litiges qu'ont entraînés, sur le plan international, les lois américaines dites D'Amato et Helms-Burton, qui avaient toutes deux des effets extraterritoriaux.

L'interception de communications internationales par satellite doit être confrontée non pas uniquement à la loi nationale, mais aussi au droit international et aux lois régissant le commerce international et les télécommunications internationales.

On ne peut donc que conclure que la réponse de la CIA est tout au plus utile sur le plan interne, mais qu'elle ne justifie absolument pas la violation des principes les plus élémentaires du droit international.

L'ancien directeur de la CIA, James Woolsey, a donné le même type de justification dans un article, devenu fameux, du *«Wall Street Journal»* du 17 mars 2000, intitulé *«Why we spy on our allies»* (voir annexe 3). Dans cet article, où il ne fait pas preuve d'énormément de tact, M. Woolsey affirme sans ambages: *«Yes, my continental friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?»*

Cet espionnage ne vise en tout cas pas notre technologie: *«My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology isn't worth our stealing.»*

La raison invoquée pour laquelle les Américains nous espionnent serait que nos entreprises pratiquent la corruption pour décrocher des contrats internationaux importants: *«That's right, my European friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot.»*

M. Woolsey explique ensuite que si une entreprise européenne est surprise à pratiquer la corruption, les autorités américaines prennent contact avec les autorités du pays qui souhaite conclure un contrat avec cette entreprise et la dénoncent. M. Woolsey croit savoir en outre encore que les entreprises européennes sont obligées de se livrer à la corruption en raison de l'infériorité de leur système économique (Colbert) par rapport au système américain (Adam Smith).

Les services américains pratiquent également l'espionnage économique, toujours selon M. Woolsey, pour vérifier si on ne vend pas de la technologie susceptible d'avoir un double usage, c'est-à-dire, qui

zowel voor commerciële exploitatie geschikt is als voor massadestructie. Ook wordt nagegaan of er geen handel wordt bedreven met landen waartegen sancties zijn afgekondigd.

In elk geval ontkent Woolsey dat de Amerikaanse bedrijven informatie krijgen over deze economische informatie of dat de inlichtingendiensten bedrijfsgeheimen proberen te achterhalen. De vraag is alleen of we dit op zijn gezag moeten geloven en welke instantie buiten de Verenigde Staten dit kan verifiëren.

Het belangwekkende van dit artikel is dat het op een onverwacht openhartige wijze getuigt van de manier waarop de Amerikaanse overheid, en dit keer zonder het gebruikelijke diplomatieke jargon, tegen andere landen en vooral Europa aankijkt. Daarbij wordt, door iemand die het ongetwijfeld kan weten, openlijk toegegeven dat de Verenigde Staten zonder scrupules de technologische middelen inzet waarover ze beschikken om ook economische informatie te verzamelen.

De rechtvaardiging van deze spionage is dat de Amerikaanse bedrijven, die het woord corruptie uiteraard niet kennen, op voet van gelijkheid moeten kunnen concurreren met de corrupte Europese bedrijven (51). In feite komt de redenering van Woolsey er op neer dat de inferioriteit van ons economische systeem ons noopt tot corruptie om op de internationale markt met de Amerikaanse bedrijven te kunnen concurreren.

Het is enigszins verbazend dat een dergelijke kinderlijke redenering, die getuigt van een zekere ideologische blindheid, uit de pen komt van iemand die de leiding heeft gehad van de grootste inlichtingendienst ter wereld. Tenzij dit natuurlijk enkel de rechtvaardiging is van zuivere economische spionage.

Het verdwijnen van het «Oostblok» en het communistisch systeem in Oost-Europa heeft er toe geleid dat op het eind van de jaren tachtig het hoofddoel van het inlichtingenwerk verdween met een drastische inkrimping van de budgetten van de Westerse inlichtingendiensten. Door president Bush senior werd in het begin van de jaren negentig besloten tot een ingrijpende heroriëntering van de Amerikaanse inlichtingenactiviteit. Door president Clinton werd het vergaren van economische inlichtingen volledig geïmplementeerd door de oprichting van het *Trade Promotion Coordinating Committee* en het *Advocacy Center* (52) die ressorteren onder het *Department of Commerce*.

De successen die door het *Advocacy Center* worden behaald, dit wil zeggen de internationale contracten die het door zijn inspanningen aan Amerikaanse ondernemingen heeft kunnen bezorgen, worden als *success stories* vermeld op de website van het Center (53).

pourrait servir à la fois à une exploitation commerciale et à la destruction de masse. On vérifie également si on ne commerce pas avec des pays qui font l'objet de sanctions.

En tout cas, M. Woolsey nie que les entreprises américaines obtiennent ces informations économiques ou que les services de renseignements essayent de découvrir des secrets industriels. Toute la question est de savoir s'il faut le croire sur parole et quelle instance, en dehors des États-Unis, pourra vérifier la véracité de ses dires.

L'intérêt de cet article est qu'il témoigne avec une franchise inattendue — et sans recourir cette fois au jargon diplomatique habituel — de la manière dont l'autorité américaine considère les autres pays, et l'Europe en particulier. Il contient l'aveu non dissimulé — fait par une personne qui sait incontestablement de quoi elle parle — que les États-Unis utilisent sans scrupules les moyens technologiques dont ils disposent pour recueillir également des informations économiques.

La justification donnée de cet espionnage est que les entreprises américaines, pour qui la corruption est bien entendu une notion étrangère, doivent concurrencer sur un pied d'égalité les entreprises européennes corrompues (51). En fait, le raisonnement de Woolsey revient à dire que l'infériorité de notre système économique nous contraint à recourir à la corruption pour pouvoir concurrencer les entreprises américaines sur le marché international.

Il est quelque peu surprenant qu'un raisonnement aussi enfantin, qui témoigne d'un certain aveuglement idéologique, sorte de la plume de quelqu'un qui a dirigé le plus grand service de renseignements au monde. À moins bien sûr qu'il s'agisse seulement de justifier un espionnage économique pur et simple.

La disparition du «bloc de l'Est» et du système communiste en Europe orientale a entraîné, à la fin des années quatre-vingt, la disparition de l'objectif principal du travail de renseignement et une contraction considérable des budgets des services de renseignements occidentaux. Au début des années nonante, le président Bush senior a décidé une réorientation radicale de l'activité de renseignement des États-Unis. Le président Clinton a intégralement mis en œuvre la collecte de renseignements économiques par la création du *Trade Promotion Coordinating Committee* et de l'*Advocacy Center* (52), qui relèvent du Département du commerce américain.

Les succès remportés par l'*Advocacy Center*, c'est-à-dire les contrats internationaux que les entreprises américaines ont pu décrocher grâce à ses efforts, sont répertoriés à la rubrique *success stories* du site web du centre (53).

In de richtlijnen van het *Advocacy Center* wordt onder punt 1 het criterium omschreven om op de diensten een beroep te kunnen doen:

«1. The overall basis for determining the nature and extent of USG [US Government] *support for a viable bid or proposal in connection with an international transaction shall be the US national interest. A US national interest determination will first weigh and assess the foreseeable, material benefits to the US economy that may potentially be derived from a transaction, and then assess the merit of a request for USG support of any bid or proposal made in connection with the transaction.»*

In de richtlijnen wordt onder punt 6 uitdrukkelijk het volgende gestipuleerd:

«A firm seeking USG support must agree that it and its affiliates:

1. have not and will not engage in the bribery of foreign officials in connection with the matter for which advocacy assistance is being sought; and

2. maintain and enforce a policy that prohibits the bribery of foreign officials. The firm must further acknowledge that failure to comply with the terms of the agreement may result in the denial of advocacy assistance.»

Op het eerste zicht lijkt het *Advocacy Center* dus een overheidsdienst die enkel is opgericht om de belangen van de Amerikaanse bedrijfswereld te behartigen.

Het speelt echter een sleutelrol in de strategie van de Amerikaanse overheid «*to level the playing field*» dit wil zeggen de Amerikaanse bedrijven gelijke kansen te geven in de door buitenlandse bedrijven gecorrumpeerde wereld van internationale contracten. Om de balans in het voordeel van de Amerikaanse bedrijven te doen herstellen wordt gebruikt gemaakt van de via Echelon, en ook andere vormen van inlichtingengaring, ingewonnen informatie. Dat dit gebeurt kan niet betwijfeld worden gelet op de vrijmoedige tekst van Woolsey.

In elk geval is duidelijk dat de CIA betrokken is bij de werking van het *Advocacy Center*. Uit een interne nota die de notulen bevat van een vergadering van 17 augustus 1994 van het TPPC/*Advocacy Center* blijkt duidelijk de aanwezigheid van CIA-agent Bob Beamer (54).

De lijst der bestemmelingen van de agenda van de TPCC Indonesia Working Group (zie noot 54) voor 19 juli 1994 vermeldt de namen van vijf leden van de CIA.

De *working group* bespreekt blijkbaar in detail de nodige achtergrondinformatie voor het sluiten van een contract met Indonesië. Deze bevat onder meer gegevens over de *primary competitors* die ook op het contract azen.

Le point 1 des directives de l'*Advocacy Center* définit le critère à remplir pour pouvoir bénéficier de ses services:

«1. The overall basis for determining the nature and extent of USG [US Government] *support for a viable bid or proposal in connection with an international transaction shall be the US national interest. A US national interest determination will first weigh and assess the foreseeable, material benefits to the US economy that may potentially be derived from a transaction, and then assess the merit of a request for USG support of any bid or proposal made in connection with the transaction.»*

Le point 6 des directives stipule expressément ce qui suit:

«A firm seeking USG support must agree that it and its affiliates:

1. have not and will not engage in the bribery of foreign officials in connection with the matter for which advocacy assistance is being sought; and

2. maintain and enforce a policy that prohibits the bribery of foreign officials. The firm must further acknowledge that failure to comply with the terms of the agreement may result in the denial of advocacy assistance.»

À première vue donc, l'*Advocacy Center* paraît être un service public créé dans le seul but de promouvoir les intérêts des entreprises américaines.

Cependant, il joue un rôle clé dans la stratégie du gouvernement américain consistant à «*to level the playing field*», c'est-à-dire à donner aux entreprises américaines de chances égales dans un monde des contrats internationaux qui est corrompu par les entreprises étrangères. Pour rétablir la balance en faveur des entreprises américaines, on utilise les informations collectées par Echelon et d'autres formes de collecte d'informations. Vu la franchise du discours de Woolsey, il est indéniable que cela se passe.

Il est clair, en tout cas, que la CIA est associée au fonctionnement de l'*Advocacy Center*. Une note interne contenant le compte rendu du TPPC/*Advocacy Center* du 17 août 1994 révèle clairement la présence de l'agent de la CIA Bob Beamer (54).

La liste des destinataires de l'ordre du jour du *TPCC Indonesia Working Group* (*cf.* note 54) pour le 19 juillet 1994 porte les noms de cinq membres de la CIA.

Ce groupe de travail discute apparemment en détail de l'information de base nécessaire pour la signature d'un contrat avec l'Indonésie. Cette information comporte notamment des données sur les *primary competitors* qui briguent également le contrat.

In elk geval blijkt daaruit duidelijk dat de inlichtingendiensten betrokken zijn bij informatiegaring die verder gaat dan het opsporen van corruptie bij de concurrentie. Via Echelon zijn zij ook in staat om prijszetting en bedrijfsstrategieën van de concurrerende bedrijven te onderscheppen.

In de *success stories* die door het *Advocacy Center* op het internet worden gepubliceerd wordt trouwens melding gemaakt van het succesvol sluiten van een contract ten belope van 2,6 miljard dollar met Jakarta voor de bouw van een elektriciteitscentrale (het «Paiton project») door *Mission Energy Company*.

Alhoewel de bedrijven die een beroep doen op het *Advocacy Center* zelf moeten verklaren niet aan omkoping te doen is het Paitonproject berucht omwille van de corruptie die geleid heeft tot het sluiten van het contract. De dochter van president Soeharto zou gratis 0,75% van de aandelen gekregen hebben, ter waarde van 15 miljoen dollar. Samen met haar schoonbroer zou de familie Soeharto voor 50 miljoen dollar aandelen gekregen hebben (55).

Een onafhankelijk onderzoek vanwege *Arthur Andersen and Co* voor het Internationaal Monetair Fonds wees uit dat het contract 72% boven de normale prijs lag en dat honderden miljoenen dollars niet konden verantwoord worden (56). Het gevolg was dat de geproduceerde elektriciteit niet door Indonesië kon worden betaald.

Ook het contract dat door *Raytheon Company* met de Braziliaanse regering voor het *Amazon Surveillance System* is gesloten, is gedrenkt in een sfeer van corruptie. Ook dit contract wordt vermeld in de *success stories* van het *Advocacy Center*. Duncan Campbell meldt dat de politie de telefoon heeft afgeluisterd van Julio Cesar Gomes Dos Santos, een topadviseur van de Braziliaanse president. Hieruit bleek dat Dos Santos de vertegenwoordiger van *Raytheon*, Jose Assumpcão, sprak over smeergeld voor de voorzitter van de commissie voor Financïen van de Senaat teneinde steun te krijgen voor het project. Alhoewel er geen vervolgingen werden ingesteld heeft Dos Santos, samen met de minister voor de Luchtmacht, Mauro Granda, ontslag genomen. Deze onthullingen leidden tot een onderzoek door de Braziliaanse Senaat en vertraagden de start van het project met drie jaar (57).

In het verslag van Duncan Campbell wordt de corruptie rond verschillende van de projecten die in de *success stories* van het *Advocacy Center* worden opgenomen uitvoerig gedocumenteerd.

Het feit dat Amerikaanse ondernemingen moeten verklaren dat zij niet aan omkoping doen alvorens op het *Advocacy Center* een beroep te kunnen doen blijkt in elk geval aan de praktijken van Amerikaanse bedrijven niet veel te veranderen.

Belangrijk is ook om aan te stippen dat de Verenigde Staten nog nooit de moeite hebben genomen

Il ressort en tout cas clairement de ce qui précède que les services de renseignements sont associés à la collecte d'informations qui va plus loin que le dépistage de la corruption chez les concurrents. Grâce à Echelon, ils sont également en mesure d'intercepter les prix et les stratégies des entreprises concurrentes.

Dans les *success stories* publiées sur internet par l'*Advocacy Center*, on fait d'ailleurs mention de la conclusion réussie d'un contrat de 2,6 milliards de dollars avec Djakarta pour la construction d'une centrale électrique (le «projet Paiton») par la *Mission Energy Company*.

Bien que les entreprises qui font appel à l'*Advocacy Center* doivent déclarer qu'elles ne se livrent pas à la corruption, on connaît le projet Paiton en raison de la corruption qui a permis la conclusion du contrat. La fille du président Suharto aurait reçu gratuitement 0,75% des actions, d'une valeur de 15 millions de dollars. Avec son beau-frère, la famille Suharto aurait reçu des actions pour un montant de 50 millions de dollars (55).

Une enquête indépendante menée par *Arthur Andersen et Co* pour le Fonds monétaire international a montré que le contrat excédait de 72% le prix normal et que des dépenses s'élevant à des centaines de millions de dollars ne trouvaient aucune justification (56). La conséquence en a été que l'électricité produite était trop chère pour l'Indonésie.

Le contrat que la *Raytheon Company* a conclu avec le gouvernement brésilien pour l'*Amazon Surveillance System* baigne lui aussi dans une atmosphère de corruption. Ce contrat figure lui aussi parmi les *success stories* de l'*Advocacy Center*. Duncan Campbell déclare que la police a écouté les conversations téléphoniques de Julio Gomes Dos Santos, un conseiller de premier plan du président brésilien. Ces écoutes ont montré que Dos Santos et le représentant de *Raytheon*, Jose Assumpcão, ont parlé de verser des pots-de-vin au président de la commission des Finances du Sénat afin d'obtenir un soutien pour le projet. Même si on n'a pas engagé de poursuites, Dos Santos, ainsi que le ministre de la Force aérienne, Mauro Granda, ont démissionné. Ces révélations ont incité le Sénat brésilien à mener une enquête et ont retardé de trois ans le début du projet (57).

Dans son rapport, Duncan Campbell fournit des documents détaillés à l'appui de la corruption dans laquelle ont baigné plusieurs des projets figurant parmi les *success stories* de l'*Advocacy Center*.

Le fait que les entreprises américaines, avant de faire appel à l'*Advocacy Center*, doivent déclarer qu'elles ne se livrent pas à la corruption, ne change manifestement pas grand-chose aux pratiques des entreprises américaines.

Il est important de souligner aussi que les États-Unis n'ont jamais pris la peine d'apporter des preuves

om op een geloofwaardige manier aan te tonen dat corruptie aan de basis ligt van door een Europese onderneming gesloten contracten.

De begeleidingscommissies menen dat de geruststellende verklaringen van de Amerikaanse of Britse autoriteiten terzake niet aanvaard kunnen worden. De interceptie van communicaties vanuit België of andere Europese landen valt buiten elke nationaal- of internationaal-rechtelijke regeling. De landen van Echelon hebben hun activiteiten steeds geheim gehouden. De landen die het lijdend voorwerp zijn van deze COMINT-activiteit kunnen daarop geen enkele controle uitoefenen.

De parlementaire controle op deze activiteit is, zelfs binnen het Verenigd Koninkrijk, onbestaande (58).

De begeleidingscommissies komen op grond van deze elementen tot het besluit dat de Amerikaanse inlichtingendiensten systematisch economische inlichtingen inwinnen en dit zowel op macro-economisch vlak als op het niveau van individuele bedrijven. Deze informatie wordt doorgegeven aan overheidsinstellingen met het doel om Amerikaanse bedrijven te bevoordelen bij het inwinnen van buitenlandse contracten.

Er zijn geen concrete aanwijzingen dat deze informatie wordt doorgespeeld naar individuele bedrijven of dat het gaat om echte industriële spionage.

Het gebruik van de ingewonnen inlichtingen moet Europese bedrijven vele contracten hebben doen verliezen. Deze praktijk hypothekeert de vrije handel en het zou de moeite lonen om dit voor te leggen aan de Wereldhandelsorganisatie.

Het lijkt dus aannemelijk te besluiten dat de ingeroepen chronische corruptie van Europese ondernemingen vooral een voorwendsel is om economische inlichtingen in te winnen.

Alhoewel de begeleidingscommissies niet hebben kunnen achterhalen via welke kanalen deze informatie wordt ingewonnen gaan zij ervan uit dat hiervoor ook een beroep wordt gedaan op COMSAT-onderschepping via Echelon vanuit grondstations die in Europese landen gelegen zijn (*Menwith Hill* en *Bad Aibling*) (59).

De bezorgdheid van de begeleidingscommissies of de tijdelijke commissie van het Europees Parlement wordt dus duidelijk gedeeld met parlementsleden van de landen die deel uitmaken van Echelon zelf. Op zich is dat niet verwonderlijk omdat het bestaan van dergelijke praktijken onverenigbaar is met de principes van democratische rechtsstaten. Ook in het Amerikaans parlement is trouwens de vraag gesteld of het interceptiesysteem Echelon niet de grondwettelijke rechten van de Amerikaanse burgers schond. In februari 2000 werd door de directeur van CIA, de

crédibles montrant que la corruption serait à la base de contrats conclus par une entreprise européenne.

Les commissions du suivi estiment que les déclarations rassurantes des autorités américaines ou britanniques en la matière sont inadmissibles. L'interception des communications émises à partir de la Belgique ou d'autres pays européens ne s'inscrit dans le cadre d'aucune règle nationale ni internationale. Les pays membres d'Echelon ont toujours tenu leurs activités secrètes. Les pays qui subissent cette activité COMINT ne peuvent aucunement la contrôler.

Le parlement, même au Royaume-Uni, n'exerce aucun contrôle sur cette activité (58).

Ces éléments permettent aux commissions du suivi de conclure que les services de renseignements américains recueillent systématiquement des informations économiques et ce, tant sur le plan macro-économique qu'au niveau des entreprises individuelles. On transmet ces informations à des organismes publics pour aider les entreprises américaines à décrocher des contrats à l'étranger.

Il n'y a pas d'indice concret montrant que ces informations seraient transmises à des entreprises individuelles ou qu'il s'agirait d'un véritable espionnage industriel.

L'utilisation des informations recueillies a probablement fait perdre de nombreux contrats aux entreprises européennes. Pareille pratique hypothèque la liberté des échanges commerciaux; il serait judicieux de soumettre la question à l'Organisation mondiale du commerce.

On peut donc raisonnablement conclure que les Américains prétextent surtout la corruption chronique qui serait pratiquée par les entreprises européennes pour recueillir des informations économiques.

Bien que les commissions du suivi n'aient pas pu déterminer par quels canaux cette information est recueillie, elles partent du principe que pour les obtenir, on utilise également le système Echelon qui permet d'intercepter les communications par satellite à l'aide de stations terrestres situées dans des pays européens (*Menwith Hill* et *Bad Aibling*) (59).

L'inquiétude des commissions du suivi ou de la commission temporaire du Parlement européen est donc clairement partagée par les parlementaires des pays qui font eux-mêmes partie du système Echelon. Ce n'est pas étonnant en soi, puisque l'existence de pareilles pratiques est inconciliable avec les principes de l'État de droit démocratique. Le parlement américain s'est du reste, lui aussi demandé si le système d'interception Echelon ne violait pas les droits constitutionnels des citoyens américains. En février 2000, le directeur de la CIA, le directeur de la NSA et l'avocat

directeur van NSA en de advocaat-generaal een verslag voorgelegd aan het Amerikaans Congres dat de wettelijke normen omschrijft die de inlichtingendiensten hanteren voor SIGINT-activiteiten, met inbegrip van elektronische bewaking (60). Het verslag verzekert dat NSA en CIA zorgvuldig *the Foreign Intelligence Surveillance Act (FISA), the Executive Order No 12333* evenals het Vierde Amendement van de Amerikaanse Grondwet naleven. Uit de nota blijkt dat de bewakingstechnologie zo wordt gebruikt dat het vergaren van inlichtingen over Amerikaanse burgers die hun toestemming niet hebben verleend zoveel mogelijk wordt beperkt. Deze regels zijn evenwel niet van toepassing op niet-Amerikaanse staatsburgers ...

4. INTERNATIONAL LAW ENFORCEMENT TELECOMMUNICATION SEMINARS (ILETS)(61)

In de rand van de onthullingen rond Echelon kwam ook aan het licht dat sinds 1993 politie- en inlichtingendiensten van verschillende landen deelnamen aan de *«International Law Enforcement Telecommunications Seminars»* (ILETS). Deze vergaderingen beogen een technische vereenvoudiging van de interceptie door een technische normalisatie van de communicatieapparatuur.

Op de ILETS-vergadering van 1994 te Bonn werden de deelnemers het eens over een document met politieke richtlijnen dat in bijlage een lijst bevatte van *«international user requirements»* (IUR 1.0 of IUR 95) dat de eisen opsomt waaraan de verschillende telecommunicatie-exploitanten moeten voldoen om intercepties te vereenvoudigen. Deze IUR 1 werd de basis voor een resolutie van de Raad van 17 januari 1995 betreffende de legale interceptie van het telecommunicatieverkeer (62). Deze resolutie werd pas op 4 november 1996 gepubliceerd. In de bijlage van deze resolutie zijn eisen geformuleerd die door de politie- en inlichtingendiensten worden gesteld aan de aanbieders van netwerken en diensten. Deze eisen gelden zowel voor bestaande als nieuwe communicatietechnologieën (satelliet- en internetcommunicatie). Bij het aanvaarden van de resolutie hebben de lidstaten de intentie uitgesproken om de principes van de resolutie op te nemen in de nationale wetgeving (63).

Het doel van deze resolutie is ervoor te zorgen dat in alle lidstaten de technische voorwaarden beschikbaar zijn om de autoriteiten in het kader van hun nationale bevoegdheden werkelijk toegang te verschaffen tot de gewenste gegevens zodat ze een reëel gebruik kunnen maken van de bevoegdheden die het nationale recht hun verleent.

De Raad neemt er nota van dat de «Eisen ... een belangrijke samenvatting vormen van de behoeften van de bevoegde autoriteiten met betrekking tot de

général ont présenté au Congrès américain un rapport décrivant les normes légales que les services de renseignements utilisent pour les activités SIGINT, y compris la surveillance électronique (60). Le rapport assure que la NSA et la CIA respectent scrupuleusement le *Foreign Intelligence Surveillance Act* (FISA), l'*Executive Order Nº 12333* ainsi que le Quatrième Amendement de la Constitution américaine. La note montre qu'on utilise la technologie de surveillance de manière à limiter au maximum la collecte d'informations sur des citoyens américains qui n'auraient pas donné leur autorisation. Les règles ne sont toutefois pas applicables aux personnes qui ne sont pas citoyennes des États-Unis ...

4. INTERNATIONAL LAW ENFORCEMENT TELECOMMUNICATION SEMINARS (ILETS)(61)

En marge des révélations concernant le réseau Echelon, il est apparu également que depuis 1993, les services de police et de renseignements de plusieurs pays participaient aux *«International Law Enforcement Telecommunications Seminars»* (ILETS). Ces réunions ont pour but de faciliter les interceptions sur le plan technique par le biais de la normalisation technique des équipements de communication.

Lors de la réunion ILETS qui s'est tenue à Bonn en 1994, les participants ont approuvé un document de directives politiques qui comportait en annexe une liste de *«international user requirements»* (IUR 1.0 ou IUR 95) énumérant les spécifications auxquelles les opérateurs de télécommunications doivent se conformer pour faciliter les interceptions. Cette IUR 1 a servi de base à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (62). Cette résolution n'a été publiée que le 4 novembre 1996. L'annexe de cette résolution contient des spécifications que les services de police et de renseignements imposent aux opérateurs de réseaux et de services. Ces spécifications s'appliquent aux technologies de communications existantes comme aux technologies nouvelles (communications par satellites et par l'internet). En approuvant la résolution, les États membres ont fait part de leur intention de transposer les principes de la résolution dans la législation nationale (63).

L'objet de la résolution est de veiller à ce que dans tous les États membres, les conditions techniques requises soient présentes pour fournir aux autorités, dans le cadre de leurs compétences légales, un accès effectif aux données souhaitées de manière à leur permettre d'exercer réellement les compétences que leur confère le droit national.

Le Conseil prend note du fait que «les spécifications ... constituent un condensé important des besoins des autorités compétentes pour la réalisation

technische realisatie van de wettelijk toegestane interceptie in moderne telecommunicatiesystemen». De Raad bepleit in zijn resolutie onder meer «dat bij de bepaling en tenuitvoerlegging van de maatregelen ... met voornoemde eisen rekening moet wordt gehouden en verzoekt de lidstaten en de voor Justitie en Binnenlandse Zaken bevoegde ministers samen te werken om te komen tot een daadwerkelijke realisering van de eisen met betrekking tot netwerkexploitanten en dienstenverstrekkers».

Met een daaropvolgend *«Memorandum of Understanding»* (MOU), dat niet werd gepubliceerd, werden derde landen verzocht de technische vereisten van de resolutie in de praktijk om te zetten. Bovendien moeten technische vernieuwingen zowel aan het secretariaat van de Raad als aan het FBI (!) worden meegedeeld. De reden die hiervoor werd opgegeven is het feit dat communicatietechnologie vaak in handen is van multinationale ondernemingen is zodat de samenwerking met de interceptieautoriteiten van derde landen met belangrijke bedrijven onontbeerlijk is.

Dit memorandum werd door de lidstaten van de Europese Unie en Noorwegen ondertekend op 23 november 1995. De Verenigde Staten, Australië en Canada deelden schriftelijk mee dat zij zouden zorgen voor de omzetting in intern recht.

Tijdens de volgende vergaderingen werden deze IUR aangepast aan nieuwe communicatietechnieken.

Op 23 april 1999 is een nieuwe ontwerpresolutie ingediend(64) om die van 1995 aan te passen aan nieuwe communicatietechnologieën zoals satelliet- en internetcommunicatie. Dit ontwerp werd door het Europees Parlement aangenomen(65) maar door de Raad voorlopig bevroren.

Het «ontdekken» van ILETS heeft in verschillende Europese landen wel wat stof doen opwaaien omdat de parlementaire controle-instanties van verschillende Europese landen die aan deze vergaderingen deelnemen niet op de hoogte waren van het bestaan van deze seminaries.

Ook nemen zowel inlichtingendiensten als politiediensten aan deze vergaderingen deel terwijl de wetgeving en de finaliteit van de onderscheiden diensten verschillend is.

De eerste vergadering had plaats in 1993 in Quantico, op initiatief van het FBI(66). Daarna werden vergaderingen gehouden in Bonn (1994), Canberra (1995), Dublin (1997), Ottawa (1998) en Lyon (1999).

België nam sinds 1994 deel aan de ILETS-seminaries. Aanvankelijk nam alleen de APSD en de rijkswacht deel. Later heeft ook de Veiligheid van de Staat regelmatig aan de vergaderingen deelgenomen

technique des moyens d'interception légale dans les systèmes modernes de télécommunications». Dans sa résolution, le Conseil déclare notamment «que les spécifications précitées doivent être prises en considération lors de la définition et de l'exécution de l'interception légale des télécommunications» et demande aux États membres «d'inciter les ministres responsables des télécommunications à soutenir cette position et à coopérer avec les ministres de la Justice et des Affaires intérieures, afin d'appliquer ces spécifications en ce qui concerne les opérateurs de réseaux et des fournisseurs de services».

Dans un *«Memorandum of Understanding»* (MOU), ultérieur, non publié, les pays tiers ont été invités à mettre en pratique les spécifications techniques de la résolution. En outre, les innovations techniques doivent être communiquées à la fois au secrétariat du Conseil et au FBI (!). La raison invoquée est que les technologies des communications sont souvent détenues par des entreprises multinationales, de sorte qu'il est indispensable de collaborer avec les autorités chargées de l'interception dans les pays où sont établies des entreprises importantes.

Le mémorandum a été signé le 23 novembre 1995 par les États membres de l'Union européenne et la Norvège. Les États-Unis, l'Australie et le Canada ont communiqué par écrit qu'ils veilleraient à transposer les spécifications dans leur droit national.

Lors des réunions suivantes, les IUR ont été adaptées aux nouvelles techniques de communication.

Un nouveau projet de résolution(64) a été déposé le 23 avril 1999 dans le but d'adapter la résolution de 1995 aux nouvelles technologies de communication comme l'internet et les communications par satellite. Ce projet de résolution a été adopté par le Parlement européen(65) mais il a été provisoirement gelé par le Conseil.

La «découverte» des ILETS a toutefois provoqué des remous dans plusieurs pays européens parce que les instances de contrôle parlementaire de plusieurs des pays qui prennent part à ces réunions n'étaient pas au courant de l'existence des séminaires.

De plus, les services de renseignements participent à ces réunions au même titre que les services de police, alors que ces services ne sont pas soumis aux mêmes législations et ont une finalité différente.

La première réunion a eu lieu à Quantico, en 1993, à l'initiative du FBI(66). Les suivantes se sont tenues à Bonn (1994), Canberra (1995), Dublin (1997), Ottawa (1998) et Lyon (1999).

La Belgique est présente aux séminaires ILETS depuis 1994. Au début, seuls le SGAP et la gendarmerie y participaient. Plus tard, la Sûreté de l'État a elle aussi assisté régulièrement aux réunions, bien que ne

alhoewel deze over geen enkele bevoegdheid beschikt inzake onderschepping van communicaties.

In het STOA-verslag wordt de achtergrond uiteengezet waarin ILETS ontstaan is (67).

De Verenigde Staten proberen al jaren om de inlichtingen- en politiediensten een gemakkelijker toegang te verschaffen tot persoonlijke communicaties. In de eerste plaats werd gepoogd om zowel telefoonmaatschappijen als alle andere communicatieoperatoren te verplichten om bewakingscapaciteit in te bouwen. In de tweede plaats werd gepoogd om de verspreiding van encriptiesoftware te beperken.

Eind van de jaren tachtig probeerden de Amerikaanse politiediensten, via een programma dat intern bekend stond onder de naam *«Operation Root Canal»*, telefoonmaatschappijen er toe te bewegen de interceptie van telefoongesprekken te vergemakkelijken. Hoewel de maatschappijen dit weigerden werd in 1994 door het Congres een wet gestemd, *«Communications Assistance for Law Enforcement Act»* (CALEA) die operatoren oplegde dat gesprekken moesten kunnen onderschept worden door de overheid. Fabrikanten werden verplicht om met de politiediensten samen te werken teneinde te verzekeren dat hun apparatuur aan bepaalde technologische vereisten voldeed. Deze wet is nog steeds niet in werking getreden omdat het FBI nog striktere bepalingen wil invoeren. Tegelijk probeerde het FBI zijn technische voorschriften ook door bevriende landen te doen aanvaarden. Het is in dit kader dat ILETS is ontstaan en het verklaart meteen waarom de eerste vergadering in Quantico plaatshad.

Het IUR 1.0 aangenomen door ILETS en omgezet in de resolutie van 1995 is gebaseerd op het FBI-verslag *«Law Enforcement Requirements for the Surveillance of Electronic Communications»* dat werd opgesteld in 1992 en aangepast in 1994.

Sinds het begin van de jaren negentig hebben de Amerikaanse inlichtingendiensten ook enorme inspanningen geleverd om zich ervan te verzekeren dat zij de beschikking zouden houden over de versleutelingscode van computers zodat zij zich op elk gewenst moment toegang konden verschaffen tot versleutelde communicatie. Dit verklaart de harde strijd van de Verenigde Staten tegen de vrije ontwikkeling van versleutelingssoftware en waarom zij hebben geijverd voor de inbouw van «key-recovery-systems» (68) in computers. Ook Europese landen hebben dergelijke restricties op vrije versleuteling overwogen of geïmplementeerd (Frankrijk en het Verenigd Koninkrijk).

Tijdens de ILETS-vergadering van 1998 werd besloten de IUR aan te passen met het oog op de versleutelingsproblematiek (69). Deze nieuwe IUR werd als ENFOPOL 98 aan de werkgroep «politiesamenwerking» voorgesteld op 3 september 1998 en bevatte onder meer bepalingen omtrent versleuteling. Het

disposant d'aucune compétence en matière d'interception des communications.

Le rapport STOA décrit le contexte dans lequel les ILETS ont vu le jour (67).

Les États-Unis s'efforcent depuis des années de faciliter l'accès des services de police et de renseignements aux communications privées. En premier lieu, on a tenté d'obliger les compagnies de téléphone et tous les autres opérateurs de communications d'intégrer une capacité de surveillance. Ensuite, on a tenté de limiter la diffusion des logiciels de cryptage.

À la fin des années quatre-vingt, les services de police américains ont essayé, par l'intermédiaire d'un programme dénommé *«Operation Root Canal»*, d'amener les compagnies de téléphone à faciliter l'interception des conversations téléphoniques. Bien que les compagnies aient refusé, le Congrès a voté en 1994 une loi intitulée *«Communications Assistance for Law Enforcement Act»* (CALEA), en vertu de laquelle les opérateurs étaient tenus de permettre l'interception des conversations par les autorités. Les fabricants étaient contraints de collaborer avec les services de police pour garantir que leurs équipements répondent à certaines exigences technologiques. Cette loi n'est toujours pas entrée en vigueur, car le FBI entend introduire des dispositions plus sévères encore. En même temps, le FBI a essayé de faire accepter aussi ses spécifications par les pays amis. C'est dans ce contexte que sont nées les ILETS et cela explique en même temps pourquoi la première réunion a été organisée à Quantico.

L'IUR 1.0 adopté par les ILETS et transposé dans la résolution de 1995 est basé sur un rapport du FBI intitulé *«Law Enforcement Requirements for the Surveillance of Electronic Communications»*, rédigé en 1992 et adapté en 1994.

Depuis le début des années nonante, les services de renseignements américains ont déployé également d'énormes efforts pour s'assurer qu'ils continueraient à disposer du code de cryptage des ordinateurs afin de pouvoir accéder à tout moment aux communications cryptées. C'est pourquoi les États-Unis ont toujours lutté avec âpreté contre le libre développement des logiciels de cryptage et œuvré à l'intégration de «key-recovery-systems» (68) dans les ordinateurs. Des pays européens (la France et le Royaume-Uni) ont eux aussi envisagé ou instauré de telles restrictions à la liberté de cryptage.

Au cours de la réunion ILETS de 1998, il a été décidé d'adapter les IUR au problème de cryptage (69). Ces nouveaux IUR ont été présentés comme ENFOPOL 98 au groupe de travail «Coopération policière» le 3 septembre 1998 et contenaient notamment des dispositions concernant le cryptage. La

Oostenrijks voorzitterschap van de Raad stelde voor de nieuwe IUR, net als in 1995, over te nemen als een resolutie van de Raad. Tot nog toe is dit niet gebeurd.

Het debat over de toegang van politie- en inlichtingendiensten tot versleutelde gegevens en communicatie is in dit geval nog niet beëindigd.

Enerzijds ligt het voor de hand dat binnenlandse orde en veiligheid vereisen dat politie en inlichtingendiensten informatie moeten kunnen inwinnen over extremistische bewegingen, terroristische groeperingen en de georganiseerde misdaad.

Als deze gebruik maken van versleutelde communicatie wordt het werk van deze diensten aanzienlijk bemoeilijkt. Het is dan ook evident dat de betrokken diensten nadenken over manieren om zich toegang te verschaffen tot de versleutelde communicatie en computerbestanden.

Anderzijds is de manier van de besluitvorming over deze materie dermate ondoorzichtig dat ze ernstige vragen oproept over de wijze waarop binnen de Europese Unie de politionele samenwerking georganiseerd wordt en de democratische controle op de de Europese regelgeving tot stand komt. De ontwikkeling van bewakingtechnologie raakt de grondrechten van alle burgers en de bescherming van de privacy, ook met betrekking tot elektronische bestanden, wordt in Europa zeer sterk beschermd zowel door het EVRM, door Europese richtlijnen als door het interne recht van de verschillende lidstaten.

De vrij doorzichtige manier waarop Amerikaanse diensten zowel de Europese inlichtingen- als politiediensten als de Europese Raad hun agenda hebben opgedrongen roept ernstige vragen op over de democratische controle op de sluipende Europese besluitvorming. Het Europees Parlement, en mogelijk de Raad, was helemaal niet op de hoogte van het verband tussen de Amerikaanse voorschriften, het IUR 1 uitgewerkt door ILETS en de technische voorschriften die door de resolutie werden voorgesteld. Geen enkele nationale assemblee was trouwens op de hoogte van het bestaan van de ILETS-seminaries.

Het probleem is dat over de vraag of en in welke mate er technische voorschriften worden opgelegd aan communicatie-, computer- en telecommunicatieproducenten of -operatoren pas een beslissing kan genomen worden na een debat in de parlementen van de Europese lidstaten. Daarbij dient, in België in elk geval, eerst een wettelijke regeling getroffen te worden voor de interceptie van communicaties door de inlichtingendiensten — tot nader order is dit nog steeds verboden. De Europese Unie is zelfs helemaal niet bevoegd in deze materie: de toelaatbaarheid van afluistermaatregelen valt onder de nationale bevoegdheid van de lidstaten (70).

Of en in welke mate de bevoegde overheden een toegangssleutel wordt gegeven voor versleutelde

présidence autrichienne du Conseil a proposé de reprendre les nouveaux IUR, comme en 1995, sous la forme d'une résolution du Conseil. Jusqu'à présent, cela n'a pas été fait.

En tout cas, le débat sur l'accès des services de police et de renseignements à des informations et à des communications cryptées n'est pas encore terminé.

D'une part, il est évident que l'ordre et la sécurité intérieure requièrent que la police et les services de renseignements puissent collecter des informations sur les mouvements extrémistes, les groupes terroristes et le crime organisé.

Si ceux-ci utilisent des communications cryptées, le travail de ces services se complique considérablement. Il va donc de soi que les services concernés refléchissent au moyen d'avoir accès aux communications et aux fichiers informatiques cryptés.

D'autre part, la prise de décisions en la matière est tellement peu transparente qu'elle soulève de sérieuses questions quant à la manière dont on organise la coopération policière dans l'Union européenne et dont on exerce le contrôle démocratique sur l'élaboration des règles européennes. Le développement de la technologie de surveillance affecte les droits fondamentaux de l'ensemble des citoyens et la vie privée est très protégée en Europe, y compris pour ce qui est des fichiers électroniques, à la fois par la CEDH, par des directives européennes et par le droit interne des divers États membres.

La manière assez évidente dont les services américains ont imposé leur ordre du jour aux services de renseignements et de police européens comme au Conseil européen soulève de graves questions sur le contrôle démocratique d'un mode de décision européen qui manque de transparence. Le Parlement européen — et peut-être même le Conseil — ne connaissait absolument pas le lien unissant les prescriptions américaines, les IUR 1 élaborés par les ILETS et les prescriptions techniques proposées par la résolution. Au demeurant, aucune assemblée nationale n'était informée de l'existence des séminaires ILETS.

Le problème est qu'on ne peut trancher la question de savoir s'il faut imposer des prescriptions techniques aux producteurs ou aux opérateurs de communications informatiques ou de télécommunications, et dans quelle mesure, qu'après un débat au sein des parlements des États membres de l'Union. À cet égard, il faut d'abord, en Belgique en tout cas, légiférer sur l'interception des communications par les services de renseignements, pareille interception étant interdite jusqu'à nouvel ordre. L'Union européenne n'est même aucunement compétente en la matière: c'est aux État membres eux-mêmes qu'il appartient d'autoriser ces mesures d'écoute (70).

La question de savoir si l'on donnera aux autorités compétentes une clé d'accès aux matériels ou aux

hard- of software is evenzeer een nationale bevoegdheid.

De betrokkenheid van nationale politie- en inlichtingendiensten en de Europese werkgroep «Politionele samenwerking» bij de implementatie van de agenda van de Amerikaanse inlichtingendiensten zonder enige behoorlijke kennisgeving aan het Europees Parlement of de parlementen van de lidstaten kan niet anders beschouwd worden dan als een uitschuiver van formaat.

Ongetwijfeld beantwoorden de inspanningen van de betrokken diensten op een oprechte bezorgdheid over een zo efficiënt mogelijke invulling van hun wettelijke opdrachten. De vraag is of zij er zich van bewust zijn wiens spel zij spelen.

De begeleidingscommissies vragen zich af of een betere uitvoering van de politieopdrachten niet een voorwendsel is voor en heel andere agenda. In september 1996 verklaarde David Herson, het hoofd van de EU senior officers' group on Information Security het volgende over het Amerikaans «key recovery project» (waarin NSA de hand heeft):

«Law Enforcement» is a protective shield for all the other governmental activites ... We're talking about foreign intelligence, that's what all this is about. There is no question (that) «law enforcement» is a smoke screen.»

ILETS is voor de Amerikaanse inlichtingendiensten een instrument om hun prioriteiten inzake bewakingstechnologie op te dringen, aan de Europese Unie en aan de andere deelnemende landen.

Wellicht te goeder trouw hebben de Europese inlichtingen- en politiediensten zich geleend als waterdragers van dit beleid en hebben zij daardoor het inwinnen van inlichtingen buiten de specifieke opdrachten van openbare orde en veiligheid vergemakkelijkt (onder meer economische inlichtingen).

Uiteraard zullen de belangen van de Europese Unie en de Verenigde Staten wat betreft de behoeften inzake bewakingstechnologie grotendeels samenvallen. Het staat buiten kijf dat de strijd tegen het terrorisme en de georganiseerde criminaliteit behoefte heeft aan aangepaste technologische middelen. Beslissingen hierover kunnen echter alleen maar worden genomen na een openbaar parlementair debat en op grond van een wettelijke habilitatie waarbij voorzien wordt in een afdoende vorm van toezicht.

De begeleidingscommissies wijzen er wel uitdrukkelijk op dat de Belgische politie- en inlichtingendiensten weliswaar hebben deelgenomen aan de ILETS-seminaties maar dat zij daarbij hun wettelijke bevoegdheden niet hebben overschreden.

De begeleidingscommissies komen ook tot de bevinding dat ILETS niet tot doel had om op Euro-

logiciels cryptés constitue également une compétence nationale.

L'association des services de police et de renseignements nationaux et du groupe de travail européen «Coopération judiciaire» à l'exécution du programme des services de renseignements américains, sans information convenable du Parlement européen ni des parlements des États membres, ne peut être considérée que comme un écart d'envergure.

Il ne fait aucun doute que les efforts des services concernés sont dictés par la volonté sincère de remplir leurs missions légales aussi efficacement que possible. La question est de savoir s'ils se rendent compte de qui ils font le jeu.

Les commissions du suivi se demandent si une meilleure exécution des missions de police ne sert pas de prétexte à un tout autre scénario. En septembre 1996, David Herson, chef du «senior officers' group on Information Security» de l'Union européenne déclarait au sujet du «key recovery project» américain (dans lequel le NSA joue un rôle):

«Law Enforcement» is a protective shield for all the other governmental activites ... We're talking about foreign intelligence, that's what all this is about. There is no question (that) «law enforcement» is a smoke screen.»

Les ILETS sont un instrument permettant aux services de renseignements américains d'imposer leurs priorités en matière de technologie de surveillance à l'Union européenne et aux autres pays participants.

Les services de police et de renseignements européens ont été, sans doute de bonne foi, les porteurs d'eau de cette politique et ont facilité ainsi la collecte d'informations en dehors du cadre des missions spécifiques concernant la sûreté et l'ordre public (notamment des informations économiques).

Certes, les besoins en matière de technologie de surveillance de l'Union européenne et des États-Unis sont en grande partie concordants. Il ne fait aucun doute que la lutte contre le terrorisme et la criminalité organisée requiert des moyens technologiques adaptés. Toutefois, des décisions en la matière ne peuvent être prises qu'après un débat parlementaire public et sur la base d'une habilitation légale assortie d'une forme suffisante de contrôle.

Les commissions du suivi soulignent cependant que les services de police et de renseignements belges ont certes participé aux séminaires ILETS, mais que ce faisant ils n'ont pas outrepassé leurs compétences légales.

Les commissions du suivi concluent également que les ILETS ne visent pas à instaurer un contrôle supra-

pees niveau te komen tot een supranationaal toezicht op telecommunicatie.

5. INTERCEPTIESYSTEMEN IN ANDERE LANDEN

Hoewel de begeleidingscommissies zich hebben voorgenomen om vooral over Echelon te rapporteren zijn zij er zich van bewust dat ook andere landen SIGINT-activiteiten ontwikkelen. SIGINT, COMSAT-onderschepping en automatische filtering van de onderschepte communicaties via sleutelwoorden zijn dus zeker geen monopolie van de UKUSA-landen. Daarom geven de begeleidingscommissies een kort overzicht van deze activiteiten in andere landen voor zover zij hierover bronnen hebben gevonden.

5.1. Frankrijk

In een voortreffelijk gedocumenteerd artikel, gepubliceerd in «*Le nouvel Observateur*» van 5-11 april 2001, schetst Vincent Jauvert een overzicht van de COMSAT-interceptiemogelijkheden van de Franse DGSE (Direction générale de la sécurité extérieure).

Het artikel vermeldt dat Frankrijk in de afgelopen tien jaar een mondiale interceptiecapaciteit heeft opgebouwd.

In het «centre radioélectrique» in de Périgord (Domme), naast de luchthaven van Sarlat, bevindt zich sinds 1974 het voornaamste interceptiestation van Frankrijk.

Een ander station is verborgen in het tropische oerwoud van Frans Guyana en heeft de codenaam «Frégate». Een derde installatie, die in 1998 werd gerealiseerd, bevindt zich op de wand van de krater Dziani Dzaha op het Franse eiland Mayotte (Komoren) in de Indische Oceaan. Beide stations worden samen met de Bundesnachrichtendienst (BND), de Duitse inlichtingendienst, uitgebaat. Het station «Frégate» wordt trouwens geopend door de toenmalige chefs van DGSE en BND. Beide stations bieden het voordeel dat ze vlak bij de evenaar liggen. Vanuit Mayotte kan COMSAT van Afrika, het Midden-Oosten en Azië onderschept, vanuit Kourou wordt de satellietcommunicatie boven het Noord-Amerikaanse continent onderschept.

Het vierde station bevindt zich ten westen van Parijs, op het plateau van Orgeval, te Alluets-le-Roi.

Gelet op de omvang van dit systeem is Frankrijk in staat om wereldwijd aan COMSAT-interceptie te doen.

national des télécommunications au niveau européen.

5. SYSTÈMES D'INTERCEPTION EXISTANT DANS D'AUTRES PAYS

Bien que les commissions de suivi aient projeté de faire rapport surtout sur Echelon, elles sont conscientes du fait que d'autres pays développent aussi des activités de nature SIGINT. Les activités SIGINT, les systèmes d'interception COMSAT et le filtrage automatique des communications interceptées sur la base de mots clés ne constituent donc certainement pas un monopole des pays UKUSA. Aussi les commissions de suivi donnent-elles un bref aperçu des activités de ce type qui sont développées dans d'autres pays, pour autant qu'elles aient trouvé des sources les concernant.

5.1. France

Dans un article excellemment documenté qui a été publié dans le *Nouvel Observateur* du 5-11 avril 2001, Vincent Jauvert donne un aperçu des possibilités d'interception COMSAT de la Direction générale de la sécurité extérieure (DGSE) française.

L'article signale que la France a développé une capacité d'interception mondiale au cours des dix dernières années.

Le centre radioélectrique situé dans le Périgord (Domme), à côté de l'aéroport de Sarlat, abrite la principale station d'interception de France.

Une autre station qui a reçu le nom de code «Frégate» est dissimulée dans la forêt tropicale en Guyane française. Une troisième installation, qui a été construite en 1998, se trouve sur un versant du cratère Dziani Dzaha sur l'île française de Mayotte (Comores) dans l'océan Indien. Ces deux stations sont exploitées en collaboration avec le Bundesnachrichtendienst (BND), le service de renseignements allemand. La station «Frégate» a d'ailleurs été inaugurée par les chefs de l'époque de la DGSE et du BND. Ces deux stations présentent l'avantage d'être situées près de l'équateur. Il est possible d'intercepter, de la station de Mayotte, les informations COMSAT en provenance d'Afrique, du Moyen-Orient et d'Asie, et, de la station de Kourou, les informations en provenance du continent nord-américain.

La quatrième station se trouve à l'ouest de Paris, sur le plateau d'Orgeval, à Alluets-le-Roi.

Grâce à l'amplitude de ce système, la France est en mesure d'intercepter des informations COMSAT partout dans le monde.

In het artikel wordt verder gemeld dat de DGSE zijn onderscheppingscapaciteit nog verder wil uitbouwen en dat het daartoe de nodige budgettaire middelen heeft gekregen. In het verslag van de Franse Assemblée nationale over de begroting 2001 wordt hier door rapporteur Jean-Michel Boucheron trouwens uitdrukkelijk op gewezen (71):

« En matière d'équipement, l'effort portera sur la recherche du renseignement par moyen technique et sur les activités d'appui et de logistique. En 2001, comme en 2000, il faudra ainsi maintenir les compétences en matière de cryptologie ainsi qu'adapter l'équipement destiné au recueil et à l'exploitation du renseignement d'origine électromagnétique à l'ouverture de nouveaux centres d'écoutes et d'interception.

L'interception des liaisons de satellites de télécommunication reste une priorité du service. Le renouvellement du super calculateur est aussi prévu pour 2001 vraisemblablement en coopération avec le CEA. »

Wat opvalt in het Franse systeem is dat van alle democratische landen die over interceptiesystemen beschikken, Frankrijk het enige land is dat geen wettelijke regeling heeft uitgewerkt met betrekking tot het recht op privacy van de burgers of een vorm van toezicht heeft georganiseerd voor de COMSAT-activiteit van de DGSE.

In zijn artikel geeft Vincent Jauvert aan dat ook het Franse systeem het geïntercepteerde COMSAT-verkeer automatisch filtert via trefwoorden of adressen (72) (net zoals het « dictionary »-systeem van Echelon dus).

De laatste zin in het geciteerde verslag over de begroting 2001 van Defensie heeft zijn belang. De samenwerking met het Commissariat à l'énergie atomique (CEA) houdt namelijk verband met het gebruik van een supercomputer die dient voor de ontcijfering van versleutelde communicatie (73).

In zijn artikel geeft Jauvert ook aan dat een belangrijk deel van de SIGINT-activiteit van de DGSE bestaat uit het inwinnen van economische informatie en dat de DGSE reeds een twintigtal jaren in nauwe symbiose werkt met een aantal publieke en private ondernemingen ...

De gegevens van het artikel stemmen bijna volledig overeen met wat door Duncan Campbell aan de begeleidingscommissies werd meegedeeld tijdens de hoorzitting van 8 juni 2001.

De begeleidingscommissies kunnen, gelet op het ontbreken van officiële bronnen, weinig met zekerheid vaststellen over de Franse SIGINT-activiteit. In elk geval is het duidelijk dat Frankrijk over een belangrijke, wereldomvattende SIGINT-capaciteit beschikt en dat het zeer vermoedelijk ook inlichtingen van economische aard inwint. Vermoedelijk is dit dan ook de reden waarom Frankrijk nogal lauw heeft

L'article précité signale en outre que la DGSE souhaite encore augmenter sa capacité d'interception et qu'elle a obtenu les moyens budgétaires nécessaires à cet effet. Jean-Michel Boucheron, l'auteur du rapport de l'Assemblée nationale française sur le budget 2001 (71), le souligne d'ailleurs explicitement dans les termes suivants :

« En matière d'équipement, l'effort portera sur la recherche du renseignement par moyen technique et sur les activités d'appui et de logistique. En 2001, comme en 2000, il faudra ainsi maintenir les compétences en matière de cryptologie ainsi qu'adapter l'équipement destiné au recueil et à l'exploitation du renseignement d'origine électromagnétique à l'ouverture de nouveaux centres d'écoutes et d'interception.

L'interception des liaisons de satellites de télécommunication reste une priorité du service. Le renouvellement du super calculateur est aussi prévu pour 2001 vraisemblablement en coopération avec le CEA. »

Ce qui frappe en ce qui concerne le système français, c'est que, contrairement à tous les autres pays démocratiques disposant de systèmes d'interception, la France n'a pas élaboré de réglementation légale relative au droit à la vie privée des citoyens. En outre, elle n'a organisé aucune forme de surveillance pour ce qui est de l'activité COMSAT de la DGSE.

Dans son article, Vincent Jauvert indique que, de son côté aussi (c'est-à-dire comme le système « dictionary » d'Echelon), le système français filtre automatiquement le trafic COMSAT au moyen de mots clés ou d'adresses (72).

La dernière phrase du rapport précité sur le budget de la Défense pour 2001 a son importance. La collaboration avec le Commissariat à l'énergie atomique (CEA) concerne en effet l'utilisation d'un superordinateur servant au décryptage des communications cryptées (73).

M. Jauvert souligne également dans son article qu'une bonne partie de l'activité SIGINT consiste à recueillir des informations de nature économique et que la DGSE travaille depuis une vingtaine d'années déjà en symbiose étroite avec un certain nombre d'entreprise publiques et privées ...

Les données citées dans l'article correspondent presque entièrement à ce que M. Duncan Campbell a communiqué aux commissions d'accompagnement au cours d'une audition du 8 juin 2001.

L'absence de sources officielles empêche les commissions d'accompagnement de faire beaucoup de constatations sûres concernant les activités SIGINT. Il est en tout cas clair que la France dispose d'une capacité SIGINT d'envergure mondiale et qu'elle recueille plus que probablement aussi des renseignements de nature économique. C'est probablement la raison pour laquelle la France a réagi avec

gereageerd op het bekend worden van Echelon en vooral gereageerd heeft op de economische schade die het ondervindt.

5.2. Nederland

In tegenstelling tot de Franse overheid heeft de Nederlandse regering een vrij grote openhartigheid aan de dag gelegd over de eigen interceptiemogelijkheden, de wettelijke basis ervan en de doelstellingen.

In zijn notitie «Het grootschalig afluisteren van moderne telecommunicatiesystemen» (74) zet minister de Grave van Defensie de Nederlandse situatie als volgt uiteen:

«Op basis van de bepalingen van het Wetboek van strafvordering ... hebben de opsporingsdiensten in Nederland voldoende bevoegdheden om openbaar Nederlands telecommunicatieverkeer af te tappen en de bijbehorende informatie op te vragen.

De feitelijke uitvoering van het intercepteren en selecteren van niet-kabelgebonden telecommunicatie ten behoeve van de MID (Militaire Inlichtingendienst) en de BVD (de Binnenlandse Veiligheidsdienst) geschiedt door de afdeling verbindingsinlichtingen van de MID.

(...)

Hierbij dient te worden opgemerkt dat uit interceptie verkregen informatie slechts wordt gebruikt ten behoeve van de wettelijke taakuitvoering van de diensten. Zo wordt zoals reeds aangegeven in de beantwoording van Kamervragen (zie aanhangsel *Handelingen II*, 1999-2000, nr. 1112) bijvoorbeeld geen informatie door de diensten aan het Nederlandse bedrijfsleven verstrekt.

Ten aanzien van de samenwerking van de diensten op het gebied van SIGINT kan, (...) worden opgemerkt dat de hoofden van de diensten op grond van artikel 13 van de wet op de inlichtingen- en veiligheidsdiensten contacten onderhouden met inlichtingen- en veiligheidsdiensten van andere landen. Deze samenwerking bestaat voor het grootste deel uit de uitwisseling van gegevens. Hierbij wordt erop toegezien dat Nederlandse belangen niet geschaad worden. Ook worden op verzoek technische en andere vormen van ondersteuning verleend. In het wetsvoorstel WIV (wetsvoorstel op de inlichtingen- en veiligheidsdiensten) is deze bevoegdheid expliciet opgenomen.

Voor de openbare telecommunicatienetten- en diensten die door aanbieders in Nederland worden aangeboden geldt dat de aftapbaarheid hiervan in principe op een toekomstvaste wijze is ondergebracht in de bepalingen van de telecommunicatiewet. Concreet betekent dit dat alle nieuwe systemen bij introductie op de Nederlandse markt direct aftapbaar voor

tiédeur à l'annonce de l'existence d'Echelon et s'est surtout plainte des dommages économiques qu'elle subit.

5.2. Pays-Bas

Contrairement aux autorités françaises, le gouvernement néerlandais a fait preuve d'une assez grande sincérité quant à ses propres possibilités d'interception, à leur base légale et aux objectifs poursuivis.

Dans sa note «*Het grootschalig afluisteren van moderne telecommunicatiesystemen* (74), le ministre de la Défense de Grave décrit la situation des Pays-Bas de la manière suivante:

(trad.) «Sur la base des dispositions du Code d'instruction criminelle, ... les services de recherche ont, aux Pays-Bas, suffisamment de compétences pour écouter les conversations véhiculées par les réseaux publics néerlandais de télécommunication et pour demander des renseignements complémentaires.

L'exécution effective de l'interception et de la sélection des télécommunications non «câblodiffusées» à l'intention du MID (*Militaire Inlichtingendienst*) et du BVD (*Binnenlandse Veiligheidsdienst*) est assurée par la section verbindingsinlichtingen du MID.

(...)

Il faut remarquer ici que les informations obtenues par interception ne sont utilisées qu'aux fins de l'exécution des tâches légales des services. C'est ainsi que, comme on l'a déjà signalé dans la réponse à des questions posées à la Chambre (voir, en annexe, les *Annales II*, 1999-2000, n° 1112), les services ne fournissent par exemple aucune information aux entreprises néerlandaises.

S'agissant de la collaboration des services dans le domaine SIGINT, on peut (...) faire remarquer que les chefs des services entretiennent, en application de l'article 13 de la loi sur les services de renseignements et de sécurité, des contacts avec des services de renseignements et de sécurité d'autres pays. Cette collaboration consiste principalement à échanger des données. On veille en l'espèce à ce que les intérêts néerlandais ne soient pas lésés. Des formes d'assistance technique ou autre sont également accordées sur demande. Cette compétence est définie explicitement dans la proposition de loi WIV (*Wetsvoorstel op de inlichtingen- en veiligheidsdiensten*).

Pour ce qui est de l'écoute des réseaux et services publics de télécommunication proposés par les offreurs aux Pays-Bas, on considère, en principe, que les dispositions qui la régissent sont celles de la loi sur les télécommunications et que ces dispositions n'hypothèquent pas l'avenir. Cela signifie concrètement que, lors de leur introduction sur le marché

de bevoegde autoriteiten dienen te zijn. Om dit in de toekomst daadwerkelijk te effectueren is de handhaving van de aftapbepalingen van de telecommunicatiewet van essentieel belang (75).»

Minister de Grave gaat in zijn nota ook in op de vraag over de onderschepping van buitenlands communicatieverkeer.

«De bevoegdheid voor het afluisteren van telecommunicatieverkeer waarvan de oorsprong of de bestemming in het buitenland ligt is momenteel in de Nederlandse wet niet expliciet geregeld. Indien het internationaal recht de rechtsmacht zou aanknopen bij de plaats waar het af te tappen signaal wordt opgevangen, dan zou de rechtercommissaris ook telecommunicatie van burgers die zich in het buitenland bevinden kunnen laten aftappen. Gaat het om landen van de Europese Unie, dan gelden evenwel de regels van de EU-Rechtshulpovereenkomst (zie hoofdstuk 5) voor zover het gaat om het aftappen voor strafvorderlijke doeleinden. Wat betreft de activiteiten van de BVD en de MID wordt verwezen naar de eerdergenoemde expliciete bevoegdheid in dit kader met de daaraan verbonden waarborgen, opgenomen in het wetsvoorstel WIV.»

De minister besluit:

«Het stelsel van wetgeving bestaande uit het Wetboek van strafvordering, het wetsvoorstel WIV en de aftapbepalingen van de telecommunicatiewet is als geheel een *conditio sine qua non* om, in een veranderende telecommunicatie-omgeving, de betreffende Nederlandse diensten op een toekomstvaste wijze in staat te blijven stellen om bevoegd informatie te vergaren.»

Het Nederlandse afluisterstation bevindt zich te Zoutkamp in Groningen en wordt bediend door de *Militaire Inlichtingendienst*. Gelet op de verklaringen van de Nederlandse overheid menen de begeleidingscommissies dat het op geen enkele manier in verband kan worden gebracht met Echelon en louter voor Nederland werkt.

5.3. Duitsland (76)

De Bundesnachrichtendienst (BND) is de federale inlichtingendienst die onder de bevoegdheid valt van de bondskanselier. Hij is als enige dienst belast met het vergaren en evalueren van inlichtingen over het buitenland die van belang zijn voor het veiligheids- en buitenlandse beleid. Voorts is deze dienst verantwoordelijk voor militaire buitenlandse verkenningen en actief op het vlak van SIGINT.

Afdeling 2 van de BND wint inlichtingen in door het onderscheppen van buitenlandse communicatie

néerlandais, tous les nouveaux systèmes doivent pouvoir être écoutés directement par les autorités compétentes. Pour la réalisation concrète de cet objectif à l'avenir, le maintien des dispositions de la loi sur les télécommunications concernant les écoutes est essentiel (75).»

Dans sa note, le ministre de Grave évoque aussi la question de l'interception des télécommunications étrangères.

(trad.) «La loi néerlandaise actuelle ne règle pas explicitement la compétence en matière d'écoute des télécommunications dont l'origine ou la destination se trouve à l'étranger. Au cas où le droit international, situerait la compétence juridictionnelle à l'endroit où le signal à écouter est perçu, le juge d'instruction pourrait également faire écouter des télécommunications de citoyens se trouvant à l'étranger. S'il s'agit de pays de l'Union européenne, ce sont toutefois les règles de la Convention EU sur l'entraide judiciaire (voir chapitre 5) qui sont applicables, pour autant qu'il soit question d'écoutes aux fins de procédures pénales. En ce qui concerne les activités du BVD et du MID, nous renvoyons à la compétence explicite dans ce cadre dont il a déjà été question ci-dessus et aux garanties qui l'entourent et qui sont définies dans la proposition de la loi WIV.»

Et le ministre de conclure:

(Trad.) «Le Code d'instruction criminelle, la proposition de loi WIV et les dispositions de la loi sur les télécommunications concernant les écoutes forment ensemble un dispositif législatif dont l'existence est une condition *sine qua non* pour que, dans un contexte de télécommunications en mutation, les services néerlandais concernés restent compétents pour recueillir des informations en préservant l'avenir.»

La station d'écoutes néerlandaise se trouve à Zoutkamp, dans la province de Groningue, et c'est le *Militaire Inlichtingendienst* qui en assure le fonctionnement. Les commissions du suivi estiment, sur la base des déclarations des autorités néerlandaises, que l'on ne peut établir aucun lien avec Échelon et que la station travaille exclusivement pour les Pays-Bas.

5.3. L'Allemagne (76)

Le Bundesnachrichtendienst (BND) est le service de renseignements fédéral qui relève de la compétence du chancelier fédéral. C'est le seul service chargé de recueillir et d'évaluer des renseignements sur les pays étrangers qui ont de l'importance pour la politique de sécurité et la politique étrangère. En outre, ce service est responsable de reconnaissances militaires à l'étranger et actif en matière de SIGINT.

La section 2 du BND recueille des renseignements en interceptant des communications étrangères,

waaronder COMSAT (sinds mei 2001 mag ook via kabel verzonden buitenlandse communicatie onderschept worden)(77).

De BND probeert met strategische telecommunicatiebewaking buitenlandse informatie te verstrekken. Dit gebeurt door met een aantal zoekbegrippen *(= dictionary system)* satellietcommunicatie te onderscheppen. Tijdens de hoorzitting voor de tijdelijke commissie van het EP werden ook een aantal cijfergegevens verstrekt. Van de ongeveer 10 miljoen internationale communicaties per dag van en naar Duitsland zijn er ongeveer 800 000 per satelliet. Daarvan wordt een kleine 10 % (75 000) door een zoekmachine uitgefilterd. De beperking van de interceptie gebeurt vooral omwille van technische redenen, onder meer de analysecapaciteit.

De zoekbegrippen wortden in Duitsland vooraf goedgekeurd door de G10-commissie(78).

Het Duits Grondwettelijk Hof heeft een onderzoek ingesteld naar de Duitse afluisterpraktijken. Tijdens het proces(79) zijn een aantal bijzonderheden aan het licht gekomen over de aard van de door de BND gebruikte trefwoorden. Er bestaan een aantal louter formele zoekbegrippen (verbindingen van vreemdelingen of buitenlandse firma's in het buitenland) met daarnaast 2 000 zoekbegrippen inzake proliferatie, 1 000 zoekbegrippen over wapenhandel, 500 zoekbegrippen over terrorisme en 400 zoekbegrippen over drugshandel.

Volgens Duncan Campbell beschikt de BND over een basis in de Volksrepubliek China, op Taiwan en — in samenwerking met Frankrijk — in Frans-Guyana (Kourou).

Dit laatste element wordt in elk geval bevestigd door het artikel van Vincent Jauvert in *«Le Nouvel Observateur»* die stelt dat zowel de basis in Kourou als op Mayotte door de DGSE en de BND samen worden uitgebaat.

Opnieuw moeten de begeleidingscommissies vaststellen dat naast het Verenigd Koninkrijk en Frankrijk een land van de Europese Unie over een belangrijke interceptiecapaciteit beschikt, gericht op het inwinnen van informatie uit het buitenland waarbij gewerkt wordt met sleutelwoorden.

5.4. Zwitserland

Tijdens de hoorzitting heeft Duncan Campbell er op gewezen dat, met het oog op het intercepteren van economische inlichtingen, Zwitserland bezig is met het opzetten van het SATOS-3-systeem met twee interceptiesites. Uit de beschikbare gegevens blijkt dat noch Duitsland noch Frankrijk hierbij betrokken zijn. Hij gaat er derhalve van uit dat er wordt samengewerkt met de Verenigde Staten en het Verenigd Koninkrijk.

parmi lesquelles COMSAT (depuis mai 2001, les communications étrangères transmises par câble peuvent également être interceptées)(77).

Le BNB tente de fournir des informations étrangères par la surveillance des télécommunications stratégiques. Il le fait en interceptant les communications par satellite grâce à un certain nombre de termes de recherche *(= dictionary system)*. Au cours des auditions devant la commission temporaire du PE, une série de chiffres ont également été fournis. Des quelque 10 millions de communications internationales qui entrent et sortent chaque jour d'Allemagne, il y en a environ 800 000 par satellite. Un peu moins de 10 % d'entre elles (75 000) sont filtrées par un outil de recherche. La limitation de l'interception est surtout due à des raisons techniques, notamment la capacité d'analyse.

En Allemagne, les termes de recherche sont approuvés au préalable par la commission du G10(78).

La Cour constitutionnelle allemande a ouvert une enquête sur les pratiques allemandes d'écoutes téléphoniques. Lors du procès(79), une série de détails sont apparus concernant la nature des mots clés employés par le BND. Il existe un certain nombre de termes de recherche purement formels (contacts d'étrangers ou de firmes étrangères à l'étranger), auxquels s'ajoutent 2 000 termes de recherche en matière de prolifération, 1 000 autres relatifs au trafic d'armes, 500 autres sur le terrorisme et 400 autres sur le trafic de stupéfiants.

Selon Duncan Campbell, le BND dispose d'une base en République populaire de Chine, à Taiwan et — en collaboration avec la France — en Guyane française (Kourou).

Ce dernier élément est en tout cas confirmé par l'article de Vincent Jauvert dans *Le Nouvel Observateur*, qui dit que tant la base de Kourou que celle de Mayotte sont exploitées conjointement par la DGSE et le BND.

Les commissions du suivi doivent constater à nouveau qu'outre le Royaume-Uni et la France, un pays de l'Union européenne dispose d'une capacité d'interception considérable, qui vise à recueillir des informations en provenance de l'étranger et qui fonction à l'aide de mots clés.

5.4. La Suisse

Au cours de son audition, M. Duncan Campbell a indiqué que la Suisse était en train de mettre sur pied un système SATOS-3 doté de deux sites d'interception, en vue de capter des informations économiques. Les données disponibles montrent que ni l'Allemagne ni la France ne participent à l'opération. Il suppose donc que la Suisse collabore avec les États-Unis et le Royaume-Uni.

5.5. Rusland

In het verslag van de tijdelijke commissie Echelon worden ook enige inlichtingen verwerkt over de Russische bewakingstechnologie. De Russische inlichtingendienst FAPSI *(Federal Agency of Government Communications and Information)* is verantwoordelijk voor de veiligheid van de communicatie en SIGINT. Deze dienst exploiteert of exploiteerde, aldus de tijdelijke commissie, samen met de militaire inlichtingendienst (GRU) grondstations in Letland (Skrunda, gesloten in 1998), Vietnam (Cam Ranh Bay) en Cuba (Lourdes). Recente persberichten melden dat dit laatste station eveneens zou worden gesloten. In het gebied van de Indische Oceaan liggen ook een aantal stations op Russisch grondgebied waarover verdere gegevens ontbreken.

De tijdelijke commissie van het EP besluit in elk geval dat de Russische diensten zowel militaire alsook commerciële communicatie onderschept en dat ze over voldoende stations beschikken om een wereldwijde dekking mogelijk te maken.

Over de Russische mogelijkheden inzake SIGINT-activiteiten beschikken de begeleidingscommissies over te weinig authentieke bronnen om hierover welke uitspraak dan ook te doen.

Dit valt trouwens ook buiten het bestek van dit verslag. Wel illustreert het het feit dat alle landen die over de technische mogelijkheden beschikken en over een nuttige geografische ligging wereldwijde onderscheppingsnetwerken bezitten. Met 54 000 personeelsleden beschikt het FAPSI in elk geval over een indrukwekkende analysecapaciteit.

5.6. Andere landen

In volume 2/5 van het STOA-verslag wordt vermeld dat minstens 30 andere landen over belangrijke COMINT-organisaties beschikken. Het verslag vermeldt bijvoorbeeld dat China over een belangrijke SIGINT-capaciteit beschikt met twee interceptiestations die op Rusland zijn gericht en die samen met de Verenigde Staten worden uitgebaat. Ook India, Israël en Pakistan beschikken over belangrijke SIGINT-systemen.

Tijdens de hoorzitting voor de begeleidingscommissies heeft de heer Duncan Campbell enkele gegevens verstrekt over een aantal Europese landen.

Noorwegen heeft samen met de Verenigde Staten de «NORUSA»-overeenkomst gesloten.

Spanje had tot in 1992 samen met Duitsland een basis in de buurt van Càdiz. Het is onduidelijk of Spanje deze interceptieactiviteiten alleen verderzet.

In Denemarken wordt door Amerikaanse ondernemingen druk aan een interceptiebasis gewerkt. De

5.5. La Russie

Le rapport de la commission temporaire Échelon fournit également quelques renseignements sur la technologie de surveillance russe. Le service de renseignement russe FAPSI *(Federal Agency of Government Communications and Information)* est chargé de la sécurité des communications et du SIGINT. Ce service exploite ou exploitait, selon la commission temporaire, conjointement avec le service de renseignements militaire (GRU) des stations au sol en Lettonie (Skrunda, fermée en 1998), au Vietnam (Cam Ranh Bay) et à Cuba (Lourdes). Selon des dépêches récentes, cette dernière station serait également fermée. Dans la zone de l'océan Indien, il y a également une série de stations en territoire russe, sur lesquelles les informations manquent.

La commission temporaire du PE conclut en tout cas que les services russes interceptent des communications militaires et commerciales et qu'ils disposent de suffisamment de stations pour couvrir le monde entier.

Les commissions du suivi ne disposent pas de suffisamment de sources fiables sur les moyens russes en matière de SIGINT pour pouvoir tirer quelque conclusion que ce soit.

Tel n'est d'ailleurs pas l'objet du présent rapport. Toutefois, on constate que tous les pays qui ont des moyens techniques et une situation géographique adéquate possèdent des systèmes d'interception de portée mondiale. Avec 54 000 employés, la FAPSI dispose en tout cas d'une capacité d'analyse impressionnante.

5.6. Autres pays

Dans le volume 2/5 du rapport du STOA, on peut lire que 30 autres pays au moins disposent d'organisations COMINT importantes. Le rapport mentionne par exemple que la Chine dispose d'une capacité SIGINT considérable, avec deux stations d'interception orientées vers la Russie, qu'elle exploite avec les États-Unis. L'Inde, Israël et le Pakistan disposent également de systèmes SIGINT importants.

Au cours de son audition devant les commissions du suivi, M. Duncan Campbell a fourni des renseignements sur une série de pays européens.

La Norvège a signé avec les États-Unis le pacte NORUSA.

Jusqu'en 1992, l'Espagne avait avec l'Allemagne une base commune dans la région de Cadix. On ne sait pas très bien si l'Espagne poursuit seule ces activités d'interception.

Des entreprises américaines sont en train de développer activement une base d'interception au Dane-

Deense betrokkenheid dateert van de Koude Oorlog. Door middel van stations op de eilanden in de Oostzee en op Groenland kon Rusland in het oog gehouden worden. In de context van het ruimteschild neemt het belang van Groenland ten andere opnieuw toe.

6. VERGADERINGEN MET DE LEDEN VAN DE REGERING

6.1. Hoorzitting met de heer M. Verwilghen, minister van Justitie (19 mei 2000)

De minister van Justitie verklaart dat het internationaal publiek recht geen eenduidig antwoord geeft op de vraag of de interceptie door een Staat van telecommunicatie tussen personen, die zich niet op het territorium van deze Staat bevinden, zonder dat men fysisch het grondgebied van de andere Staat betreedt, verboden is. In de context van de nieuwe informatie- en telecommunicatietechnologieën dreigt de notie «territorialiteit» immers haar traditionele invulling te verliezen.

Het telecommunicatiegeheim valt echter duidelijk onder de bescherming van de persoonlijke levenssfeer. Een eenzijdige inmenging door een Staat in de privacy van de personen die zich op het grondgebied van een andere Staat bevinden en diens bescherming genieten, is derhalve onaanvaardbaar.

Deze bescherming wordt — wat België betreft — juridisch vastgelegd in artikel 8 van de Europese Verklaring van de rechten van de mens, artikel 22 van de Grondwet, de artikelen 259*bis* en 314*bis* van het Strafwetboek en artikel 109*ter* van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (de zogenaamde «Belgacom-wet»). Inzake de verwerking en het opslaan van het geïntercepteerde materiaal is bovendien de wet van 8 december 1992 inzake de bescherming van persoonsgegevens van toepassing.

Buitenlandse diensten hebben dus geen enkele bevoegdheid om op Belgisch grondgebied telecommunicatie te onderscheppen. Overeenkomstig de Belgische wet zijn zij overigens strafbaar indien zij gebruik maken van een territoriaal aanknopingspunt in België.

Van het bestaan van een systeem zoals «Echelon» moet een bijzondere impuls uitgaan inzake informaticabeveiliging.

Op dit vlak is er voor de overheid een belangrijke rol weggelegd bij het propageren van het veilig gebruik van de nieuwe technologieën, en met name door de oprichting van een permanent institutioneel platform, verplichte veiligheidsvereisten en het sensibiliseren van industrie en particulieren. Inzonderheid

mark. La participation danoise date de la Guerre froide. Les stations situées sur les îles de la mer Baltique et au Groenland permettaient de surveiller la Russie. D'autre part, dans l'optique de la création d'un bouclier de l'espace, l'importance du Groenland croît à nouveau.

6. RÉUNIONS AVEC LES MEMBRES DU GOUVERNEMENT

6.1. Audition de M. Verwilghen, ministre de la Justice (19 mai 2000)

Le ministre de la Justice explique que le droit international public ne donne pas de réponse non équivoque à la question de savoir si l'interception par un État de télécommunications entre des personnes qui ne se trouvent pas sur son territoire, sans que l'on pénètre physiquement sur le territoire de l'autre État, est interdite. La notion de territorialité risque en effet de perdre sa signification traditionnelle dans le contexte des nouvelles technologies de l'information et des télécommunications.

Le secret des télécommunications relève toutefois nettement du domaine de la protection de la vie privée. L'ingérence unilatérale d'un État dans la vie privée de personnes se trouvant sur le territoire d'un autre État qui leur accorde sa protection est dès lors inacceptable.

En ce qui concerne le droit belge, cette protection est consacrée par l'article 8 de la Déclaration européenne des droits de l'homme, l'article 22 de la Constitution, les articles 259*bis* et 314*bis* du Code pénal et l'article 109*ter* de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (dite «loi Belgacom»). La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel est en outre applicable au traitement et au stockage du matériel intercepté.

Les services étrangers n'ont donc aucune compétence pour intercepter des télécommunications sur le territoire belge. Ils sont d'ailleurs punissables conformément au droit belge s'ils font usage d'un point de rattachement territorial en Belgique.

L'existence d'un système du type d'«Echelon» constitue une incitation particulière à se protéger sur le plan informatique.

À cet égard, les pouvoirs publics ont un rôle important à jouer pour stimuler l'utilisation sûre des nouvelles technologies, notamment en instaurant une plate-forme institutionnelle permanente, en prévoyant des exigences de sécurité contraignantes et en sensibilisant l'industrie et les personnes privées. C'est

artikel 109*ter*F van de «Belgacom-wet» biedt nieuwe perspectieven voor het versleutelen van gegevens.

Politieke initiatieven zijn enkel op het niveau van de Europese Unie (EU) zinvol. Gelet op de eis van het Verenigd Koninkrijk om precies de inlichtingendiensten niet op te nemen in de overeenkomst tussen de EU-lidstaten inzake rechtshulp, vreest de heer Verwilghen echter dat een juridisch-normatieve actie op dit niveau slechts een geringe kans op slagen heeft. Het verdient wel aanbeveling om — op grond van de gemeenschapstrouw — het Verenigd Koninkrijk op dit punt politiek te isoleren.

Daarnaast meent de minister dat er bij de EU-lidstaten die tevens lid zijn van de «G7» en «G8», *in casu* Duitsland, Frankrijk en Italië, aangedrongen kan worden om dit vraagstuk alsnog op deze fora aan de orde te stellen.

De minister herinnert ook aan zijn voorstel om een structuur in het leven te roepen die snel kan tussenkomen bij een bedreiging van de systemen voor gegevensuitwisseling in België. Op grond van het zorgvuldigheidsbeginsel en onder het toezicht van de gerechtelijke overheden zouden dan de nodige preventieve maatregelen genomen kunnen worden. Hij zal — samen met de minister van Telecommunicatie en Overheidsbedrijven en Participaties — binnenkort aan de Ministerraad de oprichting van een interministerieel comité voorstellen dat de nodige preventieve en repressieve maatregelen moet nemen ter beveiliging van de informatienetwerken op ons grondgebied.

De minister meent eveneens dat het afluisteren van telefoongesprekken door de Veiligheid van de Staat wellicht opnieuw moet bekeken worden zonder evenwel in de fouten te vervallen die we aan anderen verwijten.

Ten slotte meent de heer Verwilghen dat het op internationaal vlak volstaat de actie van het Europees Parlement te steunen. Een duidelijke stellingname voorziet hij ten vroegste na de informele top van de Europese ministers van Binnenlandse Zaken en Justitie van 29 mei 2000.

Tijdens de daaropvolgende bespreking werd er op gewezen dat een onderscheid dient te worden gemaakt tussen de technische interceptiemiddelen als dusdanig en de filosofie van het gebruik ervan. Op voorwaarde dat het gebruik van deze middelen een sluitende wettelijke regeling krijgt, kan het inzetten ervan onze veiligheid ten goede komt.

Tevens wordt er op gewezen dat het «Echelon»-netwerk mogelijk bijgedragen heeft en nu nog steeds bijdraagt tot de beveiliging van België. Het mag dus niet uitsluitend negatief beoordeeld worden. Indien de Europese middelen van een zelfde orde zouden zijn als de Amerikaanse zou er op Europees niveau wellicht precies hetzelfde gebeuren.

surtout l'article 109*ter*F de la «loi Belgacom» qui offre de nouvelles perspectives en ce qui concerne le cryptage des données.

Les initiatives politiques ne sont utiles que si elles sont prises au niveau de l'Union européenne (UE). Eu égard à l'exigence du Royaume-Uni de ne pas inclure précisément les services de renseignements dans la Convention relative à l'entraide judiciaire entre les États membres de l'UE, M. Verwilghen craint cependant qu'une action juridico-normative à ce niveau n'ait que peu de chances de réussir. Il est toutefois indiqué d'isoler politiquement le Royaume-Uni sur ce point, en invoquant la fidélité communautaire.

En outre, le ministre estime que l'on peut insister auprès des États membres de l'UE qui sont également membres du «G7» et du «G8», en l'occurrence l'Allemagne, la France et l'Italie, pour qu'ils mettent la question à l'ordre du jour de ces forums.

Le ministre rappelle aussi qu'il avait proposé de créer une structure pouvant intervenir rapidement en cas de menaces sur les systèmes d'échange de données en Belgique. Sur la base du principe de précaution et sous la surveillance des autorités judiciaires, on pourrait alors prendre les mesures préventives nécessaires. Avec le ministre des Télécommunications et des Entreprises et Participations publiques, le ministre proposera sous peu au Conseil des ministres de créer un comité interministériel chargé de prendre les mesures préventives et répressives nécessaires pour sécuriser les réseaux d'information sur notre territoire.

Le ministre estime également qu'il faudra probablement réexaminer la question des écoutes téléphoniques organisées par la Sûreté de l'État, sans toutefois commettre les erreurs que nous reprochons à autrui.

Pour finir, M. Verwilghen pense qu'il suffit, au niveau international, d'appuyer l'action du Parlement européen. Il prévoit que l'on n'adoptera une position claire au plus tôt qu'à l'issue du sommet informel des ministres européens de l'Intérieur et de la Justice du 29 mai 2000.

Au cours de la discussion qui a suivi l'audition, on a souligné qu'il convient de faire une distinction entre les moyens d'interception techniques en tant que tels et la philosophie qui sous-tend leur utilisation. À condition que l'utilisation de ces moyens soit assortie d'une réglementation légale adéquate, elle peut profiter à notre société.

On souligne également que le réseau «Echelon» a peut-être contribué et contribue toujours à la sécurité de la Belgique. On ne peut donc l'assortir uniquement d'une appréciation négative. Si les moyens européens étaient de la même nature que les moyens américains, on constaterait peut-être les mêmes choses en Europe qu'aux États-Unis.

Ook werd geopperd dat mogelijk alleen een supranationaal gerechtelijk instituut, dat voor elk misdrijf over een eenduidige definitie beschikt, voor het gebruik van bewakingstechnologie een wettelijke oplossing kan aanreiken. Dit betekent echter dat men het eens moet worden over deze definities en dat er een gemeenschappelijk opsporingsapparaat in het leven geroepen moet worden. Rekening houdend met het feit dat deze voorwaarden zelfs in de Europese Unie nog niet vervuld zijn, valt te vrezen dat dit niet in de onmiddellijke toekomst verwezenlijkt kan worden.

Ook de minister van Justitie meent dat de voorliggende problematiek slechts opgelost kan worden door middel van een Europese regelgeving waarin bepaald wordt in welke gevallen er inlichtingen verzameld kunnen worden en in welke niet. Daarbij dient het inzetten van dergelijke middelen aan een driedubbele toetsing onderworpen te worden, met name: deze door de verantwoordelijke voor het onderzoek, deze door de onderzoeksrechter en ten slotte deze van de bodemrechter die geroepen is om desgevallend over de gerezen betwistingen te oordelen.

Binnen de Europese Unie ontstaat een gelijkaardige wetgeving op het vlak van telecommunicatie en het afluisteren van telefoonverkeer ingevolge de aanbeveling van het Ministercomité van de Raad van Europa van 7 februari 1995 aan de lidstaten over de bescherming van de gegevens van persoonlijke aard op het vlak van de telecommunicatie, inzonderheid rekening houdende met de telefoondiensten en de resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer. In deze context herinnert de minister tevens aan de inspanningen in het kader van zowel Europol als Eurojust.

De minister betreurt het ontbreken van een strafrechtelijk middel om — in het kader van de oneerlijke concurrentie — op te treden tegen industriële of economische spionage.

6.2. Vergadering met de heer Guy Verhofstadt, eerste minister, en de heer André Flahaut, minister van Landsverdediging (19 juli 2000)

De eerste minister verklaart dat de regering de vier aanbevelingen, die het Comité I in zijn « Vervolg op het rapport over het mogelijk bestaan van een Amerikaans systeem « Echelon » genaamd, voor het intercepteren van telefoon- en faxverkeer in België » geformuleerd heeft, positief benadert.

De regering zal niet nalaten de Belgische inlichtingendiensten de opdracht te geven, meer dan tot nu het geval was, alle informatie in te winnen inzake het verzamelen van economische inlichtingen.

Il a également été suggéré que seul un institut judiciaire supranational, disposant d'une définition univoque pour chaque délit, puisse éventuellement apporter une solution légale à l'utilisation de la technologie de surveillance. Cela signifie toutefois qu'il faut se mettre d'accord sur ces définitions et créer un instrument de repérage commun. Comme ces conditions ne sont même pas encore remplies dans l'Union européenne, l'intervenant craint que cela ne puisse pas se réaliser dans un avenir proche.

Le ministre de la Justice estime lui aussi que le problème qui nous occupe ne peut être résolu qu'au moyen d'une réglementation européenne qui prévoit dans quels cas des renseignements peuvent être recueillis et dans quels cas pas. Dans l'hypothèse d'une réglementation de ce genre, il convient de soumettre l'utilisation de pareils moyens à un triple contrôle: celui effectué par le responsable de l'enquête, celui effectué par le juge d'instruction et, enfin, celui effectué par le juge du fond qui sera appelé, le cas échéant, à se prononcer sur les contestations qui seraient apparues.

Une législation similaire relative aux télécommunications et aux écoutes téléphoniques voit le jour au sein de l'Union européenne à la suite de la recommandation du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications. Dans ce contexte, le ministre rappelle aussi les efforts qui ont été entrepris dans le cadre et d'Europol et d'Eurojust.

Le ministre regrette qu'il n'existe pas d'instrument pénal permettant d'intervenir, dans le cadre de la concurrence déloyale, contre l'espionnage industriel ou économique.

6.2. Réunion avec M. Guy Verhofstadt, premier ministre, et M. André Flahaut, ministre de la Défense nationale (19 juillet 2000)

Le premier ministre déclare que le gouvernement aborde positivement les quatre recommandations formulées par le Comité R dans son suivi du rapport sur « l'éventualité d'un système américain « Echelon » d'interception des communications téléphoniques et par fax en Belgique ».

Le gouvernement ne manquera pas de charger, plus que ce n'était le cas jusqu'à présent, les services de renseignement belges de recueillir toute information concernant la collecte de renseignements économiques.

Vervolgens zal de regering onderzoeken in hoeverre deze beide diensten voor het vervullen van deze taken bijkomende technische en menselijke middelen nodig hebben zonder dat deze hun organieke taken in het gedrang brengen.

Verder lijkt het hanteren van het algemeen beginsel van de voorzichtigheid in het beleid van de informatiebeveiliging een evidentie.

Inzake de vraag naar een nieuwe federale dienst, belast met het gecentraliseerd beleid inzake de informatiebeveiliging, herinnert de heer Verhofstadt aan de beslissing van het ministerieel comité voor Inlichting en Veiligheid van 16 februari 2000 om een technische werkgroep *ad hoc* in het leven te roepen die dient na te gaan van welke bestaande federale dienst of instelling de bevoegdheden uitgebreid kunnen worden met cryptografie en informatiebescherming.

Deze werkgroep bestaat — naast de afgevaardigden van de leden van dit comité — ook uit vertegenwoordigers van de ministers van Economie en Wetenschappelijk Onderzoek, Ambtenarenzaken en Modernisering van de openbare besturen alsmede van Telecommunicatie en Overheidsbedrijven en Participaties.

De eerste minister acht het niet wenselijk om een klacht neer te leggen bij het Europees Hof voor de rechten van de mens tegen de Europese landen die bij Echelon betrokken zijn en stelt voor de resultaten af te wachten van de tijdelijke commissie die in het Europees Parlement werd opgericht.

Tijdens de gedachtewisseling komt naar voor dat België binnen de Europese Unie steun zou moeten zoeken bij gelijkgezinde lidstaten vooraleer enige actie te ondernemen.

Opvallend is in dit verband de passieve houding die door een aantal Europese landen wordt aangenomen (de Duitse Bondsrepubliek, Frankrijk).

De begeleidingscommissies bepleitten een versnelde toename van de overheidsinspanningen inzake de bescherming van de privacy, de overheidsinformatie en van de economische gegevens.

Daarbij moet de overheid nadenken over de manier waarop zij haar burgers en ondernemingen kan beschermen tegen afluisterpraktijken van buitenlandse mogendheden en dient een overheidsdienst de opdracht te krijgen hoe het Belgische beslissingsproces op politiek en economisch vlak beveiligd kan worden.

Tenslotte drukken de begeleidingscommissies hun verwondering uit over de passiviteit van de Belgische inlichtingendiensten in deze problematiek.

Ensuite, il examinera dans quelle mesure ces deux services ont besoin de moyens techniques et humains supplémentaires pour accomplir ces tâches, sans que ne soit compromis l'exercice de leurs missions organiques.

Pour le reste, l'application du principe général de prudence dans la politique de protection des informations paraît évidente.

En ce qui concerne la demande d'un nouveau service fédéral chargé de la politique centralisée en matière de protection des informations, M. Verhofstadt rappelle la décision du comité ministériel du Renseignement et de la Sécurité du 16 février 2000 de créer un groupe de travail technique *ad hoc* chargé d'examiner de quel service ou organisme fédéral existant on peut étendre les compétences à la cryptographie et à la protection des informations.

Ce groupe de travail est constitué, outre des délégués des membres dudit comité, de représentants des ministres de l'Économie et de la Recherche scientifique, de la Fonction publique et de la Modernisation des administrations publiques ainsi que des Télécommunications et des Entreprises et Participations publiques.

Le premier ministre ne juge pas souhaitable de porter plainte auprès de la Cour européenne des droits de l'homme contre les pays européens impliqués dans le réseau Echelon et propose d'attendre les résultats des travaux de la commission temporaire qui a été créée au sein du Parlement européen.

Il ressort de l'échange de vues que la Belgique devrait rechercher, avant d'engager la moindre action au sein de l'Union européenne, l'appui d'États membres qui partagent sa manière de voir.

Ce qui surprend à cet égard, c'est l'attitude passive qu'adoptent une série de pays européens (la République fédérale d'Allemagne, la France).

Les commissions de suivi plaident en faveur d'un développement accéléré des efforts des autorités en matière de protection de la vie privée, de l'information des pouvoirs publics et des données économiques.

Les autorités doivent réfléchir en l'espèce à la manière dont elles peuvent protéger les citoyens et les entreprises contre les écoutes téléphoniques organisées par des puissances étrangères et il y a lieu de charger un service public d'examiner comment on peut protéger le processus décisionnel belge sur les plans politique et économique.

Enfin, les commissions de suivi se disent étonnées de la passivité des services de renseignements belges face à cette problématique.

7. JURIDISCHE ANALYSE VAN HET SYSTEEM ECHELON

De begeleidingscommissies hebben tijdens hun vergadering van 26 juni 2001 een hoorzitting gehouden met de heer P. Thomas, voorzitter van de Commissie voor de bescherming van het privé-leven, en de heer D. Yernault van de Université libre de Bruxelles, over de juridische aspecten van het Echelon-interceptiesysteem en dat zowel vanuit het perspectief van de Belgische wetgeving als dat van het internationaal recht.

7.1. Toepassingvandeprincipesinzakebescherming van de persoonlijke levenssfeer op het Echelonsysteem — Analyse van de heer P. Thomas (80), voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer

Privé-telecommunicatie wordt beschermd tegen kennisneming ervan door derden door de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en ook door de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en telecommunicatie.

De Commissie voor de bescherming van de persoonlijke levenssfeer heeft het initiatief genomen om over de informatie waarover zij beschikte met betrekking tot het bestaan en de werking van het interceptiesysteem «Echelon» een debat te organiseren in de groep van artikel 29, die op Europees niveau de vertegenwoordigers samenbrengt van de verschillende nationale controleautoriteiten die verantwoordelijk zijn voor de bescherming van de persoonsgegevens. Na die debatten werd de officiële aanbeveling van de groep van artikel 29 van 3 mei 1999 goedgekeurd (81).

Wat ook het doel van het onderscheppen van boodschappen moge zijn, vaststaat dat de algemene en verkennende aard ervan haaks staat op de beginselen van zowel het nationale als het internationale recht die een dergelijk grootschalig toezicht verbieden.

Het nationaal recht staat de verwerking van persoonsgegevens en in het bijzonder het onderscheppen van telecommunicatie slechts toe onder strikt bepaalde voorwaarden en met betrekking tot een welbepaalde persoon.

Krachtens artikel 5 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens mogen die persoonsgegevens niet worden gebruikt op een wijze die onverenigbaar is met de doeleinden.

7. ANALYSE JURIDIQUE DU SYSTÈME ÉCHELON

Au cours de leur réunion du 26 juin 2001, les commissions de suivi ont organisé une audition de M. P. Thomas, président de la Commission de la protection de la vie privée, et de M. D. Yernault de l'Université libre de Bruxelles sur les aspects juridiques du système d'interception Echelon, vus sous l'angle de la législation belge et sous celui du droit international.

7.1. Application des principes de protection de la vie privée au système «Echelon» — Analyse de M. P. Thomas, président de la Commission de la protection de la vie privée (80)

Les télécommunications privées sont protégées par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et également par la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées contre toute prise de connaissance par un tiers à la communication.

Au regard des informations dont elle disposait sur l'existence et le fonctionnement du système d'interception dénommé «Echelon», la Commission de la protection de la vie privée a pris l'initiative d'un débat sur la question au sein du groupe de l'article 29, qui rassemble au niveau européen les représentants des différentes autorités de contrôle nationales responsables de la protection des données à caractère personnel. La recommandation officielle du groupe de l'article 29 du 3 mai 1999 a été adoptée à la suite de ces débats (81).

Quel que soit l'objectif des interceptions, leur caractère général et exploratoire se heurte aux principes de droit tant national qu'international, qui proscrivent une telle surveillance sur une grande échelle.

Le droit national ne permet le traitement de données à caractère personnel, et en particulier l'interception des télécommunications, que dans des conditions strictement définies, et à l'encontre d'une personne déterminée.

En vertu de l'article 5 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ces données ne peuvent être excessives par rapport à l'objectif poursuivi.

Krachtens artikel 3 van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en -telecommunicaties (82) wordt een dergelijke onderschepping slechts zeer uitzonderlijk toegestaan door de onderzoeksrechter indien er ernstige aanwijzingen bestaan dat de wet wordt overtreden en dat de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.

Op Europees niveau gaat het algemeen en verkennend toezicht op de telecommunicatie in tegen inzonderheid de beginselen vervat in het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950 en tegen de interpretatie van artikel 8 van het Verdrag door het Europees Hof voor de rechten van de mens.

Het Europees Hof voor de rechten van de mens (83) heeft gesteld dat een toezichtsysteem (84) artikel 8 van het Europees Verdrag tot bescherming van de mensenrechten eerbiedigt voor zover:

— bewakingsmaatregelen zijn alleen mogelijk wanneer er aanwijzingen zijn dat iemand ernstige misdrijven plant, begaat of begaan heeft;

— ze mogen slechts getroffen worden wanneer iedere andere manier om de feiten vast te stellen geen kans van slagen heeft of ernstig belemmerd wordt;

— de bewaking mag slechts de verdachte zelf betreffen, of de personen die vermoedelijk met hem in contact staan.

Twee Europese richtlijnen bevestigen de verplichting om de persoonlijke levenssfeer en het vertrouwelijk karakter van de oproepen te beschermenn: richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (85).

Maatregelen ter versterking van de veiligheid en het vertrouwelijke karakter van de telecommunicatieoproepen moeten, met inachtneming van deze richtlijnen, op nationaal en internationaal niveau bevorderd worden.

Deze aanbeveling is actueler dan ooit, nu de inspanningen van de G8, de Raad van Europa en de Belgische Staat zich toespitsen op het onderscheppen van telecommunicatieverkeer om de computercriminaliteit te bestrijden. Elk initiatief om de inhoud en de gegevens van telecommunicatieoproepen technisch toegankelijk te maken, moet rekening houden met bovenvermelde fundamentele principes, moet

En vertu de l'article 3 de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (82), une telle interception n'est prévue qu'à titre exceptionnel, par le juge d'instruction, s'il existe des indices sérieux d'infraction à la loi et que les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

Au niveau européen, une surveillance générale et exploratoire des télécommunications va à l'encontre en particulier des principes de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et de l'interprétation de l'article 8 de la Convention par la Cour européenne des droits de l'homme.

La Cour européenne des droits de l'homme (83) a considéré qu'un système de surveillance (84) est conforme à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme dans la mesure où:

— les mesures de surveillance ne peuvent être effectuées que dans les cas où des indices permettent de soupçonner quelqu'un de projeter, accomplir ou avoir accompli certaines infractions graves;

— elles ne peuvent être prescrites que si l'établissement des faits d'une autre manière est voué à l'échec ou considérablement entravé;

— la surveillance ne peut concerner que le suspect lui-même ou les personnes présumées avoir des contacts avec lui.

Deux directives européennes consacrent également l'obligation de protection de la vie privée et la confidentialité des communications: la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (85).

Il importe qu'au niveau national et au niveau international, et dans le respect de ces textes, l'on encourage la prise de mesures visant à renforcer la sécurité et la confidentialité des télécommunications.

Cette recommandation prend tout son sens à l'heure actuelle, alors que, dans le cadre des travaux du G8, du Conseil de l'Europe et de l'État belge, les efforts convergent afin de faciliter l'interception des télécommunications dans le but de lutter contre la criminalité informatique. Toute initiative visant à rendre techniquement accessibles le contenu et les données de télécommunications doit tenir compte des

geschieden binnen een transparant kader, en in verhouding staan tot het beoogde doel.

7.2. Het Europees Verdrag voor de rechten van de mens (EVRM) als argument tegen het Echelonsysteem (86), D. Yernault

1. Het Europees Hof voor de rechten van de mens verbiedt gerechtelijke noch administratieve afluisterpratijken (87). Aangezien de afluisterpraktijken echter afwijken van het principiële recht op eerbiediging van het privé-leven en van de briefwisseling, dat bekrachtigd wordt in § 1 van artikel 8 EVRM moet, overeenkomstig § 2 van deze bepaling, aan drie cumulatieve voorwaarden voldaan worden: het wettigheidsprincipe, het legitimiteitsprincipe en het principe van de noodzaak in een democratische samenleving.

2. De regeringen en de inlichtingendiensten beweren dat het privé-leven van de eigen burgers geëerbiedigd wordt.

Het probleem is echter dat de elektronische inlichtingendiensten hun apparaten ook naar het buitenland, naar andere grondgebieden richten ... Deze handelwijze druist volledig in tegen het basisprincipe van het internationaal recht: de territoriale soevereiniteit. Zij druist ook in tegen een belangrijk persoonsrecht: de intimiteit van het privé-leven.

3. Een Staat zou de internationale rechtscolleges kunnen adiëren: het Internationaal Gerechtshof voor de schending van zijn territoriale soevereiniteit of het VN-Comité voor de mensenrechten overeenkomstig artikel 41 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, wegens de schending van artikel 17 daarvan. Een Europese Staat kan zich in de eerste plaats tot het Europees Hof voor de rechten van de mens wenden.

Particulieren en Staten staan juridisch gezien echter niet op voet van gelijkheid. Particulieren kunnen de schending van de territoriale soevereiniteit in strijd met artikel 2 van het VN-Charter niet aanvoeren voor het Internationaal Gerechtshof.

Bovendien kunnen individuen alleen bepalingen aanvoeren die hun rechten effectief beschermen: de Universele Verklaring van de rechten van de mens heeft, voor de Staten en dus voor individuen, geen dwingende rechtskracht (het is gewoon een resolutie van de algemene vergadering van de VN). Ook artikel 22 van het Internationaal Verdrag betreffende de telecommunicatie (Handvest van de Internationale Vereniging voor telecommunicatie) zet de lidstaten er alleen toe aan alle nodige maatregelen te nemen om de

principes fondamentaux susmentionnés et être effectuée dans un cadre transparent et proportionnel aux objectifs poursuivis.

7.2. Efficacité de la Convention européenne des droits de l'homme (CEDH) pour contester le système « Echelon » (86), D. Yernault

1. La Cour européenne des droits de l'homme n'interdit pas les écoutes judiciaires, ni même les écoutes administratives (87) mais ces écoutes, en ce qu'elles dérogent au principe du respect du droit à la vie privée et du respect de la correspondance porté par le § 1er de l'article 8 CEDH, doivent, conformément au § 2 de cette disposition, respecter trois conditions cumulatives, à savoir: le principe de légalité, le principe de légitimité et le principe de nécessité dans une société démocratique.

2. Il faut constater que les gouvernements et leurs services de renseignements assurent que la vie privée de leurs concitoyens est respectée.

Le problème est que les services de renseignements électroniques dirigent leurs appareils vers l'étranger, d'autres territoires, ... Une telle situation est en contradiction fondamentale avec un principe à la base même du droit international: la souveraineté territoriale. Une situation en contradiction fondamentale avec un droit immanent de la personne: l'intimité de la vie privée.

3. Il est concevable qu'un État saisisse les juridictions internationales: la Cour internationale de justice pour violation de sa souveraineté territoriale ou le Comité des droits de l'homme de l'ONU en vertu de l'article 41 du Pacte international relatif aux droits civils et politiques pour violation de l'article 17 de celui-ci. Un État européen pourrait surtout utilement saisir la Cour européenne des droits de l'homme.

Néanmoins, particuliers et États ne sont, juridiquement parlant, pas sur un pied d'égalité. Invoquer une violation de la souveraineté territoriale en contradiction avec l'article 2 de la Charte de l'ONU devant la Cour internationale de justice est impossible pour les premiers.

Les individus ne peuvent de surcroît invoquer que des dispositions qui protègent effectivement leurs droits: la Déclaration universelle des droits de l'homme n'a, pour les États et donc pour les individus, aucune force juridique contraignante (c'est une simple résolution de l'assemblée générale de l'ONU). De même, l'article 22 de la Convention internationale des télécommunications (charte de l'UIT) n'engage ses États parties qu'à prendre toutes les mesures possibles pour garantir la confidentialité des télécommu-

geheimhouding van de internationale telecommunicatie te waarborgen. Dit verdrag heeft dus ook geen rechtstreekse gevolgen voor individuen.

Ook de mogelijkheid om het Echelonnetwerk aan te vallen voor het VN-Comité voor de mensenrechten zijn zeer beperkt, aangezien de Verenigde Staten en het Verenigd Koninkrijk niet zijn toegetreden tot het facultatief protocol dat individuen de mogelijkheden biedt om een zaak voor dat Comité te brengen. Het heeft ook geen zin om de Amerikaanse rechtscolleges te adiëren aangezien de waarborgen uit de Amerikaanse grondwet niet van toepassing zijn op « niet-Amerikanen ».

In zekere zin komt men uit juridische noodzaak tot het EVRM, dat het meest geschikte instrument is ter verdediging van de fundamentele rechten.

4. Het EVRM regelt ontegensprekelijk de internationale betrekkingen van de Staten, vanuit hun grondgebied of wegens de activiteiten van hun instellingen die gevolgen hebben buiten het grondgebied.

• Het is een instrument van Europese openbare orde : geheel van objectieve plichten die de Europese Staten aangegaan zijn voor hun onderlinge betrekkingen maar vooral jegens de burgers binnen hun rechtsgebied; in 1995 werd het EVRM door het Hof van Straatsburg zelf omschreven als een instrument voor de Europese openbare orde;

• Het is een internationaal verdrag : het EVRM is een verdrag dat Staten internationaal verantwoordelijk kan stellen op het vlak van de bescherming van de fundamentele vrijheden; de huidige interpretatie van artikel 1 EVRM maakt het ontegensprekelijk mogelijk de verantwoordelijkheid vast te stellen van Staten die :

— ofwel actief meewerken aan Echelon (zoals blijkbaar het Verenigd Koninkrijk);

— ofwel er passief aan meewerken (wat eerder door Duitsland het geval zou zijn) door hun grondgebied open te stellen voor diensten van derden;

• Het is een bijzonder internationaal verdrag omdat de Staten die het goedkeuren, op grond van artikel 53 erkennen dat het juridisch voorrang heeft op iedere andere internationale of nationale norm die de fundamentele rechten in mindere mate beschermt dan het Verdrag.

5. Artikel 8 EVRM is een concrete regel die aan de basis ligt van het hele Europese recht ter bescherming van het privé-leven (88).

Iedere onderschepping van een bericht betekent een inmenging in het privé-leven in de zin van artikel 8, § 1, EVRM, en kan krachtens artikel 8, § 2,

nications internationales. Cette convention n'emporte donc pas d'effet direct pour les individus.

Les possibilités de saisir le Comité des droits de l'homme de l'ONU sont singulièrement réduites, si l'on veut contester Echelon, puisque les USA et le Royaume-Uni n'ont pas adhéré au protocole facultatif permettant la saisine individuelle du Comité. Il serait tout aussi vain d'ailleurs de vouloir saisir les juridictions américaines puisque les garanties constitutionnelles américaines ne sont pas applicables aux personnes « non américaines ».

C'est donc en quelque sorte par nécessité juridique que l'on a recours à la CEDH, qui constitue l'instrument le plus apte à la défense des droits fondamentaux.

4. La CEDH régit incontestablement les rapports internationaux des États, que ce soit à partir de leur territoire ou en raison du comportement de leurs organes déployant leurs effets en dehors du territoire.

• Elle est un instrument de l'ordre public européen : tissu d'obligations objectives contractées par les États européens dans leurs relations entre eux mais aussi et d'abord à l'égard des particuliers sous leur juridiction; la CEDH a été qualifiée en 1995 par la Cour de Strasbourg elle-même d'instrument de l'ordre public européen;

• Elle est un traité international : la CEDH est un traité qui permet la mise en œuvre de la responsabilité internationale des États dans le domaine de la protection des droits fondamentaux; l'interprétation actuelle de l'article 1er CEDH permet sans conteste d'établir la responsabilité des États qui :

— soit participeraient activement à Echelon (ce qui serait le cas du Royaume-Uni);

— soit y participeraient passivement (ce qui serait plutôt le cas de l'Allemagne) en mettant leur territoire à disposition de services tiers;

• Elle est un traité international ayant donc une nature particulière parce qu'en y adhérant, les États, en vertu de son article 53, reconnaissent sa primauté juridique sur toute autre norme internationale ou interne qui serait moins protectrice des droits fondamentaux portés par la Convention.

5. L'article 8 CEDH est une règle concrète sous les auspices de laquelle l'intégralité du droit européen visant à la protection de la vie privée s'est en tout temps placé (88).

Toute interception de communication est constitutive d'une ingérence dans la vie privée au sens de l'article 8, § 1er, CEDH qui ne peut passer pour valide au

EVRM slechts gewettigd zijn indien drie voorwaarden samen vervuld zijn: de wettigheid, de legitimiteit en de noodzaak in een democratische samenleving.

1) de wettigheidsvoorwaarde legt verschillende verplichtingen op:

— er moet een «wet» bestaan die de inmenging toestaat;

— een «wet» moet toegankelijk zijn. Echelon is dus overduidelijk in tegenspraak met artikel 8 EVRM, aangezien de parlementen van de Staten die aan Echelon zouden meewerken zelf geen weet hebben van de internationale overeenkomsten die de werkwijze van hun inlichtingendiensten regelen. Een Brits staatsburger heeft al geen toegang tot de geldende normen. Hoe zouden de staatsburgers van een ander land het dan hebben?

• de «wet» moet «voorzienbaar» zijn. Geheime toezichtsmaatregelen die gerechtvaardigd zijn met het oog op de nationale veiligheid kunnen weliswaar een versoepeling van de toepassingsvoorwaarden vereisen , maar de betrokken personen moeten voldoende duidelijk weten welke bestuurlijke praktijken gelden inzake veiligheidsonderzoeken;

• de «wet» moet het internationaal recht eerbiedigen. Overeenkomstig het EVRM moet elke inmenging de «wet» eerbiedigen. Een flagrante schending van het internationaal recht impliceert dus automatisch dat de «wet» niet geëerbiedigd is, vooral als het een zo belangrijk principe betreft als de eebiediging van de territoriale soevereiniteit van andere Staten, dat immers de grondslag vormt van het internationaal recht;

• de «wet» moet artikel 53 EVRM eerbiedigen, dat bevestigt dat het verdrag voorrang heeft op alle interne of internationale rechtsregels die de rechten van de mens minder beschermen.

Echelon is dus duidelijk in strijd met de wettigheidsvoorwaarde.

2) Interceptie kan alleen legitiem zijn als ze een van de doeleinden nastreeft die limitatief zijn opgesomd in artikel 8, § 2.

3) De Europese jurisprudentie over de derde voorwaarde die bij de interceptie van telecommunicatie moet worden nageleefd, namelijk de noodzaak in een democratische maatschappij, is even omvangrijk. In dit verband kan het Echelonnetwerk op twee belangrijke punten worden bekritiseerd: de schending van het verbod op exploratieve en algemene afluisterpraktijken enerzijds en het ontbreken van procedurele waarborgen anderzijds.

— Staten beschikken over een zekere beoordelingsruimte aangaande de noodzaak van inmengingen in de persoonlijke levenssfeer. Het arrest Klass

regard de l'article 8, § 2, CEDH que si elle répond à trois conditions cumulatives: la légalité, la légitimité et la nécessité dans une société démocratique.

1) la condition de légalité impose plusieurs obligations:

— une «loi» doit exister pour permettre une ingérence;

— une «loi» doit être «accessible». Il ne fait alors vraiment plus aucun doute qu'Echelon est contraire à l'article 8 de la CEDH étant donné que les Parlements des États censés participer à Echelon ignorent eux-mêmes les accords internationaux régissant la manière d'opérer de leurs services de renseignements. Un citoyen britannique n'a déjà pas accès aux normes applicables. Que dire alors des citoyens des autres États?

• la «loi» doit être «prévisible». Même si les mesures de surveillance secrètes justifiées par la sécurité nationale commandent un assouplissement de la condition d'accessibilité, toutes les personnes intéressées doivent connaître avec suffisamment de clarté les pratiques administratives gouvernant les enquêtes de sécurité;

• la «loi» doit respecter le droit international. Pour être conforme à la CEDH, une ingérence doit respecter la «loi». Une violation flagrante du droit international ne saurait donc non plus mener à conclure que la «loi» a été respectée, surtout quand il s'agit d'un principe aussi éminent que celui du respect dû à la souveraineté des autres États qui est le fondement même du droit international;

• la «loi» doit respecter l'article 53 CEDH qui consacre la primauté de la Convention sur toute autre norme interne ou internationale qui serait moins protectice des droits de l'homme.

Echelon est donc clairement en infraction avec cette condition de légalité.

2) Une interception ne sera légitime que si elle poursuit un des buts strictement énumérés par l'article 8, § 2.

3) Par contre, la jurisprudence européenne relative à la troisième condition que doivent respecter les interceptions de télécommunications, à savoir celle de leur nécessité dans une société démocratique, est tout aussi substantielle. Deux reproches majeurs peuvent être formulés à ce titre à l'égard d'Echelon: sa contradiction avec l'interdiction des écoutes exploratoires et générales, d'une part, et son déficit de garanties procédurales, d'autre part.

— Pour apprécier la nécessité des ingérences dans la vie privée, les États jouissent d'une marge d'appréciation, mais l'arrêt Klass contre Allemagne

versus Duitsland van 1978 heeft echter bevestigd dat die marge niet onbeperkt is, omdat geheime toezichtsmaatregelen de democratie anders zouden ontkrachten onder het mom van ze te verdedigen. Vandaar het verbod op verkennende en algemene toezichtsmaatregelen. Daarom bekritiseert de werkgroep «Artikel 29»(89) terecht systemen voor algemene telefoontap en «sniffing», de veralgemeende controle op elektronische briefwisseling, die volstrekt strijdig zijn met artikel 8 EVRM. Moet nog worden gezegd dat daarmee de Echelon- en Carnivoresystemen werden bedoeld?

— De controle op de noodzaak waarvan sprake is in artikel 8 EVRM, vertoont ook een nieuw aspect met betrekking tot de procedurele vereisten: een inmenging wordt enkel als evenredig met het nagestreefde doel beschouwd als zij het resultaat is van een besluitvormingsproces dat billijk is voor de burger. Met betrekking tot de administratieve afluisterpraktijken, wordt minstens een voldoende efficiënte parlementaire controle geëist.

Al deze regels gelden voor algemene interceptiesystemen — of die nu alle communicatietypes kunnen onderscheppen dan wel slechts bepaalde types — maar ook voor gerichte intercepties van doelwitten.

6. Artikel 13 van het EVRM en de positieve verplichtingen verbonden aan de bescherming van andere rechten maken dat Staten de plicht hebben om schendingen te voorkomen, door wie zij ook gepleegd worden, en dat zij schendingen moeten onderzoeken en bestraffen en — indien nodig — de schade moeten herstellen.

Een Staat kan dus verantwoordelijk worden geacht voor een schending van het EVRM als hij zijn grondgebied ter beschikking stelt van een andere Staat die handelingen uitvoert die gelijk staan met een schending van het Verdrag: het is de eigen verantwoordelijkheid van de eerste Staat (hypothese van een interceptiestation op het grondgebied van de Staat).

Zoals gebruikelijk in het internationaal recht blijft een Staat verantwoordelijk voor de daden van zijn instellingen, ook als deze zich buiten het nationale territorium bevinden.

7. Handelingen van Verdragsluitende Staten met grensoverschrijdende gevolgen moeten ook de mensenrechten beschermen die het EVRM garandeert.

Ondanks het feit dat volgens het internationaal recht de territoriale soevereiniteit in acht moet worden genomen handelen een aantal teksten over de grensoverschrijdende interceptie van telecommunicatie en over het feit dat het recht op een persoonlijke levenssfeer moet worden geëerbiedigd.

Het verbod op grensoverschrijdende intercepties zonder de toestemming van de Staat waarin het doel-

de 1978 a affirmé que cette latitude n'était pas illimitée, sans quoi les mesures de surveillance secrète saperaient la démocratie au motif de la défendre. D'où l'interdiction des surveillances exploratoires et générales. C'est dès lors à bon droit que le groupe de travail «Article 29»(89) fustige les systèmes généraux d'interceptions téléphoniques ou le «sniffing», soit le contrôle généralisé du trafic des courriers électroniques, pratiques en contradiction fondamentale avec l'article 8 CEDH. Faut-il préciser qu'étaient visés les systèmes Echelon et Carnivore?

— La nouvelle dimension de l'article 8 CEDH au titre du contrôle de nécessité a trait à l'existence d'exigences procédurales: une ingérence n'est réputée proportionnée au but poursuivi que si elle intervient aux termes d'un processus décisionnel équitable pour l'individu. Dans le cas des écoutes administratives, il est au moins requis qu'existe un contrôle parlementaire suffisamment efficace.

L'ensemble de ces règles s'appliquent aux systèmes globaux d'interception, qu'ils puissent capter tout type ou seulement certains types de communications, mais aussi aux interceptions individualisées de cibles.

6. L'article 13 CEDH, comme les obligations positives inhérentes à la protection des autres droits garantis, a pour conséquence que les États ont le devoir de prévenir les violations quels qu'en soient les auteurs et, en cas de violations, d'enquêter, de punir celles-ci ainsi que, le cas échéant, de les réparer.

Un État peut donc être tenu pour responsable d'une violation de la CEDH s'il met son territoire à disposition d'un autre État, ce dernier perpétrant des actes équivalant à la violation: c'est sa responsabilité propre que le premier État engage (hypothèse de l'accueil d'une station d'interception).

Du reste, un État demeure, on ne peut plus classiquement au regard du droit international, tenu des agissements de ses organes, y compris lorsque ceux-ci se déploient en dehors du territoire national.

7. Les comportements des États parties qui ont des conséquences transfrontalières doivent eux aussi respecter la protection des droits de l'homme assuré par la CEDH.

Or, par-delà le respect dû à la souveraineté territoriale conformément au droit international général, un ensemble de textes traitent des interceptions transfrontalières de télécommunications, et du respect tout autant dû au droit à la vie privée.

L'interdiction des interceptions transfrontalières en dehors du consentement de l'État où est localisée la

wit zich bevindt, is dus slechts een specifieke toepassing van het grondbeginsel van het internationaal recht dat het Permanent Hof van Internationale Justitie in 1927 in de zaak Lotus heeft omschreven (90).

De antwoorden van de Britse regering doen uitschijnen dat het medebestuur van de basis van Menwith Hill past binnen het Akkoord van Londen dat op 19 juni 1951 is afgesloten tussen de NAVO-lidstaten betreffende de rechtspositie van hun krijgsmachten. Toch moet ook het Brits recht het EVRM naleven en mag de Britse regering zich niet eenzijdig onttrekken aan haar verplichtingen onder het voorwendsel dat zij handelt in het raam van andere internationale overeenkomsten.

Het beginsel van territoriale soevereiniteit blijft de grondslag van het algemeen internationaal recht. Als bewijs van de kracht van dit beginsel geldt de beslissing van de Europese Raad van 22 november 1996, om een gemeenschappeljke actie te ondernemen met betrekking tot beschermingsmaatregelen tegen de gevolgen van een extraterritoriale toepassing van wetgeving aangenomen door een derde land (betwisting van de Amerikaanse wetten D'Amato en Helms-Burton).

Daarom ook heeft de Raad van Europa het gebruik van grensoverschrijdende intercepties verworpen in zijn ontwerpverdrag over de cybercriminaliteit (waarover vooral onderhandeld is met de Verenigde Staten).

8. De hamvraag blijft of de interne rechtsmiddelen van de Staten, die men ervan verdenkt deel uit te maken van Echelon, al dan niet eerst moeten worden uitgeput. Op dit principe bestaan in de rechtsorde die het EVRM creëert, talrijke uitzonderingen waarvan er minstens drie kunnen worden aangevoerd als argument tegen het uitputten van de rechtsmiddelen van de Staten die aan Echelon deelnemen.

• Alleen de interne rechtsmiddelen die efficiënt zijn, dat wil zeggen die de aangevoerde schending kunnen verhelpen en die toegankelijk zijn, moeten worden uitgeput. Nemen we het voorbeeld van Duitsland dat er zich toe zou beperken op zijn grondgebied een NSA-basis te laten functioneren (Bad Aibling). Het lijkt vast te staan dat Duitsland, op grond van het vertrouwen tussen Duitsland en Amerika, niet controleert of de NSA Duitse burgers en ondernemingen afluistert. Daaruit kan men logischerwijze afleiden dat Duitsland nog veel minder toezicht uitoefent op de activiteiten van de NSA betreffende het grondgebied van derde landen. Wat is bovendien het nut van een rechtszaak tegen Duitsland wegens een schending van het EVRM, die vooral berust op het optreden van een Amerikaanse dienst onder het gezag van een uitvoerende macht die weigert te erkennen of te ontkennen dat zij betrokken is bij het Echelon-netwerk?

Dezelfde redenering gaat ook op voor het Verenigd Koninkrijk dat op zijn grondgebied geen toezicht

cible ne constitue donc jamais qu'une application particulière d'un principe fondamental du droit international formulé en 1927 par la Cour permanente de justice internationale dans l'affaire du Lotus (90).

Quand bien même, ce que semblent indiquer les réponses du gouvernement britannique, la cogestion de la base de Menwith Hill se déroulerait-elle dans le cadre de l'Accord de Londres du 19 juin 1951 passé entres les États de l'OTAN sur le statut de leurs forces, il faudrait objecter que le droit britannique doit respecter la CEDH également et que le gouvernement britannique ne pourrait se dédouaner unilatéralement des engagements y souscrits sous prétexte qu'il agit dans le cadre d'autres engagements internationaux.

Le principe de souveraineté territoriale reste la base même du droit international général. C'est si vrai que le Conseil européen, pour illustrer le propos dans un autre domaine, a décidé le 22 novembre 1996 une action commune relative aux mesures de protection contre les effets de l'application extra-territoriale d'une législation adoptée par un pays tiers (contestation des lois américaines dites D'Amato et Helms-Burton).

C'est si vrai aussi que le Conseil de l'Europe a supprimé la possibilité de recourir aux interceptions transfrontalières dans son projet de convention sur la cybercriminalité (la négociation ayant été notamment menée avec les USA).

8. La question primordiale reste avant tout celle de savoir s'il y a lieu ou non d'épuiser les voies de recours ménagées par le droit des États dont on soupçonne qu'ils font partie d'Echelon. Or, ce principe connaît, en particulier dans l'ordre juridique généré par la CEDH, plusieurs exceptions dont trois au moins peuvent être invoquées pour ne pas épuiser les recours des États participant à Echelon.

• Ne doivent être épuisés que les recours internes qui sont effectifs, c'est-à-dire qui permettent de redresser la violation alléguée, et accessibles. Prenons d'abord l'Allemagne qui se bornerait à accueillir sur son territoire une base de la NSA (Bad Aibling). Il semble établi que l'Allemagne, invoquant la confiance germano-américaine, ne contrôle pas si la NSA écoute ou non les citoyens et entreprises allemandes. On peut alors raisonnablement penser que l'Allemagne contrôle encore moins les activités de la NSA concernant des territoires nationaux tiers. Quelle serait de surcroît l'efficacité de recours dirigés contre un manquement à la CEDH par l'Allemagne qui trouve sa source première dans les agissements d'un service américain sous l'autorité d'un exécutif qui refuse de reconnaître ou démentir son implication dans Echelon?

Le même raisonnement peut être tenu à propos du Royaume-Uni en raison de son manque de vigilance

houdt op de door NSA uitgevoerde intercepties. De weigering van de Britse regering om te antwoorden op een aantal parlementaire vragen aangaande Echelon en de duidelijke onwil van het Britse Parlement om in te gaan op verzoeken van andere nationale parlementaire onderzoekscommissies wekken uiteraard niet veel vertrouwen in de efficiëntie van de Britse interne rechtsmiddelen.

Aangezien Echelon een multinationaal systeem heet te zijn, kan men zich ook afvragen welke rechtsmiddelen moeten worden uitgeput: die van alle of van één deelnemende Staat? Als het slechts één deelnemende Staat is, welke dan?

Wat de Britse rechtsmiddelen betreft, moet men ten slotte rekening houden met het arrest van de House of Lords in de zaak Holland *versus* Lamen-Wolfe van 20 juni 2000. Met betrekking tot dit eenvoudige sociale geschil dat zich afspeelde op de basis van Menwith Hill, oordeelde het House of Lords dat de Amerikaanse regering immuniteit van rechtsvervolging genoot en daarom niet voor de Britse rechtscolleges kon worden gebracht (een Lord voegde daaraan toe dat aangezien de VS geen partij is bij het EVRM, de jurisprudentie van het Hof over de immuniteiten in dit geval niet tegengeworpen kan worden).

• Met betrekking tot personen die verblijven op het grondgebied van Staten die niet deelnemen aan Echelon, kan bovendien worden gesteld dat de rechtsmacht die de Engelse diensten buiten het Engelse grondgebied uitoefenen, ongeoorloofd is krachtens het internationaal recht en het EVRM. Deze internationaal onwettige rechtsmacht is het gevolg van de verplichting om de rechtsmiddelen uit te putten van de Staat die een van zijn internationale verbintenissen, *i.c.* het EVRM, niet naleeft.

• Zelfs wanneer de intercepties in overeenstemming zijn met de interne rechtsregels van de Staten die aan Echelon deelnemen, zijn ze, volkenrechtelijk, inbreuken aangezien ze het door het internationaal recht toegestane territoriaal kader overstijgen. Deze inbreuken maken deel uit van een geheel van soortgelijke inbreuken op het recht op het privé-leven, die door de betrokken Staten herhaaldelijk gepleegd en gedoogd worden. Een dergelijk geheel van inbreuken is dus een bestuurlijke praktijk. Zij maakt iedere procedure vergeefs of ondoeltreffend omdat zij niet gebaseerd is op een wettekst of regel waarnaar de lidstaten van Echelon rechtsgeldig kunnen verwijzen. Ook in dit geval is noch een Staat, noch een individu, verplicht alle Duitse en Britse rechtsmiddelen uit te putten.

Het arrest Cyprus *versus* Turkije herinnert eraan dat het bestaan van wetgevende en bestuurlijke praktijken die overduidelijk strijdig zijn met, onder meer, artikel 8 EVRM, de verzoekende Staat, maar ook de individuen die hierop een beroep doen, ontslaat van

sur son territoire à l'endroit des interceptions effectuées par la NSA. Le refus du gouvernement britannique de répondre à plusieurs questions parlementaires portant sur Echelon ou les réticences marquées par le Parlement britannique à répondre aux demandes formulées par d'autres missions d'enquête parlementaires nationales ne sont pas non plus de nature à forger la conviction de l'efficacité des recours britanniques.

Il n'est pas interdit non plus de se demander, Échelon étant supposé être un système multinational, quels sont les recours à épuiser: ceux de tous ou d'un seul État participant? Si c'est d'un seul État, lequel?

Pour ce qui est des recours britanniques, il faut enfin tenir compte de l'arrêt rendu le 20 juin 2000 par la Chambre des Lords dans l'affaire Holland v. Lamen-Wolfe qui, dans un simple litige social s'étant déroulé sur la base de Menwith Hill, a estimé que l'immunité de juridiction du gouvernement américain empêchait que celui-ci soit appelé à la cause devant les juridictions britanniques (un Lord a ajouté que les USA n'étant pas parties à la CEDH, la jurisprudence de la Cour sur les immunités ne pourrait pas leur être opposée).

• En ce qui concerne les personnes résidant sur le territoire des États non participants à Echelon, il peut de surcroît être soutenu que la juridiction exercée par les services anglais en dehors du territoire anglais est illicite au regard du droit international et de la CEDH. Cette juridiction internationalement illicite relève de l'obligation d'épuiser les voies de recours de l'État auteur de la violation d'un de ses engagements internationaux, en l'occurrence la CEDH.

• Même si les interceptions sont conformes aux règles de droit interne des États participant à Echelon, elles n'en constituent pas moins, du point de vue du droit des gens, des violations puisqu'elles dépassent le cadre territorial autorisé par le droit international. Ces violations s'inscrivent dans un ensemble de violations semblables du droit à la vie privée, violations répétées et tolérées par les États concernés. Un tel ensemble de violations constitue donc des pratiques administratives. Celles-ci rendent vaine ou inefficace toute procédure parce qu'elles ne reposent sur aucun texte légal ou réglementaire qui puisse, en l'occurrence, être valablement invoqué par les États membres d'Echelon. Dans ce cas également, il n'y a, ni pour un État, ni pour un particulier, obligation d'épuiser les recours allemands et britanniques.

L'arrêt Chypre contre Turquie vient de rappeler que l'existence de pratiques législatives et administratives en contradiction manifeste avec, notamment, l'article 8 CEDH, dispense l'État requérant, mais également les particuliers qui s'en prévalent, de

de verplichting om alle interne rechtsmiddelen van de verwerende Staat uit te putten.

9. Door te stellen dat het bestaan van wetten en praktijken die een systeem voor de geheime bewaking van communicatie toestaan en invoeren op zich een «inmenging» vormt, vergemakkelijkt het arrest Klass aanzienlijk de taak van degenen die Echelon willen aanvechten voor de interne of Europese rechtbanken. Paradoxaal genoeg is het dus de geheime aard van de systemen voor elektronische bewaking die deze mogelijkheid biedt. De hoedanigheid van gebruiker van de telecommunicatiediensten volstaat aldus om de directe aantasting van de rechten, gewaarborgd door artikel 8 van het EVRM, aan te vechten.

Hoewel ze voor verbetering vatbaar zijn, bestaan de juridische middelen om voortaan Echelon, net zoals elk ander soortgelijk systeem trouwens, aan te vechten dus wel degelijk.

De strijd tegen het crimineel gebruik van de telecommunicatietechnologie is gewettigd maar moet ook rechtmatig zijn. Daaraan wordt terecht herinnerd in de resolutie die op 11 april 2000 werd aangenomen door de Commissie vrijheden en rechten van de burgers van het Europees Parlement.

De resolutie die werd besproken in de tijdelijke commissie van het Europees Parlement heeft voortaan de bescherming van de persoonlijke levenssfeer die door artikel 8 van het EVRM gewaarborgd wordt, beter afgebakend. Punt 26 van de resolutie:

«doet een beroep op Duitsland en het Verenigd Koninkrijk om hun voortgezette toestemming voor interceptie van communicatie door de inlichtingendiensten van de Verenigde Staten vanaf hun grondgebied afhankelijk te stellen van de vraag of deze activiteiten in overeenstemming zijn met het EVRM, dit wil zeggen dat zij voldoen aan het beginsel van proprotionaliteit, dat hun rechtsgrondslag transparant is en de gevolgen ervan voor de individuele persoon duidelijk zijn en dat er een doelmatige controle op deze activiteiten bestaat, aangezien deze landen verantwoordelijk zijn voor de conformiteit met de mensenrechten van vanaf hun grondgebied uitgevoerde — of zelfs maar gedulde — activiteiten van inlichtingendiensten.»

Zowel het algemeen internationaal recht als het internationaal en Europes recht inzake mensenrechten kunnen het privé-leven van de individuen beschermen. De principes, die in het bijzonder door het EVRM gehuldigd worden, zijn niet alleen van toepassing op Echelon. Zij gelden ook voor alle soortgelijke nationale of internationale systemen. Men mag niet vergeten dat deze beginselen in eerste instantie de gerichte interceptie van communicatie van individuen, bedrijven of niet-gouvernementele organisaties betreffen. Echelon is slechts de top van de ijsberg.

l'obligation d'épuiser les voies de recours internes ménagées par l'État défendeur.

9. L'arrêt Klass, en posant que «l'existence (...) de lois et pratiques autorisant et instaurant un système de surveillance secrète des communications constitue en soi une 'ingérence'», facilite considérablement la tâche de ceux qui désirent contester Échelon devant des juridictions internes ou européenne. C'est donc paradoxalement le caractère secret des systèmes de surveillance électronique qui offre ces facilités. La simple qualité d'usager des services de télécommunications suffit ainsi pour contester les atteintes directes aux droits garantis par l'article 8 de la CEDH que constituent les actes d'interception des télécommunications.

Même perfectibles, les moyens juridiques de contrer d'ores et déjà Échelon, comme n'importe quel autre système similaire d'ailleurs, existent donc bel et bien.

La lutte contre les usages criminels des technologies des télécommunications est légitime mais elle doit aussi être licite. C'est ce que rappelait opportunément la résolution adoptée le 11 avril 2000 par la Commission des libertés et des droits des citoyens du Parlement européen.

La résolution qui a été discutée au sein de la Commission temporaire du PE a désormais pris la juste mesure de la protection offerte à la vie privée par l'article 8 CEDH. En effet, le point 26 de la résolution:

«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.»

Tant le droit international général que le droit international et européen des droits de l'homme peuvent utilement protéger la vie privée des individus. Les principes portés en particulier par la CEDH n'ont pas seulement vocation à s'appliquer à Échelon. Ils concernent également tous les systèmes, nationaux ou internationaux, similaires. Ces principes, il convient de ne pas l'oublier, régissent d'abord la captation ciblée des communications d'individus, d'entreprises ou d'organisations non gouvernementales. Échelon n'est que la partie visible de l'iceberg.

Door de toename van de gevaren die voortvloeien uit nieuwe bewakingstechnlogieën, blijft het EVRM het doeltreffendste instrument voor de bescherming van privé-personen maar ook van de rechten van de betrokken Staten die de plicht hebben dit verdrag na te leven en het te doen naleven.

7.3. VerenigbaarheidvanEchelonofanderecommunicatie-afluistersystemen met het Gemeenschapsrecht

De Tijdelijke Commissie Echelon-interceptiesysteem van het Europees Parlement had onder meer als opdracht te onderzoeken of een communicatieafluistersysteem van het type Echelon verenigbaar is met het Gemeenschapsrecht. In zijn verslag doet de tijdelijke commissie dit in twee stappen. In een eerste stap onderzoekt de commissie of het bestaan van een dergelijk spionagesysteem verenigbaar is met het recht van de Unie. In de tweede plaats onderzoekt de commissie of het Gemeenschapsrecht wordt geschonden als het systeem wordt gebruikt voor economische spionage (91).

Over de verenigbaarheid met het EG-recht wijst de tijdelijke commissie er op dat de Europese Gemeenschap alleen kan optreden op terreinen waarop ze bevoegd is. In de richtlijnen betreffende de bescherming van gegevens, die op het EG-Verdrag (artikel 95) steunen, zijn de activiteiten ten behoeve van de Staatsveiligheid en strafrechtelijke vervolging uitgesloten. Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector gelden niet voor «verwerkingen» (artikel 3, lid 2, van richtlijn 95/46/EG) en «activiteiten» (artikel 1, lid 3, van richtlijn 97/66/EG) die verband houden met de openbare veiligheid, defensie, Staatsveiligheid en de activiteiten van de Staat op strafrechtelijk gebied.

Over de verenigbaarheid met het EU-recht wijst de tijdelijke commissie er op dat voor het gemeenschappelijk buitenlands en veiligheidsbeleid en voor de politiële en justitiële samenwerking in strafzaken geen richtlijnen bestaan die vergelijkbare bepalingen bevatten betreffende de bescherming van gegevens.

In de artikelen 6 en 7 van het Verdrag van de Europese Unie waarborgt de Unie de eerbiediging van de fundamentele rechten van het EVRM en de rechten die voorvloeien uit de gemeenschappelijke constitutionele traditie. Dit legt de Europese Unie de verplichting op deze rechten te eerbiedigen in haar wetgeving en bestuur. Omdat er op het niveau van de Unie nog niets is bepaald over de toelaatbaarheid van de bewaking van telecommunicatie ten behoeve van de veilig-

Face à la multiplication des dangers présentés par les nouvelles technologies de surveillance, la CEDH demeure l'instrument le plus efficace de protection des particuliers mais aussi des droits des États parties qui ont l'obligation de la respecter et de la faire respecter.

7.3. Compatibilité d'Echelon ou d'autres systèmes d'écoute des communications avec le droit communautaire

La Commission temporaire «système d'interception Echelon» du Parlement européen avait notamment pour mission d'examiner si un système d'écoute des communications du type Echelon est compatible avec le droit communautaire. Dans son rapport, la commission temporaire examine la question en deux étapes. Elle examine tout d'abord si l'existence d'un tel système d'espionnage est compatible avec le droit de l'Union et, ensuite, si le droit communautaire est violé en cas d'utilisation du système à des fins d'espionnage économique (91).

S'agissant de la compatibilité avec le droit européen, la commission temporaire souligne que la Communauté européenne ne peut intervenir que dans des domaines qui relèvent de sa compétence. Les directives relatives à la protection des données qui se fondent sur le Traité CE (article 95) excluent les activités nécessaires à la sûreté de l'État et aux poursuites pénales. La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ne s'appliquent pas aux «traitements» (article 3, alinéa 2, de la directive 95/46/CE) et aux «activités» (article 1er, alinéa 3, de la directive 97/66/CE) qui concernent la sécurité publique, la défense, la sûreté de l'État et les activités de l'État dans le domaine du droit pénal.

En ce qui concerne la compatibilité avec le droit de l'UE, la commission temporaire signale que pour la politique étrangère et de sécurité commune et pour la coopération policière et judiciaire en matière pénale, il n'existe aucune directive comportant des dispositions comparables relatives à la protection des données.

Aux articles 6 et 7 du Traité sur l'Union européenne, l'Union garantit le respect des droits fondamentaux définis dans la Convention européenne de protection des droits de l'homme et celui des droits qui découlent de la tradition constitutionnelle communautaire. Cela oblige l'Union européenne à respecter ces droits dans le cadre de sa législation et de son administration. Comme on n'a toujours rien prévu au niveau de l'Union concernant l'admissibilité

heids- of inlichtingendiensten is de schending evenwel nog niet aan de orde.

Als een lidstaat echter over een bewakingssysteem beschikt dat ook industriële spionage bedrijft of zijn grondgebied ter beschikking stelt van buitenlandse inlichtingendiensten impliceert dit echter zeker een schending van het EG-recht. Op grond van artikel 10 EG-Verdrag zijn de lidstaten immers tot volledige loyauteit verplicht en mogen ze geen maatregelen nemen die de doelstellingen van het verdrag in gevaar brengen.

De tijdelijke onderzoekscommissie besluit dat in de huidige stand van het Gemeenschapsrecht een bewakingssysteem als Echelon niet strijdig kan zijn met het recht van de Unie omdat dit recht geen raakpunten heeft die voor onverenigbaarheid noodzakelijk zijn.

Wordt het bewakingssysteem van zijn doel afgewend en voor economische spionage tegen buitenlandse ondernemingen gebruikt dan, aldus de commissie, is het wel strijdig met het Gemeenschapsrecht.

7.4. Juridische besluiten van de commissies

Gelet op de bevindingen van de deskundigen die de begeleidingscommissies hebben gehoord over de juridische aspecten van het Echelon-interceptiesysteem;

Gelet op de analyse van de tijdelijke commissie van het Europees Parlement over de verenigbaarheid van het interceptiesysteem Echelon met het geldende gemeenschapsrecht;

Komen de begeleidingscommissies tot de conclusie dat een interceptiesysteem dat, vanuit het buitenland, private telecommunicatie onderschept die via satelliet van en naar België komt (92):

A) strijdig is met het gemeenschapsrecht in de mate dat het voor economische spionage wordt gebruikt; deze schending geldt zowel voor de landen die zelf telecommunicaties onderscheppen als voor de landen die hun grondgebied ter beschikking stellen voor intercepties door derde landen;

• artikel 3 van de richtlijn 95/46/EG van 24 oktober 1995 met betrekking tot de bescherming van de fysieke personen ten opzichte van de verwerking van persoonsgegevens en van het vrije verkeer van deze gegevens sluit immers enkel de verwerking van persoonsgegevens van het toepassingsgebied uit die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat en de activiteiten van de Staat op strafrechtelijk gebied;

de la surveillance des télécommunications à l'usage des services de sécurité ou de renseignement, la question de la violation n'est toutefois pas encore à l'ordre du jour.

Néanmoins, si un État membre dispose d'un système de surveillance pratiquant aussi l'espionnage industriel ou met son territoire à la disposition de services de renseignements étrangers, il y a évidemment violation du droit européen. En vertu de l'article 10 du traité instituant la Communauté européenne, les États membres sont en effet tenus à une loyauté totale et ils ne peuvent pas prendre de mesures compromettant les objectifs du traité.

La commission temporaire conclut que, dans l'état actuel du droit communautaire, un système de surveillance comme Echelon ne peut pas être contraire au droit de l'Union, étant donné que ce droit ne présente aucun des points de tangence requis pour qu'il y ait incompatibilité.

La commission estime toutefois que le système de surveillance est contraire au droit communautaire s'il est détourné de son but et utilisé à des fins d'espionnage économique contre des entreprises étrangères.

7.4. Conclusions juridiques des commissions

Eu égard aux constatations des experts que les commissions de suivi ont entendus sur les aspects juridiques du système d'interception Echelon;

Eu égard à l'analyse de la commission temporaire du Parlement européen concernant la compatibilité du système d'interception Echelon avec le droit communautaire en vigueur;

Les commissions de suivi concluent que l'existence d'un système d'interception qui capte, à partir de l'étranger, des télécommunications privées relayées par satellite au départ et à destination de la Belgique (92):

A) est contraire au droit communautaire, dans la mesure où ce système est utilisé dans un but d'espionnage économique; la violation est le fait à la fois des pays qui interceptent eux-mêmes des télécommunications et des pays qui mettent leur territoire à la disposition de pays tiers pour qu'ils puissent se livrer à des interceptions de télécommunications;

• l'article 3 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données n'exclut de son champ d'application que le traitement de données à caractère personnel ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal;

• artikel 25 van deze richtlijn bepaalt dat de persoonsgegevens slechts naar een derde land mogen worden doorgegeven indien dat land een passend beschermingsniveau waarborgt, wat niet het geval is aangezien de Verenigde Staten enkel voor de eigen burgers en zij die legaal op het Amerikaans grondgebied verblijven in een bescherming voorziet;

• artikel 1.3 van de richtlijn 97/66/EG van 15 december 1997 met betrekking tot de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van de telecommunicatie voorziet enkel in een uitsluiting van het toepassingsgebied voor de activiteiten die verband houden met de openbare veiligheid, defensie, de veiligheid van de Staat en de activiteiten van de Staat op strafrechtelijk gebied; artikel 5.1 van deze richtlijn bepaalt het volgende: «De lidstaten garanderen in hun nationale reglementering het vertrouwelijk karakter van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers, indien de betrokken gebruikers daarmee niet hebben ingestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 14, lid 1» (93).

B) dat door economische spionage de verwezenlijking van de doelstellingen van het EG-Verdrag, namelijk het vrije verkeer van goederen, personen, diensten en kapitaal, in het gedrang brengt waardoor artikel 10 van het EG-Verdrag wordt geschonden dat de lidstaten de verplichting oplegt zich te onthouden van alle maatregelen welke de verwezenlijking van deze doelstellingen in gevaar kunnen brengen;

C) artikel 8.1 van het EVRM (94) schendt omdat deze interceptie van communicatie een ontoelaatbare aantasting impliceert van het privé-leven daar het niet beantwoordt aan de drie cumulatieve voorwaarden die door het Europees Hof voor de rechten van de mens worden opgelegd: wettelijkheid, legitimiteit en de noodzaak ervan in een democratische samenleving (95);

D) de nationale soevereiniteit van ons land schendt omdat ons land nooit de toelating heeft gegeven voor deze intercepties, en hiervan nooit officieel op de hoogte is gebracht.

Hoewel artikel 5 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens bepaalt dat een algemene interceptie niet proportioneel is in verhouding tot het gevolgde doel en artikel 3 van de wet van 30 juni 1994 tot bescherming van de persoonlijke levenssfeer tegen afluistering, kennisneming en opname van private communicaties en telecommunicaties een onderschepping slechts uitzonderlijk toelaat door de onderzoeksrechter, als er ern-

• l'article 25 de la même directive dispose que le transfert vers un pays tiers ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. Tel n'est pas le cas, puisque les États-Unis ne prévoient de protection que pour leurs propres citoyens et pour ceux qui résident légalement sur le territoire américain;

• l'article 1.3 de la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications n'exclut du champ d'application de la directive que les activités concernant la sécurité publique, la défense, la sûreté de l'État dans des domaines relevant du droit pénal; l'article 5.1 de la même directive dispose comme suit: «Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou des services de télécommunication accessibles au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, § 1er» (93).

B) menace la réalisation des buts du Traité CE, à savoir la libre circulation des marchandises, des personnes, des services et des capitaux, ce qui constitue une violation de l'article 10 du Traité CE qui impose aux États membres de s'abstenir de toute mesure susceptible de mettre en péril la réalisation de ces buts;

C) enfreint l'article 8.1 de la CEDH (94), parce que cette interception des communications constitue une violation inacceptable de la vie privée, du fait qu'elle ne satisfait pas aux trois conditions cumulatives qui sont imposées par la Cour européenne des droits de l'homme: légalité, légitimité et nécessité dans une société démocratique (95);

D) viole la souveraineté nationale de notre pays, étant donné que celui-ci n'a jamais autorisé ces interceptions et n'en a jamais été informé officiellement.

Bien que l'article 5 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel dispose qu'une interception généralisée n'est pas proportionnée au but poursuivi et que l'article 3 de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées n'autorise qu'à titre exceptionnel le juge d'instruction à intercepter les communications,

stige aanwijzingen bestaan van een misdrijf en als de andere onderzoeksmiddelen niet toelaten de waarheid te vinden, kunnen deze artikelen niet worden ingeroepen ingevolge het principe van de territoriale werking van de Belgische wet.

De door de heer Yernault aangehaalde motieven om te stellen dat de interne rechtsmiddelen niet dienen uitgeput te worden overeenkomstig artikel 35, § 1, EVRM overtuigen niet. Zo betekent het feit dat Duitsland bijvoorbeeld tot heden geen controle uitoefent op de activiteiten die zich afspelen in Bad Aibling niet dat een gerechtelijke uitspraak die in een dergelijke controle voorziet in rechte onmogelijk is. De verplichting de interne rechtsmiddelen uit te putten geldt inderdaad niet wanneer er sprake is van een consistente administratieve praktijk, dat wil zeggen van herhaalde handelingen die in strijd zijn met het EVRM en die door de verdragspartij in kwestie getolereerd worden (zie EHRM, Ierland t. Verenigd Koninkrijk, 18 januari 1978, § 159). Zolang echter de rechtbanken van de betrokken Staten zich niet over de in dit verslag besproken praktijken hebben kunnen uitspreken, kan niet beweerd worden dat de praktijken zondermeer getolereerd worden. Dat de House of Lords in een arrest van 20 juni 2000 beslist heeft dat de immuniteit van de Amerikaanse regering belet dat deze partij is in een sociaal geschil sluit een rechtsvordering tegen de Britse regering niet uit. Bovendien kunnen de Britse rechtbanken sinds de inwerkingtreding van de *Human Rights Act* 1998 overheidshandelingen rechtstreeks toetsen aan het EVRM.

De begeleidingscommissies besluiten dat er rechtsmiddelen om het bestaan en de activiteiten van het Echelon-systeem of andere gelijkaardige interceptiesystemen aan de rechterlijke toetsing voor te leggen waarbij, desgevallend, in laatste instantie het Europees Hof voor de rechten van de mens een uitspraak zal moeten doen.

8. BESLUITEN VAN DE BEGELEIDINGSCOMMISSIES

De opvolgingscommissies stellen vast:

1. dat verschillende Staten (in het bijzonder de grootmachten) beschikken over een globaal systeem voor het wereldwijd onderscheppen van satellietcommunicatie (COMINT);

2. dat een van deze systemen kadert in de samenwerking inzake SIGINT tussen de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland na de Tweede Wereldoorlog (het UKUSA-akkoord). Dit systeem voor het onderscheppen van informatie is bekend geworden onder de

s'il existe des indices sérieux d'infraction et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité, le principe selon lequel la loi belge n'a d'effet que sur le territoire du Royaume empêche d'invoquer ces articles.

Les motifs invoqués par M. Yernault pour affirmer qu'il n'est pas nécessaire d'épuiser les voies de recours internes conformément à l'article 35, § 1er, CEDH, ne sont pas convaincants. Ainsi, le fait que l'Allemagne — par exemple — n'a pas exercé à ce jour de contrôle sur les activités à Bad Aibling ne signifie pas qu'une décision judiciaire prévoyant un tel contrôle soit impossible. L'obligation d'épuiser les voies de recours internes ne s'applique effectivement pas lorsqu'il est question d'une pratique administrative conséquente, c'est-à-dire des actions répétées qui sont contraires à la CEDH et qui sont tolérées par la partie au traité en question (*cf.* CEDH, Irlande c. Royaume-Uni, 18 janvier 1978, § 159). Toutefois, tant que les tribunaux des États concernés n'auront pas eu la possibilité de se prononcer sur les pratiques examinées dans le présent rapport, on ne pourra pas affirmer qu'elles sont tolérées sans plus. Le fait que la Chambre des lords ait décidé, dans un arrêt du 20 juin 2000, que l'immunité du gouvernement américain ne permettait pas à celui-ci d'être partie à un conflit social, n'exclut pas la possibilité d'intenter une procédure judiciaire contre le gouvernement britannique. En outre, depuis l'entrée en vigueur du *Human Rights Act* de 1998, les tribunaux britanniques peuvent contrôller directement la conformité des actes de l'autorité britannique aux dispositions de la CEDH.

Les commissions du suivi concluent qu'il existe des voies de recours permettant de soumettre l'existence et les activités du système Echelon ou de systèmes d'interception similaires à un contrôle judiciaire, le cas échéant, la Cour européenne des droits de l'homme étant appelée à se prononcer sur la question en dernière instance.

8. CONCLUSIONS DES COMMISSIONS DE SUIVI

Les commissions de suivi constatent:

1. que plusieurs États (en particulier les grandes puissances) disposent d'un système d'interception global, à l'échelle mondiale, qui intercepte les communications par satellite (COMINT);

2. que l'un d'entre eux s'inscrit dans le cadre de la collaboration en matière de SIGINT qui unit les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande après la Deuxième Guerre mondiale (pacte UKUSA); ce système d'interception a été désigné par le vocable « Echelon » mais il n'est pas

naam «Echelon» maar draagt in de deelnemende landen niet noodzakelijk deze naam;

3. dat een aantal lidstaten van de Europese Unie beschikken over vergelijkbare globale interceptiesystemen, ook al hebben die niet allemaal dezelfde capaciteit als Echelon;

4. dat België niet over een dergelijk systeem beschikt en niet meewerkt aan een afluistersysteem van een of meerdere geallieerde landen;

5. dat de Belgische inlichtingendiensten niet bij machte zijn na te gaan of de Belgische regering, de overheidsdiensten, de bedrijven of de burgers worden afgeluisterd;

6. dat alleen de Belgische strijdmacht tegen deze praktijken wordt beschermd door de Algemene Dienst inlichting en veiligheid;

7. dat de Veiligheid van de Staat niet bij machte is de wettelijke opdracht te vervullen die zij krachtens artikel 7, 1º, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst heeft gekregen;

8. dat de globale Westerse interceptiesystemen ten tijde van de koude oorlog hebben bijgedragen tot de veiligheid van België en zijn bondgenoten;

9. dat deze globale interceptiesystemen onder meer dienen in de strijd tegen het internationale terrorisme en de internationale misdaad;

10. dat de begeleidingscommissies echter de indruk hebben dat deze globale interceptiesystemen eveneens gebruikt worden voor economische spionage;

11. dat deze systemen, die werken zonder het medeweten van de landen waarbinnen zij functioneren, onmiskenbaar de soevereiniteit van de Staat aantasten en dus het internationaal recht schenden en meer in het bijzonder, in de lidstaten van de Europese Unie, het gemeenschapsrecht;

12. dat deze systemen tevens in strijd zijn met de wettelijke bepalingen betreffende de bescherming van de persoonlijke levenssfeer — onder meer gewaarborgd door het Europees Verdrag van de rechten van de mens — en dat het bijgevolg mogelijk is hiertegen rechtsvervolging in te stellen;

13. dat de bestaande technologieën het ook voor misdaad- en terreurorganisaties mogelijk maken op grote schaal berichten te onderscheppen.

nécessairement désigné par ce vocable dans les pays participants;

3. que plusieurs pays membres de l'Union européenne disposent de systèmes d'interception globaux similaires, même s'ils ne disposent pas tous d'une capacité comparable à celle d'Echelon;

4. que la Belgique ne dispose pas d'un système équivalent et ne collabore pas à un système d'écoute mis au point par un ou plusieurs pays alliés;

5. que les services belges de renseignements ne sont pas en mesure de dépister et de repérer les écoutes dont le gouvernement, les services publics, les entreprises ou les citoyens belges feraient l'objet;

6. que seules les Forces armées belges font, à cet égard, l'objet d'une protection assurée par le Service général du renseignement et de la sécurité;

7. que la Sûreté de l'État n'est pas en mesure de remplir sa mission légale prévue à l'article 7, 1º, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

8. que les systèmes d'interception globaux occidentaux ont, au temps de la guerre froide, contribué à la sécurité de la Belgique et de ses alliés;

9. que ces systèmes d'interception globaux servent entre autres à la lutte contre le terrorisme international et contre la criminalité internationale;

10. qu'il apparaît cependant aux commissions de suivi que ces systèmes globaux d'interception servent également à des fins d'espionnage économique;

11. que ces systèmes, qui travaillent à l'insu des pays qui en sont la cible, constituent indiscutablement des atteintes à la souveraineté de l'État et qu'à ce titre, ils sont contraires au droit international et, plus particulièrement entre États membres de l'Union européenne, au droit communautaire;

12. que ces systèmes violent également les dispositions légales applicables à la protection de la vie privée des personnes garantie notamment par la Convention européenne des droits de l'homme et que des recours en justice sont dès lors possibles;

13. que les possibilités technologiques existantes permettent également aux organisations criminelles et terroristes d'intercepter des communications à grande échelle.

9. AANBEVELINGEN VAN DE BEGELEIDINGSCOMMISSIES

De begeleidingscommissies bevelen de regering aan:

1. de politieke en juridische problemen die deze wereldwijde afluistersystemen veroorzaken wanneer zij gebruikt worden door bondgenoten binnen de NAVO of door lidstaten van de EU, aan te kaarten tijdens de ministervergaderingen van deze twee organisaties waarvan België medeoprichter is;

2. het algemene voorzorgsprincipe toe te passen bij het uitstippelen van een wereldwijd en gecentraliseerd beleid ter beveiliging van de communicatie en de uitwisseling van gevoelige informatie;

3. aan de Veiligheid van de Staat en de Algemene Dienst inlichting en veiligheid van de Krijgsmacht de nodige technische en personeelsmiddelen te verschaffen om alle informatie in te winnen betreffende ieder gevaar van onderschepping van berichten ten nadele van België als bedoeld in artikel 7, 1º van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst;

4. indien nodig de wettelijke technieken aan te passen zodat het op een selectieve en streng gecontroleerde manier mogelijk wordt berichten op te sporen, af te luisteren en te onderscheppen;

5. te overwegen een dienst op te richten om de hele kwestie van de informatiebeveiliging op te lossen, alsook een elektronische bewakingspost die de regering op de hoogte kan stellen van iedere abnormale belangstelling voor gevoelige aangelegenheden;

6. elke vorm van spionage of afluisteren met een economisch oogmerk tussen de lidstaten van de Europese Unie te laten verbieden;

7. binnen de Europese Unie de oprichting te bepleiten van een Europese inlichtingendienst, met het oog op de bescherming van de vitale gemeenschappelijke belangen van de landen van de Europese Unie, in het bijzonder belast met de beveiliging van de informaticasystemen en de verdediging van de gemeenschappelijke eigen belangen van de Lidstaten tegen uitwendige bedreigingen en dat als aanvulling en in nauwe samenwerking met de nationale inlichtingendiensten;

8. van de andere EU-lidstaten de geleidelijke totstandkoming te eisen van Europese regels voor de uitwisseling van informatie tussen de inlichtingendiensten om zo het systeem van bilaterale uitwisseling af te schaffen dat niet is aangepast aan de strijd tegen het terrorisme en de georganiseerde misdaad;

9. te eisen dat de resultaten worden meegedeeld van de gesprekken die zijn opgenomen in installaties

9. RECOMMANDATIONS DES COMMISSIONS DE SUIVI

Les commissions de suivi recommandent au gouvernement:

1. de poser les questions politiques et juridiques que soulèvent ces écoutes globales lorsqu'elles sont réalisées par des États alliés au sein de l'OTAN ou par des États membres au sein de l'Union européenne dans le cadre des réunions ministérielles de ces deux organisations dont la Belgique est membre fondateur;

2. de mettre en œuvre le principe général de précaution dans l'élaboration d'une politique globale et centralisée de sécurisation des communications et de la circulation des informations sensibles;

3. de donner à la Sûreté de l'État et au Service général du renseignement et de la sécurité des Forces armées les moyens techniques et humains nécessaires en vue de recueillir toute information sur toutes menaces d'interception de communications dirigées contre la Belgique au sens de l'article 7, 1º, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

4. d'adapter, si nécessaire, les moyens légaux techniques des services de renseignements afin qu'ils puissent procéder de manière sélective et strictement contrôlée à des repérages, à des écoutes et à des interceptions;

5. d'envisager la mise en place d'un service chargé d'apporter une solution à l'ensemble de la question de la sécurisation de l'information et à la mise sur pied d'un service de veille électronique capable d'alerter le gouvernement de tout intérêt anormal pour des matières sensibles;

6. de faire interdire, entre États de l'Union européenne, tout type d'espionnage ou d'écoutes à des fins économiques;

7. de plaider, au sein de l'Union européenne, en faveur de la création d'un service de renseignement européen, en vue de protéger les intérêts vitaux communs des pays de l'Union européenne chargé en particulier de la sécurisation des systèmes d'information et de la défense des intérêts communs propres aux États de l'Union contre les menaces extérieures, et cela complémentaire et travaillant en étroite collaboration avec les services de renseignements nationaux;

8. d'exiger de nos partenaires au sein de l'Union européenne l'élaboration progressive de règles européennes d'échanges d'informations entre les services de renseignements et d'abolir ainsi entre ceux-ci le système de troc inadapté à la lutte contre le terrorisme et la criminalité organisée;

9. d'exiger la communication des résultats des écoutes enregistrées dans des installations situées

die gevestigd zijn in een land van de Europese Unie en die over Belgische gegevens beschikken en de voorwaarden te verwezenlijken om te verzekeren dat de Belgische overheid toegang krijgt tot die installaties.

De begeleidingscommissies bevelen het federale Parlement aan:

— een eerste ontmoeting te organiseren met de parlementaire organen die in de verschillende landen van de Europese Unie de inlichtingendiensten controleren, voor zover die bestaan, en daarover verslag uit te brengen bij de landen van de Europese Unie die nog niet over dergelijke organen beschikken. Die ontmoeting zou het resultaat van de parlementaire onderzoeken naar het Echelon-systeem kunnen behandelen en kan bijdragen tot de bewustwording van de noodzaak van Europese samenwerking inzake inlichtingenactiviteiten en tot de noodzaak van de parlementaire controle daarop;

— het Europees Parlement bij deze oefening te betrekken.

Dit verslag werd eenparig goedgekeurd door beide commissies.

De rapporteurs, *De voorzitters,*

Anne-Marie LIZIN. Armand DE DECKER.
Tony VAN PARIJS. Herman DE CROO.

dans un pays de l'Union européenne et disposant de données belges et de créer les conditions pour assurer l'accès à ces installations par les autorités belges.

Les commissions de suivi recommandent au Parlement fédéral:

— d'organiser une première rencontre des organes parlementaires de contrôle des services de renseignements des pays de l'Union européenne qui en disposent et d'en faire part aux pays de l'Union européenne qui n'en disposent pas encore. Cette rencontre porterait sur le résultat des enquêtes parlementaires consacrées au système Échelon, et pourrait susciter une prise de conscience relative à la nécessaire collaboration européenne en matière de renseignement ainsi que sur la nécessité du contrôle parlementaire;

— d'associer le Parlement européen à cet exercice.

Le présent rapport a été approuvé à l'unanimité par les deux commissions.

Les rapporteurs, *Les présidents,*

Anne-Marie LIZIN. Armand DE DECKER.
Tony VAN PARIJS. Herman DE CROO.

NOTEN:

(1) Van onder meer de heren Delathouwer, Deleuze, Leterme.

(2) Scientific and Technological Options Assessment: de STOA is een intern orgaan van het Europees Parlement dat de impact onderzoekt van wetenschappelijke en technologische ontwikkelingen op de samenleving, de economie of het milieu; voor haar onderzoeken doet het beroep op externe, onafhankelijke deskundigen; het STOA-panel draagt de politieke verantwoordelijkheid voor het werk van STOA en is samengesteld uit leden van het Europees Parlement.

(3) Activiteitenverslag 1999 van het Comité I, blz. 45.

(4) Activiteitenverslag 1999 van het Comité I, blz. 46.

(5) Zie het hoofdstuk 2.1.

(6) Activiteitenverslag 2000 van het Comité I, blz. 29-61.

(7) Activiteitenverslag 2000 van het Comité I, blz. 62-68.

(8) Activiteitenverslag 2000 van het Comité I, blz. 57-58.

(9) Werkdocument voor het STOA-panel, december 1999, PE 168.184.

(10) Activiteitenverslag 1999 van het Comité I, blz. 24-49.

(11) Verslag van de heren Hordies en de Donnéa, stuk Senaat, nr. 2-332/1, stuk Kamer nr. 50/430.

(12) «Een tweede spreker deelt de bezorgdheid van de vorige spreker over «Echelon». Indien het zin heeft ervoor te zorgen dat het privé-leven en onze democratie gerespecteerd worden, moet men zich afvragen — gesteld dat het «Echelon» -systeem werkelijk bestaat — wat men nog reëel kan controleren en beschermen.» Verslag vermeld in noot 11.

(13) *Development of surveillance technology and risk of abuse of economic information, The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception, Part C, Technical File*, ix-xii, Nikos Bogolikos, oktober 1999, PE 168 184 /Vol. 5/5.

(14) Verslag van de heer Hordies en mevrouw Salandra-Pelzer, stuk Senaat, nr. 2-531/1, stuk Kamer, nr. 50/813.

(15) Verslag nr. 2623 «Echelon: mythe ou réalité. Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale», 11 oktober 2000.

(16) Surveillance technology can be defined as devices or systems which can monitor, track and assess the movements of individuals, their property and other assets. (PE 166 499/Int. St./ Exec. Sum./en).

(17) De oorspronkelijke werken van journalisten als Duncan Campbell («*The Unsinkable Aircraft Carrier*», Michael Joseph Limited, London, 1984) en Nicky Hager («*Secret Power. New Zealand's role in the International Spy Network*», Craig Potton Publishing, Nelson, New Zealand, 1996) of van ex-agenten als Mike Frost («*Spyworld*», Doubleday, Toronto, 1994) zijn nog nauwelijks in de handel te vinden. Van het oorspronkelijke STOA-rapport van 1997 dat handelt over de «Technology of political control» wordt meestal enkel de «Executive Summary» (PE 166 499/Int.St./Exec.Sum.) gebruikt.

(18) Department of Defense Directive S-5100.20, The National Security Agency and the Central Security Service, 23 december 1971 (dit en vele andere op basis van de «Freedom of Information Act» door de Amerikaanse overheid vrijgegeven documenten kunnen worden gevonden op de website van de George Washington University, Washington D.C., waarop professor Jeffrey Richelson een «National Security Archive» heeft aangelegd).

NOTES:

(1) Notamment par MM. Delathouwer, Deleuze et Leterme.

(2) Évaluation des choix scientifiques et techniques: le STOA est un organe interne du Parlement européen qui examine l'incidence des évolutions scientifiques et technologiques sur la société, l'économie ou l'environnement; il confie ses travaux de recherche à des experts extérieurs et indépendants; le Groupe du STOA est responsable politiquement du travail du STOA et est composé de membres du Parlement européen.

(3) Rapport annuel 1999 du Comité R, p. 41.

(4) Rapport annuel 1999 du Comité R, p. 43.

(5) Voir le chapitre 2.1.

(6) Rapport d'activités 2000 du Comité R, pp. 29-61.

(7) Rapport d'activités 2000 du Comité R, pp. 62-68.

(8) Rapport d'activités 2000 du Comité R, pp. 57-58.

(9) Document de travail du groupe du STOA, décembre 1999, PE 168.184.

(10) Rapport annuel 1999 du Comité R, pp. 23-46.

(11) Rapport de MM. Hordies et de Donnéa, doc. Sénat, nº 2-332/1, doc. Chambre, nº 50/430.

(12) «Un deuxième intervenant partage l'inquiétude du préopinant par rapport à «Echelon». S'il y a un sens de veiller au respect de la vie privée et de notre État démocratique, il faut se demander si le système «Echelon» existe et ce qu'on peut encore effectivement contrôler et protéger.» Rapport mentionné à la note 11.

(13) *Development of surveillance technology and risk of abuse of economic information. The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception, Part C, Technical File*, ix-xii, Nikos Bogolikos, octobre 1999, PE 168.184/Vol. 5/5.

(14) Rapport de M. Hordies et Mme Salandra-Pelzer, doc. Sénat, nº 2-531/1, doc. Chambre, nº 50/813.

(15) Rapport nº 2623 «Echelon: mythe ou réalité. Rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale», 11 octobre 2000.

(16) Surveillance technology can be defined as devices or systems which can monitor, track and assess the movements of individuals, their property and other assets. (PE 166 499/Int. St./ Exec. Sum./en).

(17) Les travaux initiaux de journalistes comme Duncan Campbell («*The Unsinkable Aircraft Carrier*», Michael Joseph Limited, London, 1984) et Nicky Hager («*Secret Power New Zealand's role in the International Spy Network*», Craig Potton Publishing, Nelson, New Zealand, 1996) ou d'anciens agents tels que Mike Frost («*Spyworld*», Doubleday, Toronto, 1994) sont aujourd'hui très difficiles à trouver dans le commerce. En ce qui concerne le rapport STOA original de 1997 qui traite de la «Technology of political control», généralement seul le «Executive Summary» (PE 166 499/Int. St./Exec. Sum.) est exploité.

(18) *Department of Defense Directive S-5100.20, The National Security Agency and the Central Security Service*, 23 décembre 1971 (ce texte et de nombreux autres documents publiés par les autorités américaines en vertu du «*Freedom of Information Act*» peuvent être consultés sur le site Web de la *George Washington University, Washington D.C.*, où le professeur Jeffrey Richelson a constitué une «*National Security Archive*»).

(19) Zie bijlage 1.

(20) COMINT is the technical and intelligence information derived from foreign communications by other than the intented recipients. COMINT is produced by the collection and processing of foreign communications by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direct finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.

(21) Beide diensten hebben bijvoorbeeld richtlijn 18 uitgewerkt die dateert van 27 juli 1993: United States Signals Intelligence Directive 18: «Legal compliance and minimization procedures».

(22) 1. GCHQ The Government Communications Headquarters.

3.-(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be-

a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and

b) to provide advice and assistance about-

(i) languages, including terminology used for technical matters, and

(ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

Artikel 3 van de Intelligence Services Act van 1994.

(23) Nicky Hager, *o.c.*, blz. 20 en 22.

(24) Dit hoofdstuk is grotendeels gebaseerd op vol. 2/5 van het STOA-document (PE 168 184) *«Interception Capabilities 2000»* dat door Duncan Campbell werd opgesteld.

(25) Verslag over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (Echelon-interceptiesysteem), blz. 30-46, 11 juli 2001, Tijdelijke Commissie Echelon-interceptiesysteem, PE 305 391.

(26) Nicky Hager, *oc*, blz. 61.

(27) Alhoewel het bestaan van het UKUSA-agreement door geen van de betrokken hoofdrolspelers officieel wordt erkend zijn de begeleidingscommissies tot het besluit gekomen dat er over het bestaan van dit akkoord geen enkele twijfel kan bestaan. De begeleidingscommissies doen dit op grond van al de gegevens die in de verschillende verslagen van het het Europees Parlement en het Comité I ten overvloede zijn aangehaald. Een voorbeeld volstaat: in zijn jaarverslag 1999-2000 stelt het Britse «Intelligence and Security Committee», een parlementair toezichtsorgaan dat op grond van de Intelligence Services Act 1994 is opgericht het volgende over GCHQ «The quality of intelligence gathered clearly reflects the value of the close cooperation 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». Na een dergelijke overduidelijke en blijkbaar opzettelijke verwijzing naar het akkoord en de voornaamste betrokken partner hoeft dit punt alvast niet nodeloos verder te worden uitgespit.

(19) Voir l'annexe 1.

(20) *COMINT is the technical and intelligence information derived from foreign communications by other than the intented recipients. COMINT is produced by the collection and processing of foreign communications by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direct finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.*

(21) Par exemple, les deux services ont appliqué la directive 18 du 27 juillet 1993: *United States Signals Intelligence Directive 18: «Legal compliance and minimization procedures».*

(22) *1. GCHQ The Government Communications Headquarters.*

3.-(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be-

a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and

b) to provide advice and assistance about-

(i) languages, including terminology used for technical matters, and

(ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

Article 3 de Intelligence Services Act du 1994.

(23) Nicky Hager, *o.c.*, pp. 20 et 22.

(24) Le présent chapitre est basé en grande partie sur le vol. 2/5 du document STOA intitulé *«Interception Capabilities 2000»* (PE 168.184) de Duncan Campbell.

(25) Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon), pp. 30-46, 11 juillet 2001, Commission temporaire sur le système d'interception Echelon, PE 305 391.

(26) Nicky Hager, *oc*, p. 61.

(27) Bien que l'existence du Pacte UKUSA n'ait été reconnue officiellement par aucun des acteurs principaux concernés, les commissions du suivi sont arrivées à la conclusion qu'il ne saurait y avoir le moindre doute sur l'existence de ce pacte. Les commissions du suivi se basent sur toutes les données citées à profusion dans les différents rapports du Parlement européen et du Comité R. Un exemple suffira: dans son rapport annuel 1999-2000, l'«*Intelligence and Security Committee*» britannique, un organe parlementaire de contrôle créé sur la base de l'Intelligence Services Act 1994, parle des GCHQ en ces termes: «*The quality of intelligence gathered clearly reflects the value of the close cooperation 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*». Après une référence aussi manifeste et clairement intentionnelle au pacte et au principal partenaire concerné, le point ne doit plus être approfondi inutilement.

(28) «Canada collaborates with some of its closest and long-standing allies in the exchange of foreign intelligence ... These countries and the responsible agencies in each are the US (National Security Agency), the UK (Government Communications Headquarters), Australia (Defence Signals Directorate), and New Zealand ...», Canadian Parliamentary Security and Intelligence committee, Report, May 1995.

(29) Zie hiervoor de documenten die kunnen worden geconsulteerd in het National Security Archive (http:www.gwu.edu/~nsarchiv).

(30) In de Verenigde Staten door het «House Select Committee on Intelligence Services»; het «Intelligence and Security Committee» in het Verenigd Koninkrijk.

(31) Zie: http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(32) Bijvoorbeeld de «pod» tentoongesteld in het museum van de voormalige KGB die door Amerikaanse onderzeeërs werden geplaatst op onderzeese communicatiekabels. Zie de uitgebreide beschrijving in Vol 2/5 van het STOA-document (PE 168 184) «Interception Capabilities 2000 dat door Duncan Campbell werd opgesteld en de hoofdstukken 9 tot 11 in «Secret Power» van Nicky Hager.

(33) *lnterception capabilities — Impact and exploitation, Paper 1 Echelon and its role in COMINT*, tekst voorgesteld door Duncan Campbell aan de tijdelijke Commissie Echelon-interceptiesysteem, 22-23 januari 2001.

(34) Inlichtingen worden immers ook ingewonnen door het aftappen van kabels, het opvangen van radiosignalen of door satellieten die communicaties op de grond onderscheppen.

(35) NAVSECGRU Instruction C5450.48.8 van 3 september 1991; dit document is gedeeltelijk vrijgegeven ingevolge de «*Freedom of Information Act*» en is terug te vinden op het *National Security Archive* van de George Washington universiteit (Washington); elk document is van commentaar voorzien door Jeffrey Richelson of Michael Evans (zie bijlage 2).

(36) James Bamford, «*The Puzzle Palace*», *o.c.*

(37) In de, gecensureerde, tekst wordt onder de hoofding «*Activation of Echelon Units*». onder meer het volgende vermeld: «*... Headquarters AIA, Naval Security Group (NSG), and the National Security Agency (NSA) drafted agreements to increase AIA participation in the growing ... mission ... To accomplish this mission expansion, HQ AIA/XRXU was tasked to establish AIA units at ... bases (Detachment 2 and Detachment 3 of Headquarters 544th Intelligence Group ... These detachments had a projected activation date of 1 January 1995*».

(38) http://www.af.mil/news/factsheets/Air_Intelligence_Agency.html.

(39) http://www.aia.af.mil/common/homepages/pa/cyberspokesman/jan/atc7.htm#DET3.

(40) Vol. 2/5 van het STOA-document (PE 168.184).

(41) *Interception capabilities — lmpact and exploitation, Paper 1 Echelon and its role in COMINT*, 22-23 januari 2001.

(42) Nicky Hager, *o.c.*

(43) James Bamford, *o.c.*

(44) *Desperately seeking signals*, Jeffrey Richelson in «*The Bulletin of the Atomic Scientists*», http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html.

(45) NSA directeur Bobby Inman geciteerd door Richelson: «I have wasted more US taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career.»

(28) *Canada collaborates with some of its closest and long-standing allies in the exchange of foreign intelligence ... These countries and the responsible agencies in each are the US (National Security Agency), the UK (Government Communications Headquarters), Australia (Defence Signals Directorate), and New Zealand ..., Canadian Parliamentary Security and Intelligence committee, Report, May 1995.*

(29) Voir à ce sujet les documents qui peuvent être consultés au *National Security Archive* (http:www.gwu.edu/~nsarchiv).

(30) Aux États-Unis, par le «*House Select Committee on Intelligence Services*» et au Royaume-Uni par l'«*Intelligence and Security Committee*».

(31) Voir: http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(32) Par exemple le «pod» exposé au musée de l'ancien KGB, qui était placé par les sous-marins américains sur les câbles de communications sous-marins. Voir la description détaillée dans le Vol 2/5 du document STOA (PE 168 184) «*Interception Capabilities 2000*», qui a été rédigé par Duncan Campbell ainsi que les chapitres 9 à 11 de «*Secret Power*» de Nicky Hager.

(33) *lnterception capabilities — Impact and exploitation, Paper 1 Echelon and its role in COMINT*, texte présenté par Duncan Campbell à la Commission temporaire du système d'interception Echelon, 22-23 janvier 2001.

(34) En effet, on collecte également des renseignements par la captation des communications par câble, par l'interception des signaux radio ou par l'interception à l'aide de satellites des communications au sol.

(35) NAVSECGRU Instruction C5450.48.8 du 3 septembre 1991; une partie de ce document a été rendue publique par suite du «*Freedom of Information Act*» et elle peut être consultée dans la *National Security Archive* de l'université George Washington (Washington); chaque document est accompagné d'un commentaire de Jeffrey Richelson ou Michael Evans (voir annexe 2).

(36) James Bamford, «*The puzzle palace*», *o.c.*

(37) Dans le texte — censuré — du chapitre «*Activation of Echelon Units*», on lit entre autres ce qui suit: «*... Headquarters AIA, Naval Security Group (NSG), and the National Security Agency (NSA) drafted agreements to increase AIA participation in the growing ... mission ... To accomplish this mission expansion, HQ AIA/XRXU was tasked to establish AIA units at ... bases (Detachment 2 and Detachment 3 of Headquarters 544th Intelligence Group ... These detachments had a projected activation date of 1 January 1992.*»

(38) http://www.af.mil/news/factsheets/Air_Intelligence_Agency.html.

(39) http://www.af.mil/common/homepages/pa/cyberspokesman/jan/atc7.htm#DET3.

(40) Vol. 2/5 du document STOA (PE 168.184).

(41) *Interception capabilities — Impact and exploitation, Paper 1 Echelon and its role in COMINT*, 22-23 janvier 2001.

(42) Nicky Hager, *o.c.*

(43) James Bamford, *o.c.*

(44) *Desperately seeking signals*, Jeffrey Richelson dans «*The Bulletin of the Atomic Scientists*», http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html.

(45) Propos de Bobby, directeur de la NSA, cités par Richelson: «*I have wasted more US taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career.*»

(46) John Mills, directeur van de staf van het *House Permanent Select Committee on Intelligence*, op 5 oktober 1998, als geciteerd door Richelson: «Signals intelligence is in a crisis ... In the past four or five years technology has moved from being the friend to being the enemy of SIGINT.»

(47) *Intelligence Services Act*, 1994, artikel 1 luidt als volgt:
The Secret Intelligence Service

1.-(1) There shall continue to be a Secret Intelligence Service (in this Act referred to as «the Intelligence Service» under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be — :

a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

b) to perform other tasks relating to the actions or intentions of such persons.

(2) The functions of the Intelligence Service shall be exercisable only:

a) in the interests of national security, with particular reference to the defence and foreign politices of Her Majesty's Government in the United Kingdom; or

b) in the interests of the economic well-being of the United Kingdom; or

c) in support of the prevention or detection of serious crime.

(48) *Intelligence Services Act*, artikel 3(2), luidt als volgt:
(2) The functions referred to in subsection (1) *a)* above shall be exercisable only — :

a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

b) in the interests of the economisc well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

c) in support of the prevention or detection of serious crime.

(49) Verklaring van Georges Tenet op 12 april 2000: *«As you know, signals intelligence is one of the pillars of US intelligence. Along with our other intelligence collection activities, we rely on SIGINT to collect information about the capabilities and intentions of foreign powers, organizations, and persons to support the foreign policy and other national interests of the United States»;* te vinden op http://www.fas.org/irp/congress/2000_hr/tenet/html.

(50) «With respect to allegations of industrial espionage, the notion that we collect intelligence to promote American business interests is simply wrong. We do no to target foreign companies to support American business interests.

First, our business is to gather information vital to the national defense and foreign policy of the US. Other departments and agencies in the US have the responsibility to assist US business interests. Our valuable resources are directed elsewhere.

Second, if we are to maintain good relations with our allies, they have to know they can trust us not to become involved in missions that are not directly related to national security. That is important for us, and it is important to them as they justify their cooperation with us to their own people.

Third, if we did this, where would we draw the line? Which companies would we help? Corporate giants? The little guy? All of them? I think we quickly would get into a mess and would raise questions of whether we are being unfair to one or more of our own businesses.

Of course, SIGINT does provide economic information that is useful to the United States Government. It can provide insight into global economic conditions and trends and assist policy-

(46) John Mills, directeur de l'administration du *House Permanent Select Committee on Intelligence*, le 5 octobre 1998, propos cités par Richelson: «*Signals intelligence is in a crisis ... In the past four or five years technology has moved from being the friend to being the enemy of SIGINT.*»

(47) L'article premier de l'*Intelligence Services Act*, 1994, est rédigé comme suit:

The Secret Intelligence Service

1.-(1) There shall continue to be a Secret Intelligence Service (in this Act referred to as «the Intelligence Service» under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be — :

a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

b) to perform other tasks relating to the actions or intentions of such persons.

(2) The functions of the Intelligence Service shall be exercisable only:

a) in the interests of national security, with particular reference to the defence and foreign politices of Her Majesty's Government in the United Kingdom; or

b) in the interests of the economic well-being of the United Kingdom; or

c) in support of the prevention or detection of serious crime.

(48) L'article 3(2) de l'*Intelligence Services Act* est rédigé comme suit:

(2) *The functions referred to in subsection (1) a) above shall be exercisable only — :*

a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

b) in the interests of the economisc well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

c) in support of the prevention or detection of serious crime.

(49) Déclaration de Georges Tenet du 12 avril 2000: *«As you know, signals intelligence is one of the pillars of US intelligence. Along with our other intelligence collection activities, we rely on SIGINT to collect information about the capabilities and intentions of foreign powers, organizations, and persons to support the foreign policy and other national interests of the United States»; à retrouver sur* http://www.fas.org/irp/congress/2000_hr/tenet/html.

(50) «*With respect to allegations of industrial espionage, the notion that we collect intelligence to promote American business interests is simply wrong. We do no to target foreign companies to support American business interests.*

First, our business is to gather information vital to the national defense and foreign policy of the US. Other departments and agencies in the US have the responsibility to assist US business interests. Our valuable resources are directed elsewhere.

Second, if we are to maintain good relations with our allies, they have to know they can trust us not to become involved in missions that are not directly related to national security. That is important for us, and it is important to them as they justify their cooperation with us to their own people.

Third, if we did this, where would we draw the line? Which companies would we help? Corporate giants? The little guy? All of them? I think we quickly would get into a mess and would raise questions of whether we are being unfair to one or more of our own businesses.

Of course, SIGINT does provide economic information that is useful to the United States Government. It can provide insight into global economic conditions and trends and assist policyma-

makers in dealing with economic crises. On many occasions, it has provided information about the intentions of foreign businesses, some operated by governments, to violate US laws or sanctions or to deny US businesses a level playing field. When such information arises, it is provided to the Treasury Department, the Commerce Department, or other government agencies responsible for enforcing US laws. The ...

(51) Over de ontwikkeling van het Amerikaans beleid inzake economische spionage wordt verwezen naar *Paper 2 COMINT impact on international trade* van Duncan Campbell van de nota *Interception Capabilities — Impact and Exploitation* die op 22-23 januari 2001 werd voorgesteld aan tijdelijke commissie van het Europees parlement.

(52) Onder de hoofding «*levelling the playing field around the world*» zijn de opdrachten en de richtlijnen voor een beroep op de diensten van het Advocacy Center omschreven door het *Trade Promotion Coordinating Committee* in een nota die dateert van oktober 1996; deze nota is als bijlage opgenomen in de in noot 51 vermelde studie van Duncan Campbell.

(53) http://www.ita.doc.gov/AdvFrameset.html

(54) *«Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information. Clyde Robinson suggested that Commerce devise a matrix by late this week which identifies the key information for each project on the interagency list. The group agreed that the matrix should be for Official Use Only»;* minuten van de vergadering van 17 augustus 1994 gevoegd bij een brief van het *Departement of Commerce* met als onderwerp *TPCC Indonesia Advocacy-Finance Working Group*.

(55) Peter Waldeman and Jay Solomon, *«Power deal with cuts for the first family»,* «Wall Street Journal», 23 december 1998.

(56) Duncan Campbell, *o.c.*; punt 74.

(57) Michael S. Serill, *«Hello, how to bride?», «Time»,* 11 december 1995; Tom Squitieri, *«Raytheon hopes 3-year trek to $1.4 Brazil deal near end — satellite system on hold», «USA Today»,* 19 mei 1997.

(58) Zie hierover de parlementaire vragen die in het Britse *House of Commons* zijn gesteld over Menwith Hill: ook de Britse parlementairen krijgen geen enkele verklaring over de activiteiten die daar door Amerikaanse legereenheden worden uitgeoefend, zelfs de afspraken die tussen de Amerikaanse en Britse regering zijn gemaakt worden niet meegedeeld; in een vraag aan de *Minister of State of the Armed Forces* zegt kamerlid Bob Creyer hierover het volgende:

«To suggest, as the Minister has, that there is parliamentary accountability for that spy station in the Yorkshire hills is to torture the truth. Its establishment has been accompanied by lies, evasion, deceit and a persistent refusal by Ministers to provide proper information to elected representatives in this so-called mother of Parliaments. Indeed, the Minister of State for the Armed Forces has refused to allow Labour Members around the base. That is a curious change because in 1981 the former Secretary of State for Defence, Francis Pym, gave me permission to visit the base. The only qualification to that permission was a refusal to allow Duncan Campbell to accompany me because he knew something about the spying and procedures going on inside the base.

Parliamentary accountability is virtually non-existent. There is little point in asking questions when answers are refused. On 27 April 1988, I asked the Secretary of State for Defence:

«If he will list the agreements authorising the use of Menwith Hill communications base, Harrogate, by the United States National Security Agency.»

Mr. Ian Stewart replied:

«The use of Menwith Hill by the United States Department of Defence is subject to confidential arrangements between the

kers in dealing with economic crises. On many occasions, it has provided information about the intentions of foreign businesses, some operated by governments, to violate US laws or sanctions or to deny US businesses a level playing field. When such information arises, it is provided to the Treasury Departement, the Commerce Department, or other government agencies responsible for enforcing US laws. The ...

(51) Sur l''évolution de la politique américaine en matière d'espionnage économique, voir *Paper 2 COMINT impact on international trade*, de Duncan Campbell, dans la note *Interception Capabilities — Impact and Exploitation* qui a été présentée les 22 et 23 janvier 2001 à la commission temporaire du Parlement européen.

(52) Le *Trade Promotion Coordinating Committee* a défini les missions de l'*Advocacy Center* et les directives à suivre pour faire appel à ses services dans une note intitulée *«levelling the playing field around the world»* d'octobre 1996; cette note figure en annexe à l'étude de Duncan Campbell mentionnée dans la note nº 51.

(53) http://www.ita.doc.gov/AdvFrameset.html

(54) *«Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information. Clyde Robinson suggested that Commerce devise a matrix by late this week which identifies the key information for each project on the interagency list. The group agreed that the matrix should be for Official Use Only»;* procès-verbal de la réunion du 17 août 1994 joint à une lettre du département de Commerce relative au *TPCC Indonesia Advocacy-Finance Working Group*.

(55) Peter Waldeman and Jay Solomon, *«Power deal with cuts for the first family»,* «Wall Street Journal», 23 décembre 1998.

(56) Duncan Campbell, *o.c.*; point 74.

(57) Michael S. Serill, *«Hello, how to bride?», «Time»,* 11 décembre 1995; Tom Squitieri, *«Raytheon hopes 3-year trek to $1.4 Brazil deal near end — satellite system on hold», «USA Today»,* 19 mai 1997.

(58) Voir à ce sujet les questions parlementaires qui ont été posées à la Chambre des Communes britannique sur Menwith Hill: les parlementaires britanniques n'ont eux non plus obtenu aucune explication sur les activités qui y sont exercées par les unités de l'armée américaine, même les accords passés entre le gouvernement américain et le gouvernement britannique ne sont pas communiqués; dans une question au ministre de la Défense, le député Bob Creyer a déclaré ce qui suit:

«To suggest, as the Minister has, that there is parliamentary accountability for that spy station in the Yorkshire hills is to torture the truth. Its establishment has been accompanied by lies, evasion, deceit and a persistent refusal by Ministers to provide proper information to elected representatives in this so-called mother of Parliaments. Indeed, the Minister of State for the Armed Forces has refused to allow Labour Members around the base. That is a curious change because in 1981 the former Secretary of State for Defence, Francis Pym, gave me permission to visit the base. The only qualification to that permission was a refusal to allow Duncan Campbell to accompany me because he knew something about the spying and procedures going on inside the base.

Parliamentary accountability is virtually non-existent. There is little point in asking questions when answers are refused. On 27 April 1988, I asked the Secretary of State for Defence:

«If he will list the agreements authorising the use of Menwith Hill communications base, Harrogate, by the United States National Security Agency.»

Mr. Ian Stewart replied:

«The use of Menwith Hill by the United States Department of Defence is subject to confidential arrangements between the

United Kingdom and United States Government.» — [Official Report, 27 April 1988; Vol. 132, c. 203.]

...

In other words, elected Members of Parliament are denied information on the appropriation of more than 200 acres of land by the United States Government, who now run a spy station in the heart of our country which is linked up to a global network. That is inexcusable. If there is parliamentary accountability, the moon is made of green cheese.»; http://www.parliament.the-stationery-office.co.uk/pa/cm199394/cmhansrd/1994-03-25/Debate-6.html.

(59) In dezelfde interventie zegt Bob Creyer hierover het volgende: *«Menwith Hill is a spy station — a sophisticated version of the man in the dirty raincoat looking through a bedroom window or the pervert spying through a lavatory keyhole. Those who defend the station's invasion of our land, which has never been approved by Parliament, are no better. There is no glory or wonderful purpose involved in Menwith Hill. That is all the more true now that he cold war is over. Ministers justified the Menwith Hill base by saying it was part of the cold war, but we understand that that has finished. What is their justification for the spy station now?*

Yorkshire land has been taken from us to provide an eavesdropping centre that is virtually free from urban, electro-magnetic interference. That is why the station is sited at its current location. The station is part of a chain of such stations that span the globe. Their aim is to assert and retain United States supremacy. For example, exactly opposite to Menwith Hill, on the other side of the globe in a prohibited region in Australia stands the twin of Menwith Hill, Pine Gap station. When Menwith Hill opened, the United States air force security service listening post at Kirknewton near Edinburgh ceased operations and a former employee is quoted on page 210 of «Puzzle Palace» as saying:

«I had to keep a special watch for commercial traffic, details of commodities, what big companies were selling, like iron and steel and gas. Changes were frequent. One week I was asked to scan all traffic between Berlin and London and another week between Rome and Belgrade. Some weeks the list of words to watch for contained dozens of names of big companies. Some weeks I just had to look for commodities. All traffic» — interception material — was sent back to Fort Meade in Washington.»

Menwith Hill took over those functions and continued to pursue military eavesdropping.

Its spying grows. The cold war has ended, but the radomes number 21 after recent expansion. About 1,200 staff, who are mainly American, are employed there — the number has grown from 400 in 1980. United States staff are ordered never to mention the National Security Agency of America and to report all outside contacts with foreign nationals — the British people who live in the region — to ensure that supervision of such contacts is maintained.

...

There are two large United States firms within the military-industrial complex: Loral Space Systems Incorporated, formerly a part of Ford, and Lockheed Aerospace. They sell much of the spy equipment and they are both involved in arms sales to third-world countries. Menwith Hill gains information that would be useful to them. Lockheed and Boeing, for example, oppose the success of Airbus Industrie, which has sold many aeroplanes round the world. Can the Minister guarantee that information about commercial matters relating to Airbus Industrie and the sales of the Airbus 300, for example, has never been picked up by Menwith Hill and has never been passed on to part of the US military-industrial complex? Both Boeing and Lockheed depend for their continued existence on military contracts from the United States Government. Our Government continue to betray our people by allowing spy stations such as Menwith Hill to be dominated and operated by the United States, without any control that is visible to the people at large.

United Kingdom and United States Government.» — [Official Report, 27 April 1988; Vol. 132, c. 203.]

...

In other words, elected Members of Parliament are denied information on the appropriation of more than 200 acres of land by the United States Government, who now run a spy station in the heart of our country which is linked up to a global network. That is inexcusable. If there is parliamentary accountability, the moon is made of green cheese.»; http://www.parliament.the-stationery-office.co.uk/pa/cm199394/cmhansrd/1994-03-25/Debate-6.html.

(59) Dans la même intervention, Bob Creyer déclare ce qui suit: *«Menwith Hill is a spy station — a sophisticated version of the man in the dirty raincoat looking through a bedroom window or the pervert spying through a lavatory keyhole. Those who defend the station's invasion of our land, which has never been approved by Parliament, are no better. There is no glory or wonderful purpose involved in Menwith Hill. That is all the more true now that he cold war is over. Ministers justified the Menwith Hill base by saying it was part of the cold war, but we understand that that has finished. What is their justification for the spy station now?*

Yorkshire land has been taken from us to provide an eavesdropping centre that is virtually free from urban, electro-magnetic interference. That is why the station is sited at its current location. The station is part of a chain of such stations that span the globe. Their aim is to assert and retain United States supremacy. For example, exactly opposite to Menwith Hill, on the other side of the globe in a prohibited region in Australia stands the twin of Menwith Hill, Pine Gap station. When Menwith Hill opened, the United States air force security service listening post at Kirknewton near Edinburgh ceased operations and a former employee is quoted on page 210 of «Puzzle Palace» as saying:

«I had to keep a special watch for commercial traffic, details of commodities, what big companies were selling, like iron and steel and gas. Changes were frequent. One week I was asked to scan all traffic between Berlin and London and another week between Rome and Belgrade. Some weeks the list of words to watch for contained dozens of names of big companies. Some weeks I just had to look for commodities. All traffic» — interception material — was sent back to Fort Meade in Washington.»

Menwith Hill took over those functions and continued to pursue military eavesdropping.

Its spying grows. The cold war has ended, but the radomes number 21 after recent expansion. About 1,200 staff, who are mainly American, are employed there — the number has grown from 400 in 1980. United States staff are ordered never to mention the National Security Agency of America and to report all outside contacts with foreign nationals — the British people who live in the region — to ensure that supervision of such contacts is maintained.

...

There are two large United States firms within the military-industrial complex: Loral Space Systems Incorporated, formerly a part of Ford, and Lockheed Aerospace. They sell much of the spy equipment and they are both involved in arms sales to third-world countries. Menwith Hill gains information that would be useful to them. Lockheed and Boeing, for example, oppose the success of Airbus Industrie, which has sold many aeroplanes round the world. Can the Minister guarantee that information about commercial matters relating to Airbus Industrie and the sales of the Airbus 300, for example, has never been picked up by Menwith Hill and has never been passed on to part of the US military-industrial complex? Both Boeing and Lockheed depend for their continued existence on military contracts from the United States Government. Our Government continue to betray our people by allowing spy stations such as Menwith Hill to be dominated and operated by the United States, without any control that is visible to the people at large.

A recent «Dispatches» programme on Channel 4 examined the matter in some detail. I shall put a few quotations on the record for Parliament. Margaret Newsham is one of the few people who have worked at Menwith Hill and spoken out. She worked there from 1977 to 1981. She says:

«From the very beginning of my employment, it became very much aware to me that massive security violations were taking place. All the programmes that I did work on were subject to these abuses.» She is referring to interference in commercial traffic.

The programme's commentary on Margaret Newsham continues: «And that wasn't all. Inside Building 36D at Menwith, she was invited to listen in on an American Senator's intercepted phone call. After leaving, she informed the US Congress about what she'd seen.» Good on her. Can the Minister assure us that Menwith Hill never listens in to any telephone calls of United Kingdom Members of Parliament, not directly in the United Kingdom, but bounced back over the various satellite systems?

According to the programme, only one person in the world has ever got the National Security Agency to admit intercepting his messages. He was a United States lawyer called Abdeen Jaboro who said: «It took me 18 years to get my records finally destroyed. It is like Big Brother. It's like 1984, of — surveilling people all over the globe. And if you're British, if you're French, if you're Dutch, you're any-any people, anywhere you have no rights to complain about this. You have zero rights.»

What does it say for parliamentary democracy when people have no rights against these arrogant organisations which are given authority by a clique of people called the Government who have not come to Parliament to get any authority? It is a scandal and a disgrace, and I look forward to the Minister trying to explain that away, as he tried to at Question Time in a superficial and cliche-ridden manner.

A National Security Agency employee was quoted on the programme, but the words of an actor were used as a disguise. The Government knows all about using actors' words to disguise someone. That employee was quoted ad saying:

«Menwith Hill was responsible for intercepting ILC' and NDC'traffic from 1966 to 1976. Then came the satellite intercepts, like MOONPENNY. ILC is International Leased Carrier — basiscally, ordinary commercial traffic. Your and my phone calls. And NDC is Non-US diplomatic communications. But that job was later moved out of Menwith Hill during the 1970s, to Chicksands, where a special unit called DODJOCC was run by the NSA, direct from Menwith Hill. DODJOCC stands for Department of Defense Joint Operations Centre Chicksands. Because of the high sensitivity of its work no Britons were ever allowed in.»

Was that high sensitivity because they were intercepting British communications? Howard Teicher, National Security Council member from 1980 to 1986, said on the programme:

«As a rule I believe that the United States government would never spy on the British government, and would never direct the National Security Agency to try to collect information on British government entities or individuals.

However, having said that that would be the rule, I would never say never in this business because, at the end of the dat, national interests are national interests. And, as close as the US and the UK are, sometimes our interests diverge. So never say never. Especially in this business.»

...

What is the first priority at Menwith Hill? Will the Minister publish the agreement that allows Menwith Hill to be operated at the base near Harrogate? Why should not the people of the United Kingdom know about these matters? In a democracy, why should they be kept from them? It is an outrage that they ever have been.

What laws govern the operation of Menwith Hill? Do the United States employees there come under United Kingdom law or does the Visiting Forces Act 1952 apply to civilians? What rights do

A recent «Dispatches» programme on Channel 4 examined the matter in some detail. I shall put a few quotations on the record for Parliament. Margaret Newsham is one of the few people who have worked at Menwith Hill and spoken out. She worked there from 1977 to 1981. She says:

«From the very beginning of my employment, it became very much aware to me that massive security violations were taking place. All the programmes that I did work on were subject to these abuses.» She is referring to interference in commercial traffic.

The programme's commentary on Margaret Newsham continues: «And that wasn't all. Inside Building 36D at Menwith, she was invited to listen in on an American Senator's intercepted phone call. After leaving, she informed the US Congress about what she'd seen.» Good on her. Can the Minister assure us that Menwith Hill never listens in to any telephone calls of United Kingdom Members of Parliament, not directly in the United Kingdom, but bounced back over the various satellite systems?

According to the programme, only one person in the world has ever got the National Security Agency to admit intercepting his messages. He was a United States lawyer called Abdeen Jaboro who said: «It took me 18 years to get my records finally destroyed. It is like Big Brother. It's like 1984, of — surveilling people all over the globe. And if you're British, if you're French, if you're Dutch, you're any-any people, anywhere you have no rights to complain about this. You have zero rights.»

What does it say for parliamentary democracy when people have no rights against these arrogant organisations which are given authority by a clique of people called the Government who have not come to Parliament to get any authority? It is a scandal and a disgrace, and I look forward to the Minister trying to explain that away, as he tried to at Question Time in a superficial and cliche-ridden manner.

A National Security Agency employee was quoted on the programme, but the words of an actor were used as a disguise. The Government knows all about using actors' words to disguise someone. That employee was quoted ad saying:

«Menwith Hill was responsible for intercepting ILC' and NDC'traffic from 1966 to 1976. Then came the satellite intercepts, like MOONPENNY. ILC is International Leased Carrier — basiscally, ordinary commercial traffic. Your and my phone calls. And NDC is Non-US diplomatic communications. But that job was later moved out of Menwith Hill during the 1970s, to Chicksands, where a special unit called DODJOCC was run by the NSA, direct from Menwith Hill. DODJOCC stands for Department of Defense Joint Operations Centre Chicksands. Because of the high sensitivity of its work no Britons were ever allowed in.»

Was that high sensitivity because they were intercepting British communications? Howard Teicher, National Security Council member from 1980 to 1986, said on the programme:

«As a rule I believe that the United States government would never spy on the British government, and would never direct the National Security Agency to try to collect information on British government entities or individuals.

However, having said that that would be the rule, I would never say never in this business because, at the end of the dat, national interests are national interests. And, as close as the US and the UK are, sometimes our interests diverge. So never say never. Especially in this business.»

...

What is the first priority at Menwith Hill? Will the Minister publish the agreement that allows Menwith Hill to be operated at the base near Harrogate? Why should not the people of the United Kingdom know about these matters? In a democracy, why should they be kept from them? It is an outrage that they ever have been.

What laws govern the operation of Menwith Hill? Do the United States employees there come under United Kingdom law or does the Visiting Forces Act 1952 apply to civilians? What

individuals or companies have if they believe that they are being spied on by Menwith Hill ? For example, can the Minister give a categorical assurance that Menwith Hill is not intercepting commercial traffic ?

(60) *«Legal standards for the Intelligence Community in Conducting Electronic Surveillance»*; dit document kan geconsulteerd worden op het volgende internetadres :http://www.fas.org/irp/nsa/standards.html.

(61) De voornaamste bronnen van dit hoofdstuk zijn : (1) werkdocument 2a van de tijdelijke commissie van het Europees Parlement (PE 294.997); dit document kan worden geconsulteerd op het volgende internetadres: http://www.europarl.eu.int/tempcom/echelon/pdf/431720 en.pdf; (2) het derde opvolgingsverslag van het Comité I over « Echelon »; (3) volume 2/5, hoofdstuk 4, « *Comint and Law Enforcement* » van het STOA-verslag « *Development of surveillance technology and the risk of abuse of economic information* ».

(62) Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer, (*Publikatieblad* C 329 van 4 november 1996); opgenomen in bijlage.

(63) Notitie van de Nederlandse minister De Graeve (Defensie) aan de Tweede Kamer; de volledige notitie kan worden geconsulteerd op het internet : http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(64) Ontwerpresolutie van de Raad inzake de legale interceptie van telecommunicatie in verband met nieuwe technologieën.

(65) Wetgevingsresolutie met advies van het Europees Parlement van 7 mei 1999, *Publikatieblad* C 279, 498, van 1 oktober 1999.

(66) Werkdocument 2a van de tijdelijke commissie van het Europees Parlement (PE 294.997).

(67) STOA-verslag Volume 5/5 « *The perception of economic risks arising from the potential vulnerabilty* ».

(68) Systemen waarmee de overheid ofwel rechtstreeks ofwel via een « *trusted third party* » toegang kan krijgen tot de versleutelingscode.

(69) Eigen informatie van de begeleidingscommissies.

(70) Titel VI van het EU-Verdrag « Bepalingen inzake politiële en justitiële samenwerking in strafzaken » voorziet niet in een dergelijke bevoegdheid.

(71) Verslag over de begroting 2001, uitgebracht door de heer Boucheron; Hoofdstuk V, « *L'environnement des forces III. Le renseignement, A. La direction générale de la sécurité extérieure.* Te consulteren op het volgende internetadres : http:/www.assemblee-nationale.fr/budget/plf2001/b2624-40.asp#P4259_217712.

(72) Onder « adressen » moet men begrijpen : telefoonnummers, e-mails, faxnummers van ambassades, ministeries, internationale organisaties, NGO's, multinationals, ...

(73) Zie hierover het artikel van Vincent Jauvert.

(74) *O.c.*, http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(75) Hier wordt dus op een openlijke manier verwezen naar de doelstellingen die ILETS op internationaal vlak probeert te realiseren. Duidelijk is in elk geval dat hiervoor in Nederland een wettelijke basis bestaat.

(76) Werkdocument 5 van de tijdelijke commissie Echelon-interceptiesysteem (PE 294.997); Verslag over het wereldwijd systeem voor de interceptie van particuliere en economische commu-

rights do individuals or companies have if they believe that they are being spied on by Menwith Hill ? For example, can the Minister give a categorical assurance that Menwith Hill is not intercepting commercial traffic ?

(60) *«Legal standards for the Intelligence Community in Conducting Electronic Surveillance»*; ce document peut être consulté à l'adresse internet suivante : http://www.fas.org/irp/nsa/standards.html.

(61) Les sources principales de ce chapitre sont : (1) le document de travail 2a de la commission temporaire du Parlement européen (PE 294.997); ce document peut être consulté à l'adresse internet suivante : http://www.europarl.eu.int/tempcom/echelon/pdf/431720 en.pdf; (2) le troisième rapport de suivi du Comité R sur « Echelon »; (3) le volume 2/5, chapitre 4, « *Comint and Law Enforcement* » du rapport STOA « *Development of surveillance technology and the risk of abuse of economic information* ».

(62) Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (*Journal officiel* C 329 du 4 novembre 1996), reproduite en annexe.

(63) Note du ministre néerlandais De Graeve (Défense) à la *Tweede Kamer*; le texte complet peut être consulté sur l'internet à l'adresse suivante : http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(64) Projet de résolution du Conseil concernant l'interception légale des télécommunications dans le domaine des nouvelles technologies.

(65) Résolution législative avec avis du Parlement européen du 7 mai 1999, *Journal officiel* C 279, 498, du 1er octobre 1999.

(66) Document de travail 2a de la commission temporaire du Parlement européen (PE 294.997).

(67) Rapport STOA Volume 5/5 « *The perception of economic risks arising from the potential vulnerabilty* ».

(68) Systèmes dans lesquels les autorités ont accès, soit directement soit par l'intermédiaire d'une *« trusted third party »*, à un code de cryptage.

(69) Information propre des commissions de suivi.

(70) Le titre VI du Traité UE « Dispositions relatives à la coopération policière et judiciaire en matière pénale » ne prévoit pas pareille compétence.

(71) Rapport sur le budget 2001, fait par M. Boucheron; Chapitre V, « *L'environnement des forces III. Le renseignement, A. La direction générale de la sécurité extérieure;* à consulter à l'adresse suivante : http:/www.assemblee-nationale.fr/budget/plf2001/b2624-40.asp#P4259_217712.

(72) Par « adresses », il convient d'entendre : numéros de téléphone, adresses électroniques, numéros de télécopieurs d'ambassades, de ministères, d'organisations internationales, d'ONG, de multinationales, ...

(73) Voir à ce sujet l'article de Vincent Jauvert.

(74) *O.c.*, http://www.nrc.nl/W2/Lab/Echelon/doc010120.html.

(75) On renvoit donc ouvertement ici aux objectifs que les ILETS s'efforcent de réaliser au niveau international. Il est clair, en tout cas, qu'il existe aux Pays-Bas une base légale pour ce faire.

(76) Document de travail 5 de la commission temporaire sur le système d'interception Echelon (PE 294.997); Rapport sur le système d'interception au niveau mondial des communications

nicatie (Echelon-interceptiesysteem) van de tijdelijke commissie Echelon-interceptiesysteem, blz. 35 en volgende (PE 305.391); mevrouw Lizin, rapporteur, was aanwezig op de vergadering van 21 november 2000 tijdens dewelke de heer Enst Uhrlau een beeld schetste van de Duitse interceptiemogelijkheden.

(77) De wettelijke basis waarop de intercepties gebeuren is de wet inzake de beperking van het brief-, post- en telefoongeheim van 13 augustus 1968; deze wet werd op 28 oktober 1994 als volgt gewijzigd: *«Änderung des Gesetzes zu Artikel 10 Grundgesetz*.

Artikel 1 des Gesetzes zu Artikel 10 Grundgesetz vom 13. August 1968 (BGBl. I S. 949), das zuletzt durch Artikel 12 Abs. 4 des Gesetzes vom 14. September 1994 (BGBl. I S. 2325) geändert worden ist, wird wie folgt geändert:

[...]

«(1) Est sind die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantik Vertrages,

2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 3 Abs. 1 Satz 2 Nr. 2 bis 6 bestimmten Zwecken berechtigt, den Fernmeldeverkehr zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.»

3. § 3 wird wie folgt befaßt:

«§ 3 (1) Außer in den Fällen des § 2 dürfen auf Antrag des Bundesnachrichtendienstes Beschränkungen nach § 1 für internationale nicht leitungsgebundene Fernmeldeverkehrsbeziehungen angeordnet werden, die der nach § 5 zuständige Bundesminister mit Zustimmung des Abgeordnetengremiums gemäß § 9 bestimmt. Sie sind nur zulässig zur Sammlung von Nachrichten über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,

2. der Begehung internationaler terroristischer Anschläge in der Bundesrepublik Deutschland,

3. der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien im Sinne des Teils I der Ausfuhrliste (Anlage AL zur Außenwirtschaftsverordnung) in Fällen von erheblicher Bedeutung,

4. der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge aus dem Ausland in das Gebiet der Bundesrepublik Deutschland,

5. im Ausland begangener Geldfälschungen sowie

6. der Geldwäsche im Zusammenhang mit den in den Nummern 3 bis 5 genannten Handlungen rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. In den Fällen der Nummer 1 dürfen Beschränkungen nach Satz 1 auch für leitungsgebundene Fernmeldeverkehrsbeziehungen und für Postverkehrsbeziehungen angeordnet werden.

(2) Für Beschränkungen im Sinne des Absatzes 1 darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Die Suchbegriffe dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse führen. Satz 2 gilt nicht für Fernmeldeanschlüsse im Ausland, sofern ausgeschlossen werden kann, daß Anschlüsse

1. deutscher Staatsangehöriger oder

privées et économiques (système d'interception Echelon) de la commission temporaire sur le système d'interception Echelon, p. 35 et suivantes (PE 305.391); Mme Lizin, rapporteuse, était présente à la réunion du 21 novembre 2000, au cours de laquelle M. Enst Uhrlau a esquissé un tableau des possibilités d'interception allemandes.

(77) La base légale qui sous-tend les interceptions est la loi relative à la limitation du secret des lettres, du courrier et du téléphone du 13 août 1968; cette loi a été modifiée le 28 octobre 1994 de la manière suivante: *«Änderung des Gesetzes zu Artikel 10 Grundgesetz*.

Artikel 1 des Gesetzes zu Artikel 10 Grundgesetz vom 13. August 1968 (BGBl. I S. 949), das zuletzt durch Artikel 12 Abs. 4 des Gesetzes vom 14. September 1994 (BGBl. I S. 2325) geändert worden ist, wird wie folgt geändert:

[...]

«(1) Est sind die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantik Vertrages,

2. der Bundesnachrichtendienst im Rahmen seiner Aufgaben nach § 1 Abs. 2 des BND-Gesetzes auch zu den in § 3 Abs. 1 Satz 2 Nr. 2 bis 6 bestimmten Zwecken berechtigt, den Fernmeldeverkehr zu überwachen und aufzuzeichnen, in den Fällen der Nummer 1 auch die dem Brief- oder Postgeheimnis unterliegenden Sendungen zu öffnen und einzusehen.»

3. § 3 wird wie folgt befaßt:

«§ 3 (1) Außer in den Fällen des § 2 dürfen auf Antrag des Bundesnachrichtendienstes Beschränkungen nach § 1 für internationale nicht leitungsgebundene Fernmeldeverkehrsbeziehungen angeordnet werden, die der nach § 5 zuständige Bundesminister mit Zustimmung des Abgeordnetengremiums gemäß § 9 bestimmt. Sie sind nur zulässig zur Sammlung von Nachrichten über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,

2. der Begehung internationaler terroristischer Anschläge in der Bundesrepublik Deutschland,

3. der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien im Sinne des Teils I der Ausfuhrliste (Anlage AL zur Außenwirtschaftsverordnung) in Fällen von erheblicher Bedeutung,

4. der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge aus dem Ausland in das Gebiet der Bundesrepublik Deutschland,

5. im Ausland begangener Geldfälschungen sowie

6. der Geldwäsche im Zusammenhang mit den in den Nummern 3 bis 5 genannten Handlungen rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. In den Fällen der Nummer 1 dürfen Beschränkungen nach Satz 1 auch für leitungsgebundene Fernmeldeverkehrsbeziehungen und für Postverkehrsbeziehungen angeordnet werden.

(2) Für Beschränkungen im Sinne des Absatzes 1 darf der Bundenachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Die Suchbegriffe dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse führen. Satz 2 gilt nicht für Fernmeldeanschlüsse im Ausland, sofern ausgeschlossen werden kann, daß Anschlüsse

1. deutscher Staatsangehöriger oder

2. von Gesellschaften mit dem Sitz im Ausland, wenn der überwiegende Teil ihres Vermögens oder ihres Kapitals sowie die tatsächliche Kontrolle über die Gesellschaft deutschen natürlichen oder juristischen Personen zusteht und die Mehrheit der Vertretungsberechtigten deutsche Staatsangehörige sind, gezielt erfaßt werden. Die Suchbegriffe sind in der Anordnung zu benennen. Die Durchführung ist mit technischen Mitteln zu protokollieren; sie unterliegt der Kontrolle gemäß § 9 Abs. 2. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

(3) Bei der Durchführung von Maßnahmen nach Absatz 1 erlangte personenbezogene Daten dürfen nur zur Verhinderung, Aufklärung oder Verfolgung von Straftaten verwendet werden, die in § 2 dieses Gesetzes und in § 138 des Strafgesetzbuches bezeichnet sind, sowie von Straftaten nach den §§ 261 und 264 des Strafgesetzbuches, § 92a des Ausländergesetzes, § 34 Abs. 1 bis 6 und 8 und § 35 des Außenwirtschaftsgesetzes, §§ 19 bis 21 und 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen oder § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes, soweit gegen die Person eine Beschränkung nach § 2 angeordnet ist oder wenn tatsächliche Anhaltpunkte für den Verdacht bestehen, daß jemand eine der vorgenannten Straftaten plant, begeht oder begangen hat. § 12 des BND-Gesetzes bleibt unberührt.

(4) Der Bundesnachrichtendienst prüft, ob durch Maßnahmen nach Absatz 1 erlangte personenbezogene Daten für die dort genannten Zwecke erforderlich sind.

(5) Die nach Absatz 1 erlangen Daten sind vollständig zu den in Absatz 3 bezeichneten Zwecken den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst, dem Zollkriminalamt, dem Bundesausfuhramt, den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien zu übermitteln, soweit dies zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Die Entscheidung erfolgt durch einen Bediensteten, der die Befähigung zum Richteramt hat.

(6) Sind nach Absatz 1 erlangte Daten für die dort genannten Zwecke nicht oder nicht mehr erforderlich und sind die Daten nicht nach Absatz 5 anderen Behörden zu übermitteln, sind die auf diese Daten bezogenen Unterlagen unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu vernichten und, soweit die Daten in Dateien gespeichert sind, zu löschen. Die Vernichtung und die Löschung sind zu protokollieren. In Abständen von jeweils sechs Monaten ist zu prüfen, ob die Voraussetzungen für eine Vernichtung oder Löschung vorliegen.

(7) Der Empfänger prüft, ob er die nach Absatz 5 übermittelten Daten für die in Absatz 3 bezeichneten Zwecke benötigt. Benötigt er die Daten nicht, hat er die Unterlagen unverzüglich zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlicht sind, nicht oder nur mit unvertretbarem Aufwand möglich ist; eine Verwendung dieser Daten ist unzulässig.

(8) Betroffenen, deren Daten durch eine Maßnahme nach Absatz 1 erlangt worden sind, ist die Beschränkung des Fernmeldegeheimnisses mitzuteilen, sobald eine Gefährdung des Zwecks der Beschränkung und der Verwendung ausgeschlossen werden kann. Eine Mitteilung unterbleibt, wenn die Daten

1. vom Bundesnachrichtendienst innerhalb von drei Monaten nach Erlangung oder

2. von der Behörde, der sie nach Absatz 5 übermittelt worden sind, innerhalb von drei Monaten nach Empfang vernichtet worden sind. Die Mitteilung obliegt dem Bundesnachrichtendienst, im Falle der Übermittlung nach Absatz 5 der Empfängerbehörde.

(9) Die Kommission kann dem Bundesbeauftragten für den Datenschutz vor ihrer Entscheidung über die Zulässigkeit und Notwendigkeit einer Maßnahme nach § 9 Abs. 2 Gelegenheit zur

2. von Gesellschaften mit dem Sitz im Ausland, wenn der überwiegende Teil ihres Vermögens oder ihres Kapitals sowie die tatsächliche Kontrolle über die Gesellschaft deutschen natürlichen oder juristischen Personen zusteht und die Mehrheit der Vertretungsberechtigten deutsche Staatsangehörige sind, gezielt erfaßt werden. Die Suchbegriffe sind in der Anordnung zu benennen. Die Durchführung ist mit technischen Mitteln zu protokollieren; sie unterliegt der Kontrolle gemäß § 9 Abs. 2. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

(3) Bei der Durchführung von Maßnahmen nach Absatz 1 erlangte personenbezogene Daten dürfen nur zur Verhinderung, Aufklärung oder Verfolgung von Straftaten verwendet werden, die in § 2 dieses Gesetzes und in § 138 des Strafgesetzbuches bezeichnet sind, sowie von Straftaten nach den §§ 261 und 264 des Strafgesetzbuches, § 92a des Ausländergesetzes, § 34 Abs. 1 bis 6 und 8 und § 35 des Außenwirtschaftsgesetzes, §§ 19 bis 21 und 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen oder § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes, soweit gegen die Person eine Beschränkung nach § 2 angeordnet ist oder wenn tatsächliche Anhaltpunkte für den Verdacht bestehen, daß jemand eine der vorgenannten Straftaten plant, begeht oder begangen hat. § 12 des BND-Gesetzes bleibt unberührt.

(4) Der Bundesnachrichtendienst prüft, ob durch Maßnahmen nach Absatz 1 erlangte personenbezogene Daten für die dort genannten Zwecke erforderlich sind.

(5) Die nach Absatz 1 erlangen Daten sind vollständig zu den in Absatz 3 bezeichneten Zwecken den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst, dem Zollkriminalamt, dem Bundesausfuhramt, den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien zu übermitteln, soweit dies zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Die Entscheidung erfolgt durch einen Bediensteten, der die Befähigung zum Richteramt hat.

(6) Sind nach Absatz 1 erlangte Daten für die dort genannten Zwecke nicht oder nicht mehr erforderlich und sind die Daten nicht nach Absatz 5 anderen Behörden zu übermitteln, sind die auf diese Daten bezogenen Unterlagen unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu vernichten und, soweit die Daten in Dateien gespeichert sind, zu löschen. Die Vernichtung und die Löschung sind zu protokollieren. In Abständen von jeweils sechs Monaten ist zu prüfen, ob die Voraussetzungen für eine Vernichtung oder Löschung vorliegen.

(7) Der Empfänger prüft, ob er die nach Absatz 5 übermittelten Daten für die in Absatz 3 bezeichneten Zwecke benötigt. Benötigt er die Daten nicht, hat er die Unterlagen unverzüglich zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlicht sind, nicht oder nur mit unvertretbarem Aufwand möglich ist; eine Verwendung dieser Daten ist unzulässig.

(8) Betroffenen, deren Daten durch eine Maßnahme nach Absatz 1 erlangt worden sind, ist die Beschränkung des Fernmeldegeheimnisses mitzuteilen, sobald eine Gefährdung des Zwecks der Beschränkung und der Verwendung ausgeschlossen werden kann. Eine Mitteilung unterbleibt, wenn die Daten

1. vom Bundesnachrichtendienst innerhalb von drei Monaten nach Erlangung oder

2. von der Behörde, der sie nach Absatz 5 übermittelt worden sind, innerhalb von drei Monaten nach Empfang vernichtet worden sind. Die Mitteilung obliegt dem Bundesnachrichtendienst, im Falle der Übermittlung nach Absatz 5 der Empfängerbehörde.

(9) Die Kommission kann dem Bundesbeauftragten für den Datenschutz vor ihrer Entscheidung über die Zulässigkeit und Notwendigkeit einer Maßnahme nach § 9 Abs. 2 Gelegenheit zur

Stellungnahme in Fragen des Datenschutzes geben. Die Stellungnahme erfolgt ausschließlich gegenüber der Kommission.

(10) Das Gremium nach § 9 Abs. 1 erstattet dem Bundestag jährlich einen Bericht über die Durchführung der Maßnahmen nach den Absätzen 1 bis 9.»

(78) Deze controlecommissie wordt aangesteld door de *Bundestag* en bestaat uit acht leden.

(79) BverG, 1 BvR 2226/92 van 14 juli 1999.

(80) De volledige tekst van de heer Thomas is bij dit verslag gevoegd in bijlage 4.

(81) De volledige tekst van deze aanbeveling is bij dit verslag gevoegd in bijlage 5.

(82) Dit artikel voegt artikel 90*ter* in het Wetboek van strafvordering in.

(83) Arrest Klass van 6 september 1978, reeks A nr. 28, blz 23 en volgende.

(84) In dit geval het toezichtsysteem zoals uitgewerkt in het Duits recht.

(85) Volgens artikel 13, eerste lid, van richtlijn 95/46/EG, kan een lidstaat wettelijke maatregelen treffen ter beperking van de reikwijdte van sommige plichten (bijvoorbeeld betreffende het verzamelen van gegevens) en rechten (bijvoorbeeld het recht om hierover geïnformeerd te worden) waarin de richtlijn voorziet. Deze uitzonderingen zijn duidelijk afgebakend: de beperking moet noodzakelijk zijn ter vrijwaring van de openbare belangen die worden opgesomd in paragrafen *a)* tot *g)* van dit artikel, zoals de Veiligheid van de Staat, de landsverdediging, of het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten.

In de eerste paragraaf van artikel 14 bepaalt richtlijn 97/66/EG ook dat de lidstaten alleen kunnen afwijken van de plicht om het vertrouwelijk karakter van de oproepen op de openbare netwerken te garanderen indien dit noodzakelijk is voor het vrijwaren van de Veiligheid van de Staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsproen en vervolgen van strafbare feiten.

(86) De volledige tekst gaat als bijlage 6 bij dit verslag.

(87) Zie arrest Klass tegen Duitsland gewezen in 1978.

(88) Zo is het afluisteren van telefoongesprekken een daad van wilsdwang en dus een inmenging in het recht op eerbiediging van het privé-leven, dat gewaarborgd wordt door artikel 8 EVRM. Deze bewering is slechts een herhaling van een constante in de rechtspraak van het Europees Hof voor de rechten van de mens, die reeds in 1978 gesteld werd in het arrest Klass tegen Duitsland en leidde tot de veroordeling van drie verschillende landen in 2000: Zwitserland (arrest Amman), Roemenië (arrest Rotaru) en het Verenigd Koninkrijk (arrest Khan).

(89) Conferentie van de nationale commissies voor de bescherming van de persoonlijke levenssfeer, verbonden met DG 15 van de Commissie.

(90) «De fundamentele beperking die het internationaal recht oplegt aan een Staat is dat de Staat geen macht kan uitoefenen op het grondgebied van een andere Staat, tenzij er een regel bestaat die dit toestaat. In dat opzicht is de rechtspraak zeker territoriaal: zij kan niet worden uitgeoefend buiten het grondgebied, tenzij krachtens een regel die dit toestaat en die voortvloeit uit het internationaal gewoonterecht of uit een verdrag.»

(91) Verslag over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (Echelon-interceptiesysteem), *o.c.*, blz. 80-83.

(92) Voor de begeleidingscommissies staat het vast dat dit gebeurt in het kader van het UKUSA-akkoord, een systeem dat

Stellungnahme in Fragen des Datenschutzes geben. Die Stellungnahme erfolgt ausschließlich gegenüber der Kommission.

(10) Das Gremium nach § 9 Abs. 1 erstattet dem Bundestag jährlich einen Bericht über die Durchführung der Maßnahmen nach den Absätzen 1 bis 9.»

(78) Cette commission de contrôle est désignée par le *Bundestag* et est composée de huit membres.

(79) BverG, 1 BvR 2226/92 du 14 juillet 1999.

(80) Le texte complet de M. Thomas est annexé au présent rapport en annexe 4.

(81) Le texte complet de cette recommandation est annexé au présent rapport en annexe 5.

(82) Cet article insère l'article 90*ter* dans le Code d'instruction criminelle.

(83) Arrêt Klass, du 6 septembre 1978, série A n° 28, p. 23 et s.

(84) En l'occurrence le système de surveillance tel qu'élaboré en droit allemand.

(85) Selon l'article 13, 1er alinéa, de la directive 95/46/CE, bepalt richtlijn un État membre peut prendre des mesures législatives visant à limiter la portée de certaines obligations (par exemple concernant la collecte de données) et de certains droits (par exemple le droit d'être informé sur une collecte) prévus par la directive. Ces exceptions sont strictement énumérées: la limitation doit constituer une mesure nécessaire pour sauvegarder les intérêts publics énoncés de façon exhaustive dans les paragraphes *a)* à *g)* de cet article, tels que la Sûreté de l'État, la défense, la sécurité publique ou la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Dans son article 14, paragraphe 1, la directive 97/66/CE précise également que les États membres ne peuvent limiter l'obligation de confidentialité des communications sur des réseaux publics que lorsqu'une telle mesure constitue une mesure nécessaire pour sauvegarder la Sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales.

(86) Le texte complet se trouve en annexe 6 du présent rapport.

(87) *Cf.* l'arrêt Klass contre Allemagne rendu en 1978.

(88) Ainsi les interceptions téléphoniques sont des actes de contrainte sur une volonté et donc des ingérences dans le droit au respect de la vie privée garanti par l'article 8 CEDH. Une telle affirmation ne constitue jamais que le rappel d'une jurisprudence constante de la Cour européenne des droits de l'homme, posée dès 1978 dans l'arrêt Klass contre Allemagne et soldée par la condamnation de trois pays différents en 2000: la Suisse (arrêt Amman), la Roumanie (arrêt Rotaru) et le Royaume-Uni (arrêt Khan).

(89) Conférence des commissions nationales de protection de la vie privée, rattachée à la DG 15 de la Commission.

(90) «La limitation primordiale qu'impose le droit international à l'État est celle d'exercer, sauf l'existence d'une règle permissive contraire, tout exercice de sa puissance sur le territoire d'un autre État. Dans ce sens, la juridiction est certainement territoriale; elle ne pourrait être exercée hors du territoire, sinon en vertu d'une règle permissive découlant du droit international coutumier ou d'une convention».

(91) Rapport sur l'existence d'un système d'interception électronique planétaire auprès de personnes privées et des entreprises (système d'interception Echelon), *o.c.*, p. 80-83.

(92) Pour les commissions de suivi, il ne fait aucun doute que ces interceptions ont lieu dans le cadre du pacte UKUSA, un

bekend is geworden onder de naam Echelon zonder dat het noodzakelijk met die naam door de UKUSA-landen wordt aangeduid.

(93) Artikel 14.1 bepaalt: 1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6 en in artikel 8, leden 1 tot en met 4, bedoelde rechten en plichten, indien dit noodzakelijk is voor het vrijwaren van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het telecommunicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn 95/46/EG.

(94) *Article 8 — Right to respect for private and family life*

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

(95) Gelet op het geheim karakter van Echelon lijdt het weinig twijfel dat niet is voldaan aan de vereiste van toegankelijkheid en voorspelbaarheid van de wet — wat volgens de vaste rechtspraak van het EHRM noodzakelijk is om een inbreuk op een door het EVRM gewaarborgd recht te verantwoorden. Het is daarom niet nodig te stellen dat aan de wettigheidsvereiste niet is voldaan omdat de wet niet in overeenstemming zou zijn met het internationaal recht of artikel 53 EVRM. Deze twee vereisten maken immers geen deel uit van de vaste rechtspraak van het EHRM over de wettigheidsvereiste.

Het EHRM heeft overigens het belang van een duidelijke en toegankelijke wet beklemtoond in de arresten Kruslin t. Frankrijk en Huvig t. Frankrijk. Volgens het Hof «*Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une «loi» d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner*» (EHRM, arrest van 24 april 1990, Kruslin t. Frankrijk, § 33). In die zaak besluit het Hof dat de Franse wet niet voldeed aan de wettigheidsvereiste omdat ze niet voldoende rechtszekerheid bood.

Dat een verdragspartij bij het EVRM niet aan haar verplichtingen kan ontsnappen op grond van een overdracht van bevoegdheden aan een internationale of supranationale organisatie (zoals de NAVO) werd recentelijk nog bevestigd in het arrest Matthews t. Verenigd Koninkrijk. Het EHRM hield er het Verenigd Koninkrijk aansprakelijk voor het feit dat onderdanen van Gibraltar niet konden stemmen bij de verkiezingen voor het Europees Parlement, hoewel dit volgens het Verenigd Koninkrijk een gevolg was van het Europees Gemeenschapsrecht. Volgens het EHRM «*la Convention n'exclut pas le transfert de compétences à des organisations internationales, pourvu que les droits garantis par la Convention continuent d'être «reconnus». Pareil transfert ne fait donc pas disparaître la responsabilité des États membres*» (EHRM, arrest van 18 februari 1999, Matthews t. Verenigd Koninkrijk, § 32).

système que l'on connaît sous le nom d'Echelon, sans que les pays du pacte UKUSA utilisent nécessairement ce nom.

(93) L'article 14.1 dispose ce qui suit: 1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 5 et 6 et à l'article 8, §§ 1er à 4, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense et la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de télécommunications, comme le prévoit l'article 13, 1er alinéa, de la directive 95/46/CE.

(94) Article 8 — Droit au respect de la vie privée et familiale

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

(95) Vu le caractère secret du système Echelon, il fait peu de doute qu'on n'ait pas satisfait à la condition d'accessibilité et de prévisibilité de la loi, qui, selon la jurisprudence constante de la CEDH, doit être remplie pour que la violation d'un droit garanti par la question européenne de protection des droits de l'homme puisse être justifiée. Dès lors, il n'est pas nécessaire d'affirmer que la condition de légalité n'a pas été satisfaite parce que la loi ne respecterait pas le droit international ou l'article 53 CEDH. En effet, ces deux conditions ne font pas partie de la jurisprudence constante de la CEDH sur la condition de légalité.

Au demeurant, la CEDH a souligné l'importance de la clarté et de l'accessibilité de la loi dans les arrêts Kruslin c. France et Huvig c. France. Selon la Cour, «Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une «loi» d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner» (CEDH, arrêt du 24 april 1990, Kruslin c. France, § 33). Dans cette affaire, la Cour conclut que la loi française ne remplissait pas la condition de légalité, parce qu'elle n'offrait pas la sécurité juridique nécessaire.

Récemment, l'arrêt Matthews c. Royaume-Uni a confirmé une nouvelle fois qu'une partie à la CEDH ne peut pas échapper à ses obligations en invoquant un transfert de compétences à une organisation internationale ou supranationale (comme l'OTAN). La CEDH a tenu le Royaume-Uni responsable du fait que des ressortissants de Gibraltar n'aient pas pu participer à l'élection du Parlement européen, même si le Royaume-Uni a considéré que c'était là une conséquence du droit de la Communauté européenne. Selon la CEDH, «la Convention n'exclut pas le transfert de compétences à des organisations internationales, pourvu que les droits garantis par la Convention continuent d'être «reconnus». Pareil transfert ne fait donc pas disparaître la responsabilité des États membres» (CEDH, arrêt du 18 février 1999, Matthews c. Royaume-Uni, § 32).

59.210 — E. Guyot, n. v., Brussel