Belgische Senaat

Gewone Zitting 2001-2002

**2-191**

Plenaire vergaderingen

Woensdag 20 maart 2002

Namiddagvergadering

# Handelingen

Sénat de Belgique

Session ordinaire 2001-2002

# Annales

Séances plénières

Mercredi 20 mars 2002

Séance de l'après-midi

**2-191**

De **Handelingen** bevatten de integrale tekst van de redevoeringen in de oorspronkelijke taal. Deze tekst werd goedgekeurd door de sprekers. De vertaling – *cursief gedrukt* – verschijnt onder de verantwoordelijkheid van de dienst Verslaggeving. Van lange uiteenzettingen is de vertaling een samenvatting.

De nummering bestaat uit het volgnummer van de legislatuur sinds de hervorming van de Senaat in 1995, het volgnummer van de vergadering en de paginering.

Voor bestellingen van Handelingen en Vragen en Antwoorden van Kamer en Senaat:
Dienst Publicaties Kamer van volksvertegenwoordigers, Natieplein 2 te 1008 Brussel, tel. 02/549.81.95 of 549.81.58.

Deze publicaties zijn gratis beschikbaar op de websites van Senaat en Kamer:
www.senate.be www.dekamer.be

Afkortingen - Abréviations

| | |
|---|---|
| AGALEV | Anders Gaan Leven |
| CD&V | Christen-Democratisch & Vlaams |
| ECOLO | Écologistes |
| PRL-FDF-MCC | Parti Réformateur Libéral – Front Démocratique des Francophones – Mouvement des Citoyens pour le Changement |
| PS | Parti Socialiste |
| PSC | Parti Social Chrétien |
| SP.A | Socialistische Partij Anders |
| VL. BLOK | Vlaams Blok |
| VLD | Vlaamse Liberalen en Democraten |
| VU-ID | Volksunie-ID21 |

Les **Annales** contiennent le texte intégral des discours dans la langue originale. Ce texte a été approuvé par les orateurs.
Les traductions – *imprimées en italique* – sont publiées sous la responsabilité du service des Comptes rendus. Pour les interventions longues, la traduction est un résumé.

La pagination mentionne le numéro de la législature depuis la réforme du Sénat en 1995, le numéro de la séance et enfin la pagination proprement dite.

Pour toute commande des Annales et des Questions et Réponses du Sénat et de la Chambre des représentants: Service des Publications de la Chambre des représentants, Place de la Nation 2 à 1008 Bruxelles, tél. 02/549.81.95 ou 549.81.58.

Ces publications sont disponibles gratuitement sur les sites Internet du Sénat et de la Chambre:
www.senate.be www.lachambre.be

## Inhoudsopgave

Verslag over het eventuele bestaan van een netwerk voor het onderscheppen van communicaties, «Echelon» genaamd (Stuk 2-754) ....4

Bespreking....4

Wetsontwerp ertoe strekkende het Belgische recht in overeenstemming te brengen met het Verdrag tegen foltering en andere wrede, onmenselijke of onterende behandeling of bestraffing, aangenomen te New York op 10 december 1984 (Stuk 2-1020) (Evocatieprocedure) ....38

Algemene bespreking ....38

Artikelsgewijze bespreking ....38

Berichten van verhindering ....40

## Sommaire

Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé «Echelon» (Doc. 2-754)....4

Discussion....4

Projet de loi de mise en conformité du droit belge avec la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, adoptée à New York le 10 décembre 1984 (Doc. 2-1020) (Procédure d'évocation)....38

Discussion générale ....38

Discussion des articles ....38

Excusés ....40

**Voorzitter: de heer Armand De Decker**

*(De vergadering wordt geopend om 14.25 uur.)*

## Verslag over het eventuele bestaan van een netwerk voor het onderscheppen van communicaties, «Echelon» genaamd (Stuk 2-754)

### *Bespreking*

***Mevrouw Anne-Marie Lizin (PS)****, rapporteur. – Ik dank de minister dat hij aanwezig is. Ondanks de geringe belangstelling van mijn collega's verdient dit onderwerp een voldoende uitgebreide toelichting. Ik hoop dat de regering de tijd neemt om gedetailleerd te antwoorden op de argumenten van de Senaat en meer in het bijzonder van de commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en de veiligheidsdiensten.*

*Ik zal eerst het verslag naar voren brengen en vervolgens enkele bijkomende punten toelichten.*

*Waarom heeft het Belgische Parlement – Kamer en Senaat – en de Begeleidingscommissie het nuttig geoordeeld om een verslag op te stellen? Over dit onderwerp werden sinds 1998 immers al talrijke parlementaire vragen gesteld. Vertrekpunt voor deze parlementaire bezorgdheid over de interceptie van communicatiestromen was een tussentijds verslag dat door de Omega Foundation uit Manchester werd voorgesteld aan het STOA Panel. Dit orgaan van het Europees Parlement heeft de studie overgezonden aan de Commissie rechten en vrijheden van de burger, justitie en de binnenlandse zaken van het Europees Parlement.*

*In 1998 hebben wij bij monde van de commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en de veiligheidsdiensten aan het Comité I gevraagd om een toezichtsonderzoek te openen. In het eerste verslag dat in 1999 door het Comité I werd goedgekeurd, werden al een reeks besluiten getrokken die aanzetten tot het voortzetten van het onderzoek. Volgens het Comité I beschikken de Belgische inlichtingendiensten niet over de technische middelen om zelf te kunnen vaststellen of het systeem 'Echelon' bestaat. Zij putten hun kennis over dit onderwerp uit open bronnen.*

*Op dat ogenblik kon de Veiligheid van de Staat 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 ADIV heeft bijgevolg de toepassing van het voorzorgsprincipe aanbevolen. Het Comité I was van oordeel dat de overheid voor dit probleem moest worden gesensibiliseerd en onderschreef op die manier zonder veel moeite de conclusies van de ADIV. Wij hebben het Comité I verzocht om het probleem op de voet te volgen en wij hebben regelmatig tussentijdse verslagen over het dossier Echelon ontvangen.*

*Naast het Echelondossier bestonden er ook nog enkele parallelle dossiers, met name de pogingen om binnen te dringen in het informaticasysteem van een universitair onderzoekscentrum en verder het dossier Lernout & Hauspie, aangezien het gebied van de spraakherkenning wel eens zou*

**Présidence de M. Armand De Decker**

*(La séance est ouverte à 14 h 25.)*

## Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé «Echelon» (Doc. 2-754)

### *Discussion*

**Mme Anne-Marie Lizin (PS)**, rapporteuse. – Je remercie le ministre de la Justice de sa présence. Malgré le peu d'intérêt que suscite le sujet auprès de mes collègues, il me semble qu'il mérite un assez long développement. J'espère que le gouvernement aura le temps de répondre en détail aux arguments que le Sénat et en particulier la Commission chargée du suivi du Comité permanent de contrôle des services de renseignement et de sécurité ont développés.

Je présenterai d'abord le contenu du rapport ; je me permettrai ensuite de développer quelques points complémentaires.

Pourquoi le Parlement belge – Chambre et Sénat – et spécialement la commission du suivi ont-ils estimé utile de rédiger un rapport ? Ce sujet a donné lieu à de nombreuses questions parlementaires depuis 1998. L'inquiétude des parlementaires à propos de l'interception des communications a surtout été inspirée par une étude présentée par la Fondation Omega de Manchester au groupe du STOA. Cet organe du Parlement européen a, dès 1997, relayé cette étude au Parlement européen, à la commission des libertés et des droits de citoyens, ce qui situe d'emblée l'importance du problème.

En 1998, nous avons, via la commission du suivi du Comité permanent de contrôle des services de renseignement et de sécurité, demandé au Comité R d'approfondir cette question et d'ouvrir une enquête de contrôle. Le premier rapport, approuvé en 1999 par le Comité R, arrivait déjà à une série de conclusions incitant à poursuivre les investigations.

Les services de renseignement belges, disait le Comité R, n'ont pas la possibilité technique de constater eux-mêmes l'existence du système « Echelon ». Leur connaissance du sujet résulte de la consultation de sources ouvertes.

À ce moment-là, 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.

Le Service général de renseignement et de sécurité a dès lors recommandé le principe de précaution, façon subtile de reconnaître tout de même l'élément clé. Il ne coûtait pas cher de dire que le Comité R avait alors accepté les conclusions du SGR en estimant que les autorités devaient être sensibilisées à ce problème. Nous avons alors demandé au Comité R de rester attentif à ce problème et nous avons reçu régulièrement des rapports intermédiaires concernant le dossier Echelon.

Outre ce dossier Echelon, il existait également quelques dossiers parallèles, notamment des intrusions dans le système informatique d'un centre universitaire de recherche et chez Lernout & Hauspie, le système de reconnaissance vocale pouvant être un domaine ayant fait l'objet de ce type

*kunnen blootstaan aan zulke aanvallen. In zijn laatste verslag heeft het Comité I conclusies getrokken die interessant zijn voor onze werkzaamheden.*

*Het Comité stelt vast dat noch het bestaan, noch de omvang of het gebruik van een interceptienetwerk officieel erkend wordt door de betrokken regeringen. Wel staat het volgens het Comité I 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. Het bestaan van het UKUSA-verdrag en dat van een technische samenwerking tussen de interceptieorganismen van de vijf Angelsaksische landen is intussen officieel erkend.*

*De technische mogelijkheden van deze diensten zijn enorm: het systeem zou alle communicatie die via satellieten verloopt kunnen opvangen; 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. Men weet trouwens niet goed hoe goed en doeltreffend het systeem in de praktijk werkt. Een en ander werd neergeschreven vóór 11 september. Sindsdien kan de doeltreffendheid van het systeem in opspraak zijn gekomen.*

*Verder bestaan er ernstige aanwijzingen dat het systeem wordt gebruikt voor economische spionage. Een dergelijk interceptiesysteem vormt ongetwijfeld een aanslag op het privé-leven van de burgers en overtreedt de Europese regels in verband met de interceptie van telecommunicatie.*

*In zijn aanbevelingen stelt het Comité I vast dat de Veiligheid niet over voldoende middelen beschikt om vooruitgang te boeken op dit gebied. Het Comité I gaat ervan uit dat dit netwerk hoogstwaarschijnlijk bestaat, zonder daarvoor een sluitend bewijs te hebben. Het neemt verder ook aan dat algemeen gezien de huidige technologieën de mogelijkheden bieden aan zowel landen als criminele organisaties om op grote schaal telecommunicaties te onderscheppen. Het geeft aan dat deze handelswijze een geschikte manier is om binnen te dringen in het wetenschappelijk en economisch potentieel van een land.*

*Het Comité I vroeg de Staatsveiligheid en de ADIV op te dragen samen te werken om informatie over dit systeem te verzamelen, om aan de inlichtingendiensten de technische en menselijke middelen te verlenen die noodzakelijk zijn om deze opdracht te vervullen, de wettelijke technische middelen aan te passen, zodat zij over een wettelijk kader beschikken om op een selectieve wijze opsporingen te verrichten en communicaties te onderscheppen en af te luisteren. Wij kennen de discussie over dit onderwerp. Ook onze commissie voor de Binnenlandse Aangelegenheden heeft hierover aanbevelingen gedaan met het oog op een doeltreffende werking van de anti-terreurcellen.*

*Het Comité I heeft verder aanbevolen om de nodige menselijke middelen toe te kennen, dit wil zeggen, het gebruik van externe experts, informaticaspecialisten, ingenieurs, enzovoorts, en om de oprichting van een dienst te overwegen die belast wordt met het aanbrengen van een oplossing voor*

d'attaques. Dans son dernier rapport d'activités, le Comité R a formulé des conclusions intéressantes pour nos travaux.

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. On ne trouve aucune trace de reconnaissance du système. Toutefois, ajoute le Comité R, 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 officiellement chargés de l'interception des télécommunications. L'existence du pacte UK-USA et celle d'une collaboration technique entre les organismes d'interception des cinq pays anglo-saxons ont, entre-temps, été officiellement reconnues.

On sait, par ailleurs, dit le Comité R, que les ressources techniques et humaines de ces services sont énormes : le système serait en mesure de capter toutes les communications qui se font par satellite ; 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. On ne sait d'ailleurs pas trop quelles sont la qualité réelle et l'efficacité de ce système. Ces lignes ont été écrites avant le 11 septembre. Depuis lors, l'efficacité du système a donc pu être mise en cause.

Toutefois, ajoute le Comité R, il existe de sérieux indices selon lesquels le système serait utilisé à des fins d'espionnage économique. 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.

Les recommandations du Comité R constatent que la Sûreté ne dispose pas des moyens suffisants pour avancer dans cette matière, considèrent l'existence de ce réseau comme hautement vraisemblable, à défaut d'être prouvée ; considèrent de manière plus générale que les possibilités technologiques actuelles permettent aux États et aux organisations criminelles d'intercepter les communications à grande échelle ; considèrent qu'une telle pratique est un moyen adéquat pour entrer dans le potentiel scientifique et économique du pays.

Le Comité R demandait que l'on donne à la Sûreté de l'État et au SGR la mission de collaborer pour recueillir des informations sur ce système, de se donner les moyens techniques et humains nécessaires pour accomplir correctement cette mission, d'adapter les moyens légaux techniques pour avoir un cadre légal afin de procéder également de manière sélective à des repérages, des écoutes et des interceptions – nous connaissons le débat sur ces matières qui, lui aussi, a été l'objet de recommandations de notre commission de l'Intérieur, au titre de l'efficacité des cellules antiterroristes – de disposer de moyens humains : experts externes, informaticiens, ingénieurs, etc., et d'envisager la mise en place d'un service chargé d'apporter une solution à l'ensemble de la problématique de la sécurisation de l'information.

*het geheel van de problematiek van de beveiliging van de informatie.*

*Wij hebben dan beslist om zelf een verslag op te stellen. Ook het Europees Parlement heeft een verslag opgesteld en wij hebben het daarin gevolgd. Wij hebben de opdracht voor de begeleidingscommissie niet beperkt tot het onderzoek naar Echelon, wij hebben ook oog gehad voor andere systemen.*

*Hoe zijn wij te werk gegaan? Wij hebben getracht om meer inlichtingen in te winnen over International Law Enforcement Telecommunications Seminars. Deze seminaries vinden plaats sinds 1993 en onderzoeken hoe de diensten voor Law Enforcement – de politiediensten in de Amerikaanse betekenis van de term, dit wil zeggen de diensten belast met de toepassing van de wet – hun ervaring op informele wijze kunnen bundelen om een stelsel van normen uit te werken voor het gebruik van apparatuur, zodat in goede technologische omstandigheden en zonder al te veel kopzorgen over de wettelijkheid kan worden samengewerkt. Aangezien de technologie zich veel sneller ontwikkelt dan de wetgeving, waren er voldoende gronden om op een gegeven ogenblik aan deze werkzaamheden deel te nemen.*

*Wij willen de discussies van die seminaries uitdiepen en conclusies trekken uit de aanbevelingen van het Comité I en uit de werkzaamheden van het Europees Parlement. De Senaat en de Kamer hebben aan de heer Van Parys en aan mijzelf het vertrouwen geschonken voor het opstellen van het verslag. Wij hebben de leden van deze assemblee ontvangen, de eerste minister en mevrouw Timmermans. Vervolgens hebben wij samen met de heer Campbell het verslag besproken dat hij heeft opgesteld. Ik heb persoonlijk de heer Paque ontmoet, die in Frankrijk belast was met dezelfde problematiek. Wij hebben ook een aantal juristen ontmoet en de voorzitter zelf heeft deelgenomen aan de werkzaamheden van het Europees Parlement.*

*Ik zal de technische gegevens uit het verslag van het Europese Parlement hier niet opnieuw behandelen. Daarover is al genoeg gezegd, maar ik wil toch in herinnering brengen dat wij in de loop van onze werkzaamheden werden geconfronteerd met de noodzaak om een en ander technisch uit te diepen teneinde goed te begrijpen waarover men het nu precies heeft, en om komaf te maken met de zogenaamd systematisch anti-Amerikaanse gevoelens, zodat we ons een zo objectief mogelijk beeld kunnen vormen van wat er op het spel staat.*

*Waarin bestaat het systeem-Echelon? Wij zijn uitgegaan van richtlijn nr. 6 van het Amerikaanse ministerie van Defensie die de bevoegdheid en de functies vastlegt van de National Security Agency en van de Central Security Service.*

*De NSA wordt omschreven als de structuur die verantwoordelijk is voor de opdrachten inzake Signals Intelligence (SIGINT). Ze moet zorgen voor veilige communicatiesystemen voor alle overheidsorganen, in het bijzonder voor het ministerie van Defensie. 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)*

Nous avons alors décidé de rédiger nous-mêmes un rapport. Le Parlement européen ayant également élaboré un rapport, nous avons accompagné la démarche de ce dernier en la matière. Dans le mandat donné à la commission du suivi, nous ne nous sommes pas bornés à examiner Echelon mais nous nous sommes également penchés sur d'autres systèmes.

Comment avons-nous procédé ? Nous avons essayé d'obtenir davantage d'informations sur les *International Law Enforcement Telecommunications Seminars*. Ces séminaires, qui ont lieu depuis 1993, examinent comment les services de *Law Enforcement*, qui sont les services de police au sens américain du terme, à savoir de mise en œuvre de la loi, peuvent mettre de façon informelle leurs expériences en commun pour aboutir à des configurations de normes d'utilisation d'appareils qui permettent de collaborer dans de bonnes conditions technologiques sans trop s'inquiéter du volet légal. La technologie allant beaucoup plus vite que la législation, on peut considérer comme fondé d'avoir opté à un moment donné pour une participation à ces travaux.

Nous souhaitions approfondir ce qui s'était dit dans ces séminaires et tirer des conclusions de ce que nous disait le Comité R et de ce que nous savions des travaux du Parlement européen. Le Sénat et la Chambre ont confié à M. Van Parys et moi-même la rédaction du rapport de nos travaux. Nous avons reçu les membres de cette assemblée, le premier ministre et Mme Timmermans. Nous avons ensuite, avec lui-même, examiné le rapport de M. Campbell. J'ai personnellement vu M. Paque qui était chargé de la même question en France. Nous avons également rencontré un certain nombre de juristes et vous-même, monsieur le Président, avez participé aux travaux du Parlement européen en la matière.

Je ne redirai pas l'ensemble des éléments techniques figurant dans le rapport du Parlement européen. On en a suffisamment parlé à ce stade, mais il faut sans doute rappeler que dans toute l'évolution de ce travail, nous avons été confrontés à la nécessité de réaliser un approfondissement technique pour essayer de bien comprendre de quoi il est question quand on parle de cette matière et d'éliminer quelque peu les sentiments qui seraient systématiquement anti-américains dans tel ou tel domaine, de façon à avoir une vue la plus objective possible de ce que représente cet enjeu important.

En quoi consiste le système Echelon ? Nous sommes partis de la directive nº 6 du ministère américain de la Défense qui fixe la compétence et les fonctions de la *National Security Agency* et du *Central Security Service*.

La NSA est définie comme la structure responsable de missions en matière de *Signals Intelligence* (SIGINT). Elle veille à fournir des systèmes de communication sûrs à tous les organismes publics, en particulier au ministère de la Défense. Le CSS est chargé de l'exécution de ces opérations SIGINT.

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

Sur la base de directives telles que celles auxquelles il a été fait référence plus haut, en particulier la 6, la NSA et le CSS ont donc créé, aux États-Unis, le *United States Signals*

*omvat.*

*Op grond van richtlijnen zoals die waarnaar hierboven werd verwezen, meer in het bijzonder richtlijn 6, hebben de NSA en de CSS in de Verenigde Staten het United States Signals Intelligence System uitgebouwd. De inlichtingen over dat systeem beginnen sinds enkele jaren verspreid te geraken.*

*Globaal genomen kan men stellen dat vele landen, afhankelijk van hun financiële middelen, van de 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, in Australië en Nieuw-Zeeland zijn dat respectievelijk het Defence Signals Directorate en het Government Communications Security Bureau.*

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

*Het ligt voor de hand dat de moderne technologie voor het volgen en opsporen van telecommunicatie altijd een militair doel heeft gehad, maar – zo blijkt althans uit het verslag – van langsom meer een burgerlijk en economisch doel krijgt. Het Echelon-onderscheppingssysteem vindt zijn oorsprong in een Brits-Amerikaans pact, het zogenaamde 'UK-USA Security Agreement' dat waarschijnlijk dateert uit 1948, vlak na de oorlog. Wij kennen er nog steeds de precieze inhoud niet van, maar weten dat Canada, Nieuw-Zeeland en Australië er zich later bij hebben aangesloten.*

*Aangezien de Verenigde Staten en Engeland nog steeds niet beslist hebben het pact te publiceren, is er nog niets van de inhoud geopenbaard. Het gaat wel degelijk om een samenwerkingsverdrag inzake Signals Intelligence.*

*Onze eerste taak bestond erin na te gaan of er een onderscheppingssysteem bestond. Zoiets bewijzen is uiteraard bijzonder moeilijk. De begeleidingscommissies zijn geen academische instellingen die hun besluiten enkel op wetenschappelijke bewijzen steunen. Op grond van de documenten die zij hebben onderzocht, en van de getuigen die zij hebben gehoord, gaan zij ervan uit dat het onderscheppingssysteem Echelon wel degelijk bestaat. Volgens alle getuigen die wij hebben gehoord, behoort de Signals Intelligence in de Verenigde Staten en het Verenigd Koninkrijk tot de wettelijke opdracht van officiële organen. De uitoefening van deze activiteiten is onderworpen aan een gedetailleerde regelgeving en op de overheidsinstellingen die er zich mee inlaten, wordt soms toezicht uitgeoefend door het Parlement. Dat is alleszins het geval in de Verenigde Staten, waar verslag dient te worden uitgebracht, en ook in Groot-Brittannië, waar het parlementaire toezicht evenwel nogal zwak is.*

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

*Intelligence System*, qui est ce dont nous parlons. Les informations relatives à ce système commencent à être diffusées depuis quelques années.

D'une manière générale, on peut dire qu'un grand nombre de pays, en fonction de leurs moyens financiers 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) ; en Australie et en Nouvelle-Zélande il s'agit respectivement du *Defence Signals Directorate* et du *Government Communications Security Bureau*.

L'article 44 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 prévoit que notre propre service de renseignement 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.

Il est donc clair que, depuis toujours, l'ensemble de ces éléments qui permettent de suivre et de tracer tout ce qui se base sur ces nouvelles technologies, a été un objectif militaire et – c'est ce que le rapport démontre – de plus en plus civil et économique.

Si l'on remonte à l'origine du système d'interception Echelon, on le trouve dans un pacte, à l'origine anglo-américain, dénommé « *UK-USA Security Agreement* » daté vraisemblablement de l'immédiat après-guerre, en 1948, dont on n'a toujours pas une connaissance très précise et auquel se sont ajoutés le Canada, la Nouvelle-Zélande et l'Australie.

On ne dispose toujours pas de révélations sur ce contenu, les États-Unis et l'Angleterre n'ayant toujours pas décidé de le publier. Il s'agit bel et bien d'un pacte qui porte sur une coopération en matière de *Signals Intelligence*.

Notre première tâche consistait à vérifier l'existence d'une interception des communications internationales. Fournir une preuve de ce genre est évidemment plus que difficile. En effet, les commissions de suivi ne sont pas des institutions académiques qui n'arrivent 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. Selon l'ensemble des témoins que nous avons entendus, les États-Unis et le Royaume-Uni ont des organismes officiels dont les activités de *Signals Intelligence* constituent la mission légale. L'exercice de ces activités est réglé en détail et les activités de ces organismes publics sont parfois soumises à un contrôle parlementaire, en tout cas aux États-Unis, qui fait l'objet d'un rapport. C'est également le cas en Grande-Bretagne, quoique le contrôle parlementaire y soit assez faible.

Les activités SIGINT nécessitent l'utilisation d'installations d'interception qui sont certes entourées de la discrétion voulue mais dont l'existence ne peut pas être niée. 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.

*wetgeving van een ander land. SIGINT heeft immers per definitie betrekking op internationale communicatie.*

*Het is voor ons dan ook duidelijk dat het bestaan van Echelon erkend is en dat de omvang van de diensten die deze activiteiten materieel organiseren ook een tastbaar bewijs is van het belang ervan. We hebben dan ook geprobeerd na te gaan in welke mate het systeem wettig of onwettig is.*

*Door de uitgebreide media-aandacht zijn de meest uiteenlopende opvattingen ontstaan over de aard van Echelon. We kunnen wel zeggen dat het een geïntegreerd internationaal netwerk is waarvan de verschillende stations worden bediend door de vijf landen die deel uitmaken van UKUSA. De benaming Echelon wordt echter niet door alle UKUSA-landen gebruikt.*

*Het systeem maakt gebruik van op de grond geplaatste antennes om de neerwaarts gerichte stralenbundel van commerciële satellieten op te vangen en de signalen te bewerken met het oog op het vergaren van inlichtingen.*

*We schatten dat ongeveer een dertigtal andere landen thans over een belangrijke SIGINT-capaciteit beschikken. Het woord Echelon wordt gebruikt in de tekst van het UKUSA-akkoord. In de omschrijving van de opdrachten en de taken van de 'Naval Security Group Activity', die in Virginia is gevestigd, lezen we dat het gaat om het in stand houden en operationeel maken van een Echelonsite. Dat is waarschijnlijk de enige precieze plaats waar die tekst wordt aangehaald. Het is ook van daaruit dat het geheel van de informatieverzameling zich heeft ontwikkeld.*

*Uit de teksten van die 'Naval Security Group' waarop wij ons hebben gebaseerd, blijkt duidelijk dat de Amerikaanse militaire eenheden die belast zijn met een Echelon-opdracht zich bezighouden met dat soort interceptie. Dat wordt bevestigd in het verslag van de heer Campbell.*

*Er bestaan nuanceverschillen in het gebruik van het woord Echelon, vooral omdat het een soort referentiewoord geworden is dat enigszins het kader overschrijdt waarin het in de wetteksten wordt gebruikt.*

*De begeleidingscommissies komen tot de conclusie 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 geprogrammeerde trefwoordenlijsten die worden opgesteld door elke dienst afzonderlijk.*

*Wat doet het Echelon-netwerk? De ligging van alle grondstations is bekend en bekendgemaakt, inzonderheid dankzij het verslag van de heer Campbell en de hoorzitting met hem.*

*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.*

*Verschillende ontwikkelingen hebben het onderscheppen van communicaties ernstig bemoeilijkt: het toenemend gebruik van glasvezelkabels, waardoor op bepaalde plaatsen van de*

Il est donc clair pour nous que l'existence d'Echelon est reconnue et que l'ampleur des services qui organisent matériellement ses fonctions est évidemment aussi une preuve tangible de son importance. Nous avons donc essayé d'en mesurer le caractère légal ou illégal.

Que fait le système Echelon dans l'ensemble de cette activité de Signals Intelligence ? Du fait de l'attention que les médias lui ont accordé, diverses informations ont circulé sur la nature de ce système et l'on pourrait dire qu'Echelon est un réseau international intégré dont les différentes stations sont gérées par les cinq pays du pacte UKUSA, élargi Commonwealth.

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 sur terre pour traiter ces signaux en vue de réunir des renseignements.

Rappelons que nous estimons maintenant à une trentaine les autres pays qui disposent également d'une capacité de cette nature en « signals intelligence ». Le mot « Echelon » est utilisé dans le corps du texte « UKUSA Agreement ». Dans la définition des missions et des fonctions du « Naval Security Group Activity », basé en Virginie, on peut lire qu'il s'agit de maintenir et de rendre opérationnel un site Echelon. C'est vraisemblablement le seul endroit précis où l'on cite ce texte et c'est à partir de là que l'ensemble des informations ont été développées.

Il ressort clairement des textes de ce « Naval Security Group », sur lesquels nous avons travaillé, que les unités militaires américaines chargées d'une mission Echelon effectuent des interceptions de ce type. Le rapport de M. Campbell, que nous avons reçu, le confirme.

Il y a des nuances dans l'emploi du terme « Echelon », notamment aussi parce qu'il et devenu une sorte de mot de référence qui dépasse un peu le cadre dans lequel il est utilisé dans les textes légaux.

Les commissions de suivi concluent que le mot fait référence à l'utilisation d'ordinateurs puissants qui filtrent automatiquement des messages Comsat captés et transmettent le résultat des filtrages aux services concernés des cinq pays participants à cet accord, le filtrage étant effectué sur la base de listes de mots-clés établies indépendamment par chaque service.

Que fait ce système Echelon ? L'ensemble des implantations des stations terrestres sont aujourd'hui connues et publiées, notamment par le même rapport Campbell et dans l'audition de ce dernier.

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

Plusieurs développements ont considérablement compliqué la captation des communications. Tout d'abord, l'utilisation croissante des câbles en fibre de verre qui supposent, à certains endroits du câble, une technique d'écoute adaptée à la technologie, des progrès énormes réalisés dans les systèmes de cryptage et la croissance explosive du volume des

*kabel de afluistertechniek moet worden aangepast aan de technologie; de enorme sprong inzake de ontwikkeling van encryptiesystemen; de explosieve groei van het volume van de internationale communicaties. Hoe groter het aantal internationale communicaties, hoe lager het percentage interessante onderscheppingen.*

*Inzake de evaluatie van het Echelonsysteem hadden de meeste vragen die in het Europees parlement en de verschillende Europese nationale parlementen werden gesteld, betrekking op het ogenschijnlijke 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.*

*De Verenigde Staten en de andere UKUSA-landen verzekeren dat ze de rechten van de eigen burgers van hun land niet schenden. Ook Britse parlementsleden hebben daarover vragen gesteld. Het feit dat de rechten van de eigen burgers niet worden geschonden is duidelijk een element in het Britse rechtsstelsel. Hoe staat het echter met ons rechtsstelsel en onze bescherming?*

*Het lijkt dan ook aannemelijk dat, gelet op de bescherming van het privé-leven die door de wetten in de betrokken landen aan de eigen onderdanen wordt gewaarborgd, ook in de feiten minimale garanties worden geboden.*

*Het feit dat de regeringen in die zin officiële verklaringen hebben afgelegd, geeft ons nog geen bewijs. We kunnen wel denken dat ze ervoor zorgen dat er geen systematische inmenging zal gebeuren in de nationale vrijheden, zoals dat voor de eigen burgers is bepaald.*

*Zowel telecommunicatie- als computerbedrijven zijn betrokken bij de uitbouw van het Echelonnetwerk en het eigenlijke onderscheppingwerk. Geen enkel van die bedrijven heeft zijn klanten – bedrijven, overheden, burgers – laten weten dat hun communicaties willens en wetens onderschept werden.*

*Het bestaan van een dergelijk systeem roept allerlei vragen op, in de eerste plaats over de gevolgen 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.*

*We kunnen ons in het bijzonder vragen stellen over de rol van het Verenigd Koninkrijk in het Echelonsysteem en de verenigbaarheid ervan met zijn verbintenissen binnen de Europese Unie, zowel ten opzichte van de lidstaten als ten opzichte van het respect voor de elementaire rechten van de burgers van de andere lidstaten.*

*Onze commissie is van oordeel dat Echelon gebruikt wordt voor economische spionage. 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 verklaard dat de inlichtingendienst steunt op SIGINT-activiteit. Hij ontkende dat de inlichtingendiensten aan industriële spionage doen, maar gaf*

communications internationales. Plus grand est le nombre, plus faible est le pourcentage de captations qui se révèle intéressant.

Quant à l'évaluation du système Echelon, la plupart des questions qui ont été posées au Parlement européen et dans les divers parlements nationaux concernaient plutôt politiquement la facilité avec laquelle les services de renseignements américains, assistés par un État membre de l'UE – ce point n'étant pas sans importance pour la suite – ont pu recueillir des informations de nature économique. Le recours à cette technologie a lieu en dehors de tout cadre international légal connu.

Les États-Unis comme les autres pays du Pacte UKUSA assurent qu'ils ne violent pas les droits de leurs citoyens. Nous n'avons évidemment pas été les seuls parlementaires à poser des questions : il y en a eu au Parlement britannique. Il est clair que ne pas violer les droits de ses propres citoyens est un élément du système légal anglais mais quid de notre système et de nos protections ?

Il semble donc plausible, au vu des garanties de protection de la vie privée que les lois de ces pays assurent à leurs citoyens, qu'il existe dans les faits le respect d'un minimum de garanties.

Mais nous ne détenons pas de preuves puisque les gouvernements ont fait des déclarations officielles en ce sens. On peut alors penser qu'ils veillent à ce qu'il n'y ait pas d'intrusions systématiques dans les libertés nationales telles que définies pour les nationaux.

Des entreprises spécialisées dans les télécommunications et 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 interceptées.

On peut tout de même se poser des questions et c'est ce qu'a fait votre commission. Tout d'abord, quelles sont les répercussions pour l'Alliance atlantique ? Une partie des pays alliés espionne d'autres pays alliés sans les en informer – à moins que les séminaires ILETS aient été une façon de le faire, à moins que tout le monde ne soit informé en affirmant ne pas l'être – et sans que ces séminaires ne puissent exercer un quelconque contrôle démocratique.

Autre hypothèse : tout le monde est d'accord, dans ces milieux, pour affirmer que le contrôle démocratique est un handicap et qu'il ne doit pas être exercé. En d'autres termes, une partie de l'Alliance atlantique traite l'autre partie de la même manière qu'elle traitait l'ancien ennemi, le bloc de l'Est, ou comme elle traite des pays tels que l'Irak ou la Libye.

On peut s'interroger plus particulièrement sur le rôle du Royaume-Uni dans le système Echelon et sur la compatibilité de ce rôle avec les engagements de ce pays au sein de l'UE, tant vis-à-vis des États membres que des droits élémentaires des citoyens des autres États membres.

Utilise-t-on Echelon pour l'espionnage économique ? Notre commission a estimé que c'était le cas. Le directeur de la CIA, M. Tenet, a certes déclaré devant le House Permanent Select Committee on Intelligence, le comité permanent de

*toe dat het systeem nuttige economische informatie geeft die de beleidsmakers kunnen aanwenden in tijden van economische crisis.*

*Het kan zeer belangrijk zijn dat te weten als het gaat om bedrijven die Amerikaanse wetten of sancties schenden. Uit die vaststelling blijkt immers dat, om onderschepping van economische communicatie te verantwoorden, de Amerikaanse diensten alleen de eigen wet inroepen. Het antwoord van de CIA is dus nuttig voor binnenlands gebruik, maar geeft geen enkele verantwoording voor de schending van de beginselen van het internationale recht.*

*De voormalige CIA-directeur, James Woolsey, verklaarde eveneens dat de 'continental friends' uiteraard worden bespioneerd. Die spionage is vooral gericht op corruptie bij onze bedrijven, wat het systeem volgens de CIA verantwoordt. Daarna verklaarde Woolsey 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 tot corruptie moeten overgaan wegens de inferioriteit van hun economisch systeem ten opzichte van het Amerikaanse.*

*De CIA doet aan economische spionage om te controleren of geen technologie wordt verkocht die geschikt is voor dubbel gebruik, die dus zowel geschikt is voor commerciële exploitatie als voor militaire en paramilitaire activiteiten.*

*Het belangwekkende van dit artikel is dat het onverwacht openhartig is, zonder het gebruikelijke diplomatieke jargon. Daarbij wordt toegegeven dat de Verenigde Staten zonder scrupules de technologische middelen inzetten waarover ze beschikken om ook economische informatie te verzamelen. Economische spionage wordt dus verantwoord door het inzetten van een systeem waarvan bepaalde aspecten nuttig kunnen zijn voor de veiligheid.*

*Het verdwijnen van het Oostblok en het communistisch systeem in Oost-Europa heeft geleid tot het verdwijnen van het hoofddoel van het inlichtingenwerk en een ingrijpende heroriëntering van de activiteiten van de Amerikaanse inlichtingendiensten.*

*President Clinton heeft het vergaren van economische inlichtingen volledig geïmplementeerd door de oprichting van het Trade Promotion Coordinating Committee en het Advocacy Center, die ressorteren onder het Department of Commerce.*

*Het CIA is betrokken bij de werking van het Advocacy Center. Het is ook duidelijk dat de inlichtingendiensten betrokken zijn bij informatiegaring die verder gaat dan het opsporen van corruptie bij de concurrenten.*

*De successen die door het Advocacy Center worden behaald, namelijk 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. Elke soortgelijke Amerikaanse success story betekent echter een Europese defeat story.*

*De begeleidingscommissies menen dat de geruststellende verklaringen van de Amerikaanse en Britse autoriteiten onaanvaardbaar zijn. De interceptie van communicaties*

l'intelligence service du Sénat américain, que le service du renseignement repose sur l'activité SIGINT. Mais il a nié que les services de renseignements se livrassent à l'espionnage industriel. Il a tout de même précisé que les informations économiques utiles que l'on recueille peuvent aider les décideurs politiques en situation de crise économique. En résumé, M. Tenet a refusé d'admettre que les services de renseignements américains se livrent à l'espionnage économique mais a reconnu que ces services recueillent des informations à caractère économique.

Il peut être très important de le savoir lorsqu'il s'agit d'entreprises qui violent les lois ou les sanctions américaines. Ce constat démontre que, pour justifier l'interception des communications économiques, les services américains se basent uniquement sur leur propre législation. La réponse de la CIA est donc utile sur le plan interne, mais elle ne justifie pas la violation des principes du droit international.

L'autre directeur de la CIA, James Woolsey, qui a également été interrogé et dont l'article publié dans le Wall Street Journal a fait le tour du monde, a expliqué que, bien entendu, on espionne les « continental friends ». En effet, il est évident que cet espionnage vise en particulier des activités de corruption. « As a result you bribe a lot. », dit-il. C'est une façon précise de montrer la connaissance que la CIA peut avoir des pratiques des entreprises européennes. À l'évidence, la CIA justifie le système en expliquant qu'il lui permet de connaître des pratiques corruptrices. Selon M. Woolsey, si une entreprise européenne est surprise à pratiquer la corruption, les autorités américaines prennent contact avec celles du pays qui souhaite conclure un contrat avec cette entreprise et la dénoncent.

M. Woolsey croit savoir, en outre, que les entreprises européennes seraient obligées de se livrer à la corruption en raison de l'infériorité de leur système économique par rapport au système américain.

La CIA pratique également l'espionnage économique pour vérifier si on ne vend pas de la technologie susceptible d'avoir un double usage, qui pourrait donc servir à la fois à une exploitation commerciale et à des activités militaires ou paramilitaires, si l'on peut désigner ainsi les activités de certains groupes fondamentalistes.

L'intérêt de cet article réside dans une franchise inattendue qui ne recourt pas au jargon diplomatique habituel. Mais, surtout, il contient l'aveu non dissimulé que les États-Unis utilisent sans scrupules les moyens technologiques dont ils disposent pour recueillir des informations économiques. La question principale est qu'on justifie l'espionnage économique par un système dont certains aspects peuvent être utiles en matière de sécurité.

La disparition du « bloc de l'Est » et du système communiste en Europe orientale ont entraîné la disparition partielle de l'objectif principal du travail de renseignement et une réorientation considérable des activités des services de renseignements des États-Unis.

C'est le président Clinton qui a mis en œuvre la collecte de renseignements économiques par la création du *Trade Promotion Coordinating Committee* et de l'*Advocacy Center* qui relèvent du département du Commerce américain. Je vous renvoie au rapport écrit pour ce qui concerne les fonctions de

*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. Er wordt geen enkele parlementaire controle uitgeoefend op deze activiteit, ook niet binnen het Verenigd Koninkrijk.*

*Op grond van deze elementen komen de begeleidingscommissies 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 Amerikaanse bedrijven te bevoordelen bij het aantrekken van buitenlandse contracten. Het gaat dus wel degelijk om industriële spionage.*

*Het gebruik van de ingewonnen inlichtingen zal Europese bedrijven wellicht vele miljarden hebben doen verliezen. Deze praktijk hypothekeert de vrije handel. Het zou de moeite lonen dit voor te leggen aan de Wereldhandelsorganisatie, zodat deze kan nagaan waarvoor de ingewonnen informatie werkelijk wordt gebruikt. De Amerikanen roepen de chronische corruptie door Europese ondernemingen vooral in als voorwendsel om economische inlichtingen in te winnen.*

*De bezorgdheid van de begeleidingscommissies en van de tijdelijke commissie van het Europees Parlement wordt gedeeld door 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. Uit de meeste nota's die de CIA over de beschermingsregels heeft opgesteld, blijkt overigens 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. De vergaring is natuurlijk wel wettelijk als de betrokkenen ermee instemmen.*

*We zijn vervolgens dieper ingegaan op de kwestie van de 'International Law Enforcement Telecommunication Seminars', de ILETS. Deze techniek is volgens mij zeker niet zonder nut: op het ogenblik dat een technologie wereldwijd wordt gebruikt, is het logisch dat iedereen er gebruik wil van maken. Op het eerste gezicht was er binnen deze seminaries geen sprake van spionageactiviteiten.*

*De deelnemers waren hierover bijzonder discreet en men kan zich afvragen waarom ze niet onmiddellijk gezegd hebben dat ze samen met het FBI aan deze seminaries zouden deelnemen. Op deze seminaries kon overigens in goede omstandigheden worden samengewerkt. We hebben getracht meer over deze seminaries te vernemen.*

*Het 'ontdekken' van ILETS heeft in verschillende Europese landen wel wat stof doen opwaaien omdat de parlementaire controleorganen niet van hun bestaan op de hoogte waren.*

*De eerste vergadering had plaats in 1993 in Quantico. Daarna werden vergaderingen gehouden in Bonn in 1994, Canberra in 1995, Dublin in 1997, Ottawa in 1998 en Lyon in 1999. België neemt sinds 1994 deel aan de ILETS-seminaries. Het is de bedoeling dat gemeenschappelijke normen worden*

cet *Advocacy Center*.

Il est clair, en tout cas, que la CIA est associée au fonctionnement de l'*Advocacy Center*. Une note interne datée du 17 août 1994 révèle clairement la présence d'un agent de la CIA en son sein. Il en ressort aussi que les services de renseignements sont associés à une collecte d'informations qui va bien plus loin que le dépistage de la corruption chez les concurrents.

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 dans la rubrique *Success stories* du site web du centre. Nous citons dans le rapport un certain nombre de ces cas où des entreprises ont vainement soumissionnés. Toute *success story* américaine est évidemment aussi une *defeat story* européenne, souvent française.

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 et les pays qui subissent ce système ne peuvent aucunement la contrôler. Le parlement, même au Royaume-Uni, n'exerce aucun contrôle sur cette activité.

Les commissions du suivi ont donc conclu que les services de renseignements américains recueillaient 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 s'agit donc bien d'espionnage industriel.

L'utilisation des informations recueillies a probablement fait perdre plusieurs milliards aux entreprises européennes. Pareille pratique hypothèque la liberté des échanges commerciaux et devrait donc être soumise à l'Organisation mondiale du commerce pour qu'elle étudie l'usage réel des informations ainsi collectées. Les Américains prétextent surtout de la corruption chronique qui serait pratiquée par les entreprises européennes pour faire de l'espionnage industriel.

L'inquiétude des commissions du suivi ou de la commission temporaire du Parlement européen est partagée par les parlementaires des pays appartenant au système Echelon. Ce n'est pas étonnant en soi puisque l'existence de ces pratiques est difficilement conciliable avec les principes d'un État démocratique. La CIA reconnaît d'ailleurs dans la plupart des notes qu'elle a rédigées sur la question que les règles de protection, limitant la collecte d'informations sur les citoyens américains qui n'auraient pas donné leur autorisation, ne sont toutefois pas applicables aux personnes non citoyennes des États-Unis. Cette collecte est bien entendu un acte légal lorsque les personnes ont marqué leur accord.

Nous avons ensuite essayé d'approfondir la question des « *International Law Enforcement Telecommunications Seminars* », les ILETS. À mes yeux, cette technique est loin d'être inutile : à partir du moment où la technologie acquiert une vocation mondiale, il est logique que chacun souhaite pouvoir être connecté. Les ILETS traitent de cette question. À

*vastgelegd met betrekking tot de aanwending van deze technologieën.*

*Tijdens de ILETS-vergadering van 1998 werd besloten de 'Law Enforcement Requirements for the Surveillance of Electronic Communications' goed te keuren. Deze nieuwe regels werden als ENFOPOL 98 voorgesteld en bevatten niet alleen bepalingen over interceptie, maar ook omtrent versleuteling. Het is de bedoeling deze regels als een resolutie van de Raad over te nemen.*

*De ILETS worden door de Amerikaanse 'Law Enforcement'-diensten gebruikt om hun technologische visie aan de Europese politie- en inlichtingendiensten op te dringen. Geen enkel parlement werd over deze seminaries geïnformeerd.*

*Moeten technische voorschriften worden opgelegd aan de producenten of aan de informatica- en telecommunicatieoperatoren? Zullen we na een debat binnen de parlementen van de lidstaten van de Unie, beslissen gemeenschappelijke normen, namelijk de Amerikaanse, te aanvaarden?*

*Een soortgelijk debat is overigens al aan de gang over Galileo.*

*De begeleidingscommissies vragen zich af of een betere werking van de politie- en inlichtingendiensten niet veeleer als voorwendsel wordt gebruikt voor een andere scenario waarvan we de indruk hebben dat we het al eens meemaakten. Op deze seminaries hebben de mogelijke gebruikers van technieken die in hun land wettelijk niet veroorloofd zijn, elkaar gevonden rond een technologie die volledig door de Amerikanen wordt gedomineerd.*

*We hebben de systemen in andere landen geanalyseerd. In Frankrijk gebruikt het Commissariat à l'énergie atomique een supercomputer voor de ontcijfering van versleutelde informatie. Wellicht vreest Frankrijk economische concurrentie en is dat de reden waarom het nogal lauw heeft gereageerd op het Amerikaanse Echelon.*

*Nederland heeft een afluisterstation in de provincie Groningen.*

*Duitsland is een interessant geval omdat de Duitse inlichtingendienst eveneens informatie kan onderscheppen. Het Duits Grondwettelijk Hof heeft een onderzoek ingesteld naar de Duitse afluisterpraktijken. Tijdens het proces 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, met name verbindingen van vreemdelingen of buitenlandse firma's met het buitenland, met daarnaast 2.000 zoekbegrippen inzake proliferatie, 1.000 zoekbegrippen over wapenhandel, 500 over terrorisme en 400 over drugshandel.*

*Volgens Duncan Campbell beschikt de BND over een basis in de Volksrepubliek China, op Taiwan en in Frans-Guyana. Zowel de basis in Kourou als op Mayotte worden door de DGSE en de BND samen geëxploiteerd.*

*Over Zwitserland weten we niet veel, maar het zou wel samenwerken met de Verenigde Staten en het Verenigd Koninkrijk.*

*Rusland beschikt zeker over een wereldwijd interceptiesysteem. De Russische inlichtingendienst FAPSI*

première vue, il n'y a pas eu d'activités d'espionnage organisé au sein de ces séminaires.

Ceux-ci ont été l'objet d'une étonnante discrétion. On peut se demander pourquoi les participants n'ont pas dit tout de suite qu'ils allaient prendre part à ces séminaires avec le FBI – ce n'était en effet pas la seule activité organisée avec le FBI. En outre, ces séminaires permettaient de travailler ensemble et dans de bonnes conditions. Nous avons essayé d'en savoir davantage à ce sujet et de briser cette logique du silence. La découverte de ces séminaires a provoqué des remous dans plusieurs pays européens car les instances de contrôle parlementaire n'étaient pas du tout au courant de leur existence.

La première réunion a eu lieu en 1993 à Quantico, principal lieu de travail du FBI. Les réunions suivantes se sont tenues à Bonn, en 1994 – on voit clairement quel était le principal allié à l'époque –, puis à Canberra en 1995, à Dublin en 1997, à Ottawa en 1998 et à Lyon en 1999. Nous n'avons commencé à participer à ces séminaires qu'en 1994, donc, nous ne faisions pas partie des « vrais copains », mais nous y avons été rapidement associés, dès la réunion de Bonn. Ces séminaires donneront lieu à la définition de normes communes en matière d'utilisation des technologies.

Au cours de la réunion ILETS de 1998, il a été décidé d'adopter les « *Law Enforcement Requirements for the Surveillance of Electronic Communications* », présentés dans un texte européen, ENFOPOL 98, qui constituent une avancée dans la définition de règles normales, non seulement en matière d'interception mais également en ce qui concerne le cryptage, et doivent permettre de passer le cap d'une résolution du Conseil européen. On a beaucoup plaisanté sur le fait que ces résolutions passaient en point A – « Acceptation automatique » – dans des conseils techniques où ces points ne sont pratiquement jamais considérés comme des points politiques importants.

Il est évident que pour les services américains, plus particulièrement pour le « *Law Enforcement* », ces séminaires sont une manière d'imposer leur vision technologique aux services de police et aux services de renseignement européens. Aucune assemblée nationale n'a été informée de ces séminaires.

Faut-il imposer des prescriptions techniques aux producteurs ou aux opérateurs de communications informatiques ou de télécommunication ? Dans quelle mesure, après un débat au sein des Parlements des États membres de l'Union, peut-on réellement décider d'adopter soit des normes communes, soit les normes américaines ?

Le débat est d'ailleurs en pleine répétition pour Galileo puisque nous avons eu dans cette même salle un débat calqué sur ce type de situation, selon que l'on choisit la formule américaine ou que l'on essaye de définir, pour Galileo, des normes européennes pour le matériel.

Les commissions de suivi se demandent si une meilleure exécution des missions de police ne sert pas plutôt de prétexte à un tout autre scénario auquel nous avons le sentiment d'avoir assisté. En quelque sorte, ces séminaires ont permis de mettre ensemble, sur une base technologique complètement dominée par le partenaire américain, des utilisateurs et des partenaires possibles pour des techniques qui contrevenaient

*(Federal Agency of Government Communications and Information) beschikt over een indrukwekkende analysecapaciteit.*

*We maken deel uit van een wereldwijd vertakt inlichtingensysteem waardoor de wetgeving op de bescherming van de privacy en op de economische concurrentie kan worden omzeild.*

*Noorwegen heeft waarschijnlijk met de Verenigde Staten en Groot-Brittannië een akkoord afgesloten.*

*Nadat we economische spionage en de law enforcement-seminaries met de Verenigde Staten en de systemen in een aantal andere landen hadden bestudeerd, hebben we de minister van Justitie gehoord. Zijn uiteenzetting is op dit ogenblik wat achterhaald en we hopen dat hij ons actuele informatie zal willen verstrekken. We hebben ook de eerste minister en de minister van Landsverdediging gehoord.*

*Tijdens de gedachtewisseling is gebleken dat België eerst de steun van andere lidstaten moet trachten te vinden vooraleer we een actie op het niveau van de Unie ondernemen.*

*Er zijn niet zoveel Europese landen die zich inzake interceptie neutraal opstellen. Precies daarom kan België wellicht een kritische houding aannemen. We hebben de eerste minister nogmaals uitgelegd dat de passiviteit van de Belgische inlichtingendienst ons verbaast.*

*Vervolgens hebben we de juristen gehoord: de heer Thomas voor de Commissie voor de bescherming van het privé-leven en de heer Yernault over de juridische aspecten van het interceptiesysteem.*

*De Commissie voor de bescherming van de privé-levenssfeer heeft het initiatief genomen voor een debat over deze kwestie. Volgens de Commissie staat de algemene en verkennende aard van het onderscheppen van boodschappen haaks op de beginselen van zowel het nationale als het internationale recht die een dergelijk grootschalig toezicht verbieden. Volgens de wet van 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, mogen die gegevens niet worden gebruikt op een wijze die onverenigbaar is met de doeleinden.*

*Op Europees niveau gaat het algemeen en verkennend toezicht op de telecommunicatie in tegen inzonderheid de beginselen vervat in het Europees Verdrag tot 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. De besprekingen met de juridische experts hebben uitgewezen dat afluisterpraktijken volgens het EVRM slechts geoorloofd zijn als drie voorwaarden samen zijn vervuld: de wettigheid, de legitimiteit en de noodzakelijkheid. Welnu, dit is niet het geval.*

*Het Hof heeft geoordeeld dat de wettigheidsvoorwaarde niet werd vervuld. Vermits interceptie alleen legitiem is als welbepaalde doeleinden worden nagestreefd, is algemene interceptie natuurlijk onaanvaardbaar behalve als we zouden aannemen dat onze samenleving ten onder gaat en we dus alles moeten afluisteren. Het noodzakelijkheidsprincipe is essentieel in een democratische samenleving. De juristen hebben verwezen naar het arrest-Klass en we hebben getracht op basis daarvan te bepalen wat een Staat zich zou kunnen* aux circonstances légales dans leur pays d'origine.

Nous avons fait l'analyse des systèmes existant dans d'autres pays. Pas besoin de vous dire que cela existe en France également ; pas de source officielle en France non plus mais nous en avons longuement parlé. Le Commissariat à l'énergie atomique utilise un super ordinateur qui sert au décryptage des communications cryptées. C'est probablement la raison pour laquelle la France a réagi avec tiédeur au fait que les *success stories* américains sont souvent destinées à vaincre sur des marchés pour lequel le concurrent principal est français.

Les Pays-Bas sont aussi dotés d'une capacité située dans la province de Groningen.

L'Allemagne est un pays plus intéressant encore dans la mesure où le système de renseignement allemand est aussi performant en matière d'interception des communications. L'ensemble des systèmes allemands a fait l'objet d'une enquête par la Cour constitutionnelle allemande. Lors du procès, 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, notamment les contacts d'étrangers ou de firmes étrangères à l'étranger, auxquels s'ajoutent 2000 termes de recherche en matière de prolifération, 1000 autres sur le trafic d'armes, 500 sur le terrorisme et 400 sur le trafic de stupéfiants.

Selon M. Campbell, le BND dispose d'une base en République populaire de Chine, à Taiwan et en Guyane française – partagée avec la DGSE – à Kourou. Tant la base de Kourou que celle de Mayotte sont exploitées conjointement par la DGSE et le BND.

On ne sait pas grand chose sur la Suisse mais, visiblement, il y a une collaboration, dont la nature n'est pas précisée, avec les États-Unis et le Royaume-Uni.

La Russie dispose certainement d'un système d'interception de portée mondiale. La FAPSI – *Federal Agency of Government Communications and Information* – dispose d'une capacité d'analyse très réelle.

Nous nous trouvons devant un système du renseignement capable d'entrer dans ce monde interconnecté. C'est aussi une façon de ne pas appliquer une série de législations avec plus ou moins de respect pour la protection de la vie privée, d'une part, et de la compétition commerciale, d'autre part.

La Norvège : c'est aussi un accord particulier, vraisemblablement avec les États-Unis et la Grande-Bretagne.

Une fois acté, d'une part, ce volet certain de l'espionnage économique et, d'autre part, le contenu des séminaires de *law enforcement* avec les États-Unis et l'existence dans d'autres pays importants de ces systèmes, nous avons entendu le ministre de la Justice. Le contenu de cette audition est un peu démodé de sorte que nous espérons qu'il voudra actualiser ce qu'il nous a dit à l'époque. Nous avons aussi entendu le premier ministre et le ministre de la Défense.

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

Les pays européens vraiment neutres sur la question des

*veroorloven. Het zou interessant zijn te weten of we procedures moeten opstarten en zo ja, welke.*

*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. Een Staat blijft dus verantwoordelijk als hij een interceptiestation op zijn grondgebied toelaat. Volgens het internationaal recht blijft een Staat verantwoordelijk voor de daden van zijn instellingen, ook als deze zich buiten het nationale territorium bevinden.*

*Wat het concept territoriale veiligheid betreft, zijn we juridisch dus voldoende gewapend om de verantwoordelijkheden vast te leggen als een dergelijke situatie zich zou voordoen.*

*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.*

*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. Moeten bijvoorbeeld alle rechtsmiddelen worden uitgeput in Groot-Brittannië of in Duitsland voor Bad Aibling, dat binnenkort wordt gesloten? Onze juridische experts gaven ons drie redenen om dat niet te doen en rechtstreeks naar het Hof te stappen. Alleen de interne rechtsmiddelen die efficiënt zijn, dat wil zeggen die de aangevoerde schending kunnen verhelpen en die toegankelijk zijn, moeten worden uitgeput.*

*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 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.*

*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*

interceptions de communications ne sont pas légion. C'est sans doute une des raisons pour lesquelles c'est peut être en Belgique que l'on peut faire l'analyse critique la plus approfondie. Nous avons répété au premier ministre à quel point nous étions étonnés de la passivité des services belges de renseignements face à cette problématique.

Nous avons alors entendu des juristes, M. Thomas, pour la commission de protection de la vie privée, et M. Yernault, qui est venu nous parler d'une analyse des aspects légaux de ces activités d'interception.

La commission de protection de la vie privée a pris l'initiative d'un débat sur cette question. Selon la commission, le caractère général et exploratoire des interceptions se heurte aux principes de droit national et international qui proscrivent une telle surveillance à grande échelle. En vertu de la loi de 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.

Au niveau européen, une surveillance à caractère général et exploratoire des télécommunications va à l'encontre des principes de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 et contrevient à l'interprétation de l'article 8 de la convention de la Cour européenne des droits de l'homme. La discussion avec les experts juridiques a montré que pour plusieurs aspects de ces législations, en particulier pour la CEDH, les trois conditions cumulatives qui permettent l'exception d'écoute, c'est-à-dire la légalité, le principe de légitimité et le principe de nécessité dans une société démocratique, ne peuvent être considérées comme étant remplies.

La longue démonstration juridique contenue dans le rapport établit que la Cour a jugé que la condition de légalité n'était pas remplie. Par ailleurs, la légitimité devant être démontrée par rapport à une cible précise, les interceptions globales sont évidemment inacceptables, sauf à admettre que nous vivrons toujours dans une société qui aurait vocation à dégénérer et que, par conséquent, il faut tout écouter. Quant au principe de nécessité, il est tout aussi substantiel dans une société démocratique. Les juristes ont fait référence à l'arrêt Klass et nous avons essayé, à travers cette convention, d'arriver à déterminer ce qu'un État pourrait faire. À cet égard, il serait intéressant de savoir s'il faut entamer des procédures et, le cas échéant, d'en préciser la nature.

Un État peut donc être tenu responsable d'une violation de la convention européenne des droits de l'homme s'il met son territoire à disposition d'un autre État, ce dernier perpétrant des actes équivalant à une violation. Un État engage sa responsabilité propre quand il accueille une station d'interception, par exemple. Au regard du droit international, un État demeure responsable des agissements de ses organes, y compris lorsque ceux-ci se déploient en dehors du territoire national.

Je pense donc que par rapport au concept de sécurité territoriale, il est bien clair qu'il y a maintenant suffisamment de *background* juridique au niveau de l'application de cette convention pour estimer que les responsabilités pourraient être établies si une action était entamée.

Quand bien même, ce que semblent indiquer les réponses du gouvernement britannique, la cogestion de la base de

*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. Dit element is essentieel omdat het de mogelijkheid van een directe rechtsvordering duidelijk maakt. Dat is zeker één van de conclusies van onze werkzaamheden.*

*Zowel het algemeen internationaal recht als het internationaal en Europees 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.*

*We hebben ook het gemeenschapsrecht zorgvuldig onderzocht. We hopen dat de Belgische regering terzake een duidelijke koers zal bepalen. Het EVRM is één element. De tweede pijler van de juridische argumentatie van de commissie is gebaseerd op het gemeenschapsrecht met betrekking tot communicatieafluistersystemen. De conclusies zijn zeer duidelijk.*

*De begeleidingscommissies komen tot de conclusie dat een interceptiesysteem dat, vanuit het buitenland, private telecommunicatie onderschept die via satelliet van en naar België komt, strijdig is met het gemeenschapsrecht in de mate dat het voor economische spionage wordt gebruikt; deze schending geldt zowel voor de landen die zelf telecommunicatie onderscheppen als voor de landen die hun grondgebied ter beschikking stellen voor intercepties door derde landen.*

*We vermelden dan de artikelen van de richtlijnen op basis waarvan een rechtsvordering kan worden ingesteld. We vinden dat die interceptie een bedreiging vormt voor de verwezenlijking van de doelstellingen van het EG-verdrag, namelijk het vrije verkeer van goederen, personen, diensten en kapitaal. Het is een schending van artikel 10 van het EG-verdrag dat de lidstaten de verplichting oplegt zich te onthouden van alle maatregelen welke de verwezenlijking van die doelstellingen in gevaar kunnen brengen.*

*We vinden bovendien dat het systeem in strijd is met verschillenden bepalingen van het EVRM.*

*Wat de strijdigheid met het EG-verdrag betreft, zal de minister misschien opwerpen dat de Verenigde Staten daarbij geen partij zijn, maar Groot-Brittannië is dat wel. De commissie wenst dat zou worden nagegaan of artikel 10 van het verdrag fair wordt toegepast.*

*Tot slot kom ik tot de aanbevelingen van onze commissie. Met deze aanbevelingen kan de regering niet doen alsof er geen tekst bestaat waarin op gedetailleerde wijze wordt aangegeven welke juridische bepalingen worden geschonden. De commissie hoopt dat haar aanbevelingen aanleiding zullen geven tot een gemeenschappelijke actie en dat 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.

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. Faudrait-il épuiser toutes les voies d'action, par exemple, en Grande-Bretagne ou en Allemagne, pour Bad Aibling qui est en phase de fermeture ? Nos experts juridiques nous ont signalé trois raisons de ne pas épuiser les recours des États participant à Echelon et d'aller directement devant la Cour. Ne doivent être épuisés que les recours internes qui sont effectifs, c'est-à-dire qui permettent de redresser la violation alléguée, et accessibles.

L'Allemagne, par exemple, invoquant la confiance germano-américaine, ne contrôle pas à partir de la base en question – c'est sans doute la raison de sa prochaine fermeture – si la NSA écoute ou non les entreprises et citoyens allemands. 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 de démentir son implication dans Echelon ?

Le même raisonnement peut être tenu à propos du Royaume-Uni en raison de son manque de vigilance 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.

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. Cet élément est essentiel puisqu'il dégage la possibilité d'une action en ligne directe. C'est certainement une des conclusions de nos travaux.

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 Echelon. Ils concernent également tous les systèmes,

*regering met betrekking tot elk van de aanbevelingen een standpunt zal bepalen.*

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. Echelon n'est que la partie visible de l'iceberg.

Nous avons alors examiné tout aussi minutieusement le droit communautaire. Nous espérons vivement que le gouvernement belge prendra une orientation précise en la matière. Le volet de la CEDH est un élément ; le deuxième pilier de la démonstration juridique de la commission porte sur le droit communautaire pour les systèmes d'écoute de communications. Les conclusions sont particulièrement précises.

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, 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.

Nous vous citons alors de manière très précise les articles des directives concernées qui permettraient d'entamer une action. Nous considérons tout autant, au terme des travaux de la commission, que cette interception menace la réalisation des buts du Traité de l'Union européenne, 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, lequel impose aux États membres de s'abstenir de toute mesure susceptible de mettre en péril la réalisation de ces buts.

Bien entendu, nos conclusions portent également sur le volet que je viens de vous lire et nous considérons également que le système porte atteinte à diverses dispositions de la Convention européenne des droits de l'homme.

Je vous répète, monsieur le ministre, que, selon nous, ces pratiques sont contraires au droit communautaire, dans la mesure où l'espionnage économique est l'intérêt essentiel, et nous vous citons les directives sur lesquelles la Belgique peut se fonder. En outre, ces pratiques sont inacceptables au regard de l'article 10 du traité.

Vous m'objecterez que les États-Unis n'ont pas signé le moindre traité de l'Union européenne mais la Grande-Bretagne l'a fait. Il convient de vérifier le caractère *fair* ou non de l'application de l'article 10 du traité. Tel est le souhait de la commission.

Pour conclure, j'en viens aux recommandations de notre commission. Ces recommandations ne pourront pas permettre au gouvernement de feindre d'ignorer qu'un texte a précisé, avec beaucoup de détails, quels étaient les éléments juridiques auxquels il était contrevenu. Ne pas agir est, à cet égard, à la limite de l'action. À partir du moment où nous souhaitons que nos recommandations ne restent pas purement amicales mais donnent lieu à un travail en commun, nous espérons que le gouvernement arrêtera une position sur chacune de ces recommandations.

*De commissie beveelt 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. *zoals gevraagd door de ADIV, het algemene voorzorgsprincipe toe te passen bij het uitstippelen van een wereldwijd en gecentraliseerd beleid ter beveiliging van de communicatie;*

3. *aan de Veiligheid van de Staat en de ADIV de nodige technische en personeelsmiddelen te verschaffen om alle informatie in te winnen betreffende ieder gevaar van onderschepping van berichten ten nadele van België;*

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; – het debat over deze aanbeveling kan veel ruimer zijn dan de loutere analyse van het Echelon-systeem –*

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, met andere woorden te zorgen voor deskundigen die de daden van hackers kunnen controleren;*

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. *een evolutie na te streven naar grotere compatibiliteit en uitwisselbaarheid van informatie tussen de inlichtingendiensten om zo het systeem van bilaterale uitwisseling af te schaffen dat niet meer is aangepast aan de huidige situatie waarbij nationale veiligheidsdiensten sterk worden bedreigd door wereldwijde technologische systemen;*

9. *te eisen dat de resultaten worden meegedeeld van de gesprekken opgenomen in Europese installaties die over Belgische gegevens beschikken en ervoor te zorgen dat de Belgische overheid toegang kan krijgen tot die installaties.*

*We willen met het federale parlement een ontmoeting organiseren met de parlementaire organen die in de verschillende landen van de Europese Unie de inlichtingendiensten controleren, om, voor zover die niet bestaan, de oprichting ervan aan te raden en bij te dragen tot de bewustwording van de noodzaak van Europese*

Nous vous recommandons donc :

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 et, surtout, par des partenaires 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, comme le demande le SGR, le principe général de précaution dans l'élaboration d'une politique globale et de sécurisation ;

3. De donner à la Sûreté de l'État et au SGR les moyens techniques et humains nécessaires en vue de recueillir toute information sur toutes menaces d'interception de communications dirigées contre la Belgique ;

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 – ne vous bornez pas à répondre à la seule recommandation n 4 même si nous souhaitons aussi savoir si vous comptez progresser dans ce domaine ; le débat que permet cette recommandation nº4 va bien au-delà de l'analyse du système Echelon ;

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, autrement dit de nous doter d'experts permettant de contrôler l'action des *hackers* ;

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 travaillant en étroite collaboration avec les services de renseignements nationaux ;

8. De faire évoluer ces pratiques des services de renseignement vers une interopérabilité plus large, afin d'aller au-delà de ce système un peu médiéval de troc, datant des début des services de renseignement et se justifiant lorsque les États n'étaient pas affaiblis par ces systèmes technologiques mondialisés ;

9. D'exiger la communication des résultats des écoutes enregistrées dans les installations qui, en Europe, disposent de données belges et de créer des conditions pour assurer l'accès des autorités belges à ces installations.

Nous souhaitons encore organiser, avec l'ensemble du parlement fédéral, une rencontre des organes parlementaires de contrôle des services de renseignements afin, d'abord, de conseiller à ceux qui n'auraient pas encore créé un contrôle parlementaire de le faire et, ensuite, de susciter une prise de conscience sur la nécessaire collaboration entre services de renseignements et la nécessité du contrôle parlementaire.

Je souhaiterais maintenant formuler quelques commentaires

*samenwerking inzake inlichtingenactiviteiten en tot de noodzaak van de parlementaire controle daarop.*

*Ik zou nu graag enkele persoonlijke opmerkingen formuleren.*

**De voorzitter**. – Mevrouw Lizin, U bent al meer dan een uur aan het woord. Mag ik u dus vragen om het kort te houden.

***Mevrouw Anne-Marie Lizin (PS)**. – Ik denk dat het niet aanvaardbaar was geweest dit omvangrijke werk over een essentieel onderwerp en waaraan talrijke mensen hebben meegewerkt in slechts enkele minuten te overlopen.*

*Dit verslag is zeer belangrijk omdat het tot stand is gekomen in een land waar strategische belangen niet vaak op de voorgrond komen, maar waar zich de belangrijkste centra van een reeks internationale activiteiten bevinden. Het is dus vooral in België dat men moet proberen te weten wat er gaande is, de zaken goed te organiseren en al wie op het grondgebied verblijft te beschermen.*

*Het rapport van het comité I over het onderzoekscentrum is al een voldoende reden om deze zaak grondig te bestuderen. We hebben misschien niet zoveel grote economische en commerciële belangen te verdedigen, maar het is onze taak de bedrijven bewust te maken van het gevaar en ze de zekerheid te verstrekken dat de overheid in staat is ze te beschermen.*

*Er werd al gesproken over Lernout & Hauspie en ander sprekers zullen daar misschien nog dieper op ingaan. Het Comité I heeft aangetoond hoe groot het gevaar was. Persoonlijk denk ik dat er een soortgelijk verband kan zijn in de zaak-Tractebel. We hebben vragen gesteld aan het Comité I, die hopelijk meer duidelijkheid zullen teweegbrengen. Het gaat om belangen van een Frans bedrijf. De kern van de zaak is een interessant gegeven over Kazachstan, een land waarover de internationale gemeenschap zich momenteel veel zorgen maakt.*

*Wat ik naast het verslag nog wou vermelden, zijn de elementen die in de Amerikaanse pers zijn verschenen. De berichtgeving over de plaatsen waar Echelon en de interceptie van Signal Intelligence actief zijn, laat duidelijk uitschijnen dat die activiteit herhaaldelijk zonder enig probleem werd uitgevoerd.*

*In alle publicaties wordt ook de band met Groot-Brittannië bevestigd.*

*Wat de te oprichten dienst betreft, is de vraag hoe men aan betrouwbare externe deskundigen kan geraken. Gelet op het huidige overwicht van de Amerikaanse diensten en technologie lijkt dat zeer moeilijk.*

*Bijna alle bestaande diensten voor de bescherming en de beveiliging van computergegevens en informatiesystemen worden in grote mate gefinancierd door Amerikaans risicokapitaal en staan onder de controle van de Verenigde Staten. Daarom is de vraag of we wel betrouwbare deskundigen kunnen vinden en hoe controle kan worden uitgeoefend op externe deskundigen. De meeste specialisten worden door de Verenigde Staten aangetrokken en de meest bekwame specialisten zijn bij de CIA langsgegaan.*

personnels.

**M. le président**. – Vous parlez depuis plus d'une heure, madame Lizin. Je vous demanderai donc d'être brève.

**Mme Anne-Marie Lizin (PS)**. – Je pense qu'il n'aurait pas été acceptable, eu égard au travail accompli et vis-à-vis des personnes ayant travaillé avec nous, que nous résumions en quelques minutes cette matière qui touche à des éléments essentiels.

Pourquoi ce rapport est-il tellement important ? Parce qu'il est élaboré dans un pays où les intérêts de type stratégique n'apparaissent pas souvent au grand jour, mais qui est un lieu où se trouvent les centres principaux de toute une série d'activités internationales. C'est donc en Belgique, plutôt qu'ailleurs, qu'il faut être capable de savoir ce qui se passe, de bien organiser les choses et de protéger ceux qui sont sur le territoire.

Cela conditionne évidemment un volet économique important. Le rapport du Comité R sur le centre de recherche est, à lui seul, une raison suffisante pour étudier la question de façon détaillée. Nous ne devons pas nécessairement protéger de grands intérêts économiques et commerciaux, qui peuvent se résumer chez nous à quelques grandes entreprises, mais nous devons faire en sorte que ces dernières aient conscience du danger et la certitude qu'il y a, au niveau public, une capacité de les protéger, laquelle n'est pas aujourd'hui mise en œuvre.

Le cas de Lernout & Hauspie a été évoqué ; je suppose que d'autres intervenants en parleront plus en détails. Le Comité R a montré à quel point le danger était grand. J'ajoute personnellement que l'affaire Tractebel peut avoir un certain type de lien de cette nature. Nous espérons en tout cas que les demandes que nous avons adressées au Comité R permettront de clarifier la situation. Nous nous trouvons là en prise directe avec les intérêts d'une entreprise française. On peut donc estimer que nous sommes au centre même d'une question intéressante concernant un pays, le Kazakhstan, qui fait aujourd'hui l'objet des plus grandes préoccupations internationales.

Les considérations que je voulais émettre en complément du rapport portent sur des éléments qui ont paru dans la presse américaine. Les organes de presse américains qui parlent du système Echelon, bien au-delà des déclarations de M. Woolsey, sont très clairs. La liste des sites où l'on peut constater qu'Echelon et l'interception de *Signal Intelligence* existent, montre que c'est admis et ce, de façon répétée.

Il est clair également que le lien avec la Grande-Bretagne est affirmé dans pratiquement toutes les publications sur ce secteur aujourd'hui. Concernant le service que nous devrions établir, il est question dans le rapport d'experts externes. Il s'agit là d'un point important parce que les experts qui travailleront dans le service qui sera, nous l'espérons, instauré par la Belgique, doivent évidemment être eux-mêmes fiables. C'est une question particulièrement difficile quand on voit l'actuelle capacité des services américains en ce qui concerne la technique utilisée pour avancer.

Pratiquement tous les services de protection de cryptage et de

**De voorzitter**. – Mevrouw Lizin, mag ik u vragen te besluiten, uit respect voor de andere zes ingeschreven sprekers?

***Mevrouw Anne-Marie Lizin (PS)***. *– Legt het reglement een beperking op?*

**De voorzitter**. – Ik verzoek u te besluiten. U heeft de tijd gekregen om naast het verslag ook uw mening uiteen te zetten.

***Mevrouw Anne-Marie Lizin (PS)***. *– Als u mij het recht weigert om mijn persoonlijk standpunt te verdedigen, zal ik het recht vragen om namens mijn fractie te spreken.*

**De voorzitter**. – Goed!

**De heer Hugo Vandenberghe (CD&V)**. – Ik wil mevrouw Lizin danken voor dit op zichzelf zeer interessant rapport. De bedoeling was natuurlijk om deze namiddag enkele politieke conclusies te trekken uit de gedane vaststellingen en niet om de bestaande toestand opnieuw in detail te beschrijven. Mijn toespraak zal dan ook veel beknopter zijn.

Op de eerste plaats wil ik beklemtonen dat dit rapport geen eindpunt maar een beginpunt is. Het zet bakens uit en signaleert problemen die wij zullen moeten oplossen. Vandaag ligt de oplossing niet voor de hand. Er rijzen zowel problemen vanuit juridisch oogpunt als op het vlak van de operationaliteit: dit wil zeggen het beschermen van de rechten en van de bezittingen van onze burgers tegen het gevaar van het afluisteren door Echelon.

Ik zou willen verwijzen naar de juridische uiteenzetting in het rapport en naar het antwoord op de vraag in welke mate het geheime afluisteren van nationale en internationale telecommunicatie strijdig is met artikel 8 van het EVRM.

Sedert het arrest-Klass van 9 september 1978 van het Europees Hof voor de Rechten van de Mens is het immers een uitgemaakte zaak dat dergelijke praktijken de lezing van artikel 8 van het EVRM niet weerstaan. Er rijst dus een politieke vraag en die verdient een politiek antwoord.

Als de regering of als Kamer of Senaat kennis nemen van de mogelijkheid of de zekerheid dat haar burgers slachtoffer zijn van een inbreuk op artikel 8 van het EVRM dat de telefoontap uitdrukkelijk aan zeer strikte voorwaarden koppelt, kan het dan volstaan dit te beschrijven in een verslag? Hebben wij dan geen politieke verplichtingen op twee niveaus? Ten eerste legt het EVRM niet alleen verbodsbepalingen op die door de overheid moeten worden in acht genomen ter vrijwaring van de fundamentele rechten en vrijheden van de burgers, maar legt het tevens positieve verplichtingen op aan de overheid om de beschermde rechten te verwezenlijken en te doen eerbiedigen. Dat betekent dat als de minister van Justitie weet

**M. le président**. – Madame Lizin, veuillez conclure. Vous n'êtes pas le seul orateur de cet après-midi. Je vous demande de respecter les autres orateurs. Il y a encore six inscrits !

**Mme Anne-Marie Lizin (PS)**. – Le règlement impose-t-il une limite ?

**M. le président**. – Je vous demande de conclure. Vous avez eu tout le temps de développer toutes vos thèses au-delà du rapport.

**Mme Anne-Marie Lizin (PS)**. – Non ! Après avoir fait le rapport, je vous demande le droit d'intervenir personnellement. Si vous refusez, je demanderai le droit de parler au nom de mon groupe plus tard.

**M. le président**. – D'accord !

***M. Hugo Vandenberghe (CD&V)***. *– Je remercie Mme Lizin pour ce très intéressant rapport. L'objectif était, bien sûr, de tirer, cet après-midi, des conclusions politiques des constatations faites et non de décrire à nouveau en détail la situation. Aussi serai-je bien plus bref.*

*Ce rapport n'est qu'un début. Il met en évidence des problèmes que nous devons résoudre. Une solution n'est pas évidente aujourd'hui. Des problèmes se posent aux plans juridique et opérationnel, c'est-à-dire quant à la protection des droits et biens de nos citoyens contre le risque d'écoute au moyen du système Echelon.*

*Je voudrais rappeler l'analyse juridique présentée dans le rapport et la réponse à la question de savoir dans quelle mesure l'écoute secrète de télécommunications nationales et internationales est contraire à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme.*

*Depuis l'arrêt Klass du 9 septembre 1978 de la Cour européenne des droits de l'homme, il est établi que ces pratiques sont contraires à l'article 8. Il se pose donc une question politique qui mérite une réponse politique.*

*Si le gouvernement ou le Parlement apprend que nos citoyens sont victimes d'une violation de l'article 8, peut-il se contenter de le constater dans un rapport ? N'avons-nous pas des obligations politiques à deux niveaux ? La CEDH impose non seulement des interdictions que doivent respecter les autorités pour sauvegarder les droits et libertés fondamentaux de leurs citoyens, mais aussi des obligations positives qui contraignent les autorités à réaliser et à faire respecter les droits protecteurs. Autrement dit, si le ministre de la Justice sait ou entend dire que les télécommunications font l'objet d'écoutes, le gouvernement doit s'interroger sur les obligations positives qui s'imposent à lui.*

*Devons-nous déposer plainte contre la Grande-Bretagne et éventuellement l'Allemagne auprès de la Cour européenne des droits de l'homme ? Ce point est développé dans les*

création de *firewalls* qui existent aujourd'hui dans le monde ont été et sont financés en grande partie par du capital à risque américain et contrôlés par les États-Unis. Se posent dès lors les questions de savoir si nous aurons la capacité d'avoir des experts fiables et, dans le cas où nous nous doterions d'experts externes, comment nous contrôlerons cette matière. De plus, la plupart des spécialistes sont attirés aux États-Unis et sont inévitablement passés, s'ils sont compétents, par les sites de la CIA.

of hoort te weten dat er telecommunicatie wordt afgeluisterd, de regering zich moet buigen over de vraag welke positieve verplichtingen dit voor haar meebrengt.

Moeten wij de interstatenklacht formuleren bij het Europees Hof voor de Rechten van de Mens tegen het Verenigd Koninkrijk en eventueel tegen Duitsland om af te dwingen dat de fundamentele rechten en vrijheden van onze burgers ook door die Staten worden geëerbiedigd? Dit punt is nu definitief uitgewerkt in de conclusies. Er zijn ook tussenstappen voorgesteld maar daarmee is het probleem nog niet van de baan. Volgens mij zijn wij verplicht om de naleving van artikel 8 van het EVRM in rechte of via politieke weg af te dwingen.

Een tweede probleem is de vaststelling dat het niet alleen gaat om de bescherming van artikel 8, maar dat we met een afluistersysteem ook te maken kunnen hebben met economische spionage waardoor het patrimonium van onze burgers of de personen die op ons grondgebied verblijven, zou kunnen worden aangetast. Wetenschappelijk onderzoek, ontdekkingen die het voorwerp zijn van octrooien of patenten kunnen door telecommunicatie worden onteigend. Dat betekent dat men er kennis kan van nemen zonder er enige vergoeding te moeten voor betalen en dat men het in een concurrerend land kan gebruiken zonder het wetenschappelijk onderzoek of de exploitatiekosten te betalen.

Die vaststelling leidt ertoe dat de overheid een dubbele verplichting heeft, een juridische en een operationele. Ze is niet alleen verplicht om artikel 8 van het EVRM te eerbiedigen, maar ook om de staatsveiligheid de mogelijkheden, financiële middelen en personeel te geven om een tegenmaatregel te kunnen ontwikkelen, om te kunnen onderzoeken of er effectief sprake is van een afluistersysteem dat de belangen van onze burgers en ondernemingen bedreigt.

Uit de verklaringen die rond Lernaut & Hauspie worden afgelegd, blijkt dat deze vraag en het antwoord erop niet van theoretische aard zijn. De rapporteur vermeldde in dat verband ook Electrabel. Daarom moet er tijdens het openbaar debat in de Senaat een verduidelijking komen.

Naar aanleiding van de voorstelling van het Echelonverslag in de commissie werden er namelijk nogal wat publieke verklaringen afgelegd, onder meer door de eerste burger van het land. Ik neem aan dat zijn verklaringen boven elke verdenking staan. Een zeer terughoudende journalist van de televisie stelde de heer De Croo de vraag of hij er op de hoogte van is dat Lernaut & Hauspie het slachtoffer zou zijn geweest van een afluistersysteem, type Echelon. Zonder enig voorbehoud zoals op de dag van zijn huwelijk antwoordde hij 'ja'. Omdat een voorzitter van de Kamer toch geen lichtzinnige verklaringen aflegt, ben ik van oordeel dat ik deze verklaring vandaag opnieuw aan de orde moet stellen.

Deze zaak moet uitgeklaard worden omdat de parlementaire Commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten aan het Vast Comité I een rapport gevraagd heeft over de eventuele implicaties van Echelon of soortgelijke systemen op de activiteiten van Lernaut & Hauspie.

De Kamervoorzitter had misschien beter geen verklaring afgelegd. Het is namelijk bijzonder delicaat om over vertrouwelijke verslagen in het openbaar verklaringen af te

*conclusions. J'estime que nous sommes tenus d'imposer le respect de l'article 8 de la CEDH, que ce soit par la voie judiciaire ou la voie politique.*

*Un second problème est qu'il ne s'agit pas seulement de la protection de l'article 8 mais qu'un système d'écoute peut aussi viser à un espionnage économique, lequel peut porter atteinte au patrimoine de nos citoyens ou des personnes résidant sur notre territoire.*

*Il en résulte que les autorités ont une double obligation, juridique et opérationnelle. Elles sont non seulement tenues de respecter l'article 8 de la CEDH mais aussi de donner à la Sûreté de l'État les possibilités, les moyens financiers et le personnel nécessaires pour prendre des contre-mesures et s'assurer de l'existence d'un système d'écoute pouvant menacer les intérêts de nos citoyens et de nos entreprises.*

*On a évoqué le cas de Lernaut & Hauspie et d'Electrabel. Le président de la Chambre a lui-même dit savoir que Lernaut & Hauspie avait été victime d'écoutes opérées via un système du type Echelon. Considérant que le premier citoyen de notre pays ne peut lancer des affirmations à la légère, j'estime qu'il faut tirer cette affaire au clair. La Commission chargée du suivi du Comité permanent de contrôle des services de renseignements et de sécurité a d'ailleurs demandé au Comité R d'établir un rapport sur les implications qu'ont pu avoir le système Echelon ou des systèmes similaires sur les activités de Lernaut & Hauspie.*

*Le président de la Chambre aurait peut-être mieux fait de se taire. Il est en effet particulièrement délicat de faire des déclarations publiques peut-être peu conformes à la réalité sur des rapports confidentiels. Nous devons donc convenir d'une procédure à suivre dans des dossiers comme ceux de Tractebel et de Lernaut & Hauspie dès lors que des enquêtes judiciaires sont en cours. Des déclarations relatives à ces dossiers peuvent en effet être sorties de leur contexte et donner lieu à des extrapolations.*

*La mission confiée au Comité R dans l'affaire Lernaut & Hauspie n'est pas terminée. Il est dangereux d'aborder cette matière alors que le cadre juridique, les droits et obligations et les procédures à suivre pour défendre ses droits ne sont pas définis précisément. Nous devons être vigilants pour éviter les abus.*

*Outre le problème de la protection juridique se pose aussi celui des moyens techniques dont nous disposons pour nous protéger contre cette forme d'espionnage. La semaine dernière, la commission de la Justice a mené un débat intéressant sur l'installation d'une chambre centrale d'écoute permettant d'entendre toutes les conversations téléphoniques dans notre pays dans les conditions qu'impose la loi quant au rôle du juge d'instruction. Les possibilités techniques qu'offre une chambre d'écoute risquent d'être exploitées par un système comme Echelon qui pourrait ainsi enregistrer toutes les informations sensibles faisant l'objet d'écoutes. Disposons-nous des moyens techniques d'empêcher cet abus ?*

*Je ne suis pas étonné que si peu de sénateurs manifestent de l'intérêt pour la protection des droits et libertés fondamentaux des citoyens. En tant que chambre de réflexion, le Sénat a pourtant un rôle évident à jouer dans ce domaine.*

leggen, die misschien niet overeenstemmen met de werkelijkheid. We kunnen geen rekening houden met een dergelijke complicatie van de problemen. Ik kan hierop uiteraard niet in detail ingaan, maar we moeten afspraken maken over de te volgen procedure inzake dossiers zoals Tractebel en Lernout & Hauspie, gelet op de aan de gang zijnde gerechtelijke onderzoeken. Verklaringen over deze dossiers kunnen immers buiten hun context worden gebruikt en er kunnen extrapolaties aan worden verbonden. Een gerechtelijk onderzoek heeft toch nog altijd tot doel om de waarheid aan het licht te brengen.

De opdracht van het Vast Comité I met betrekking tot de zaak Lernout & Hauspie is niet beëindigd. Gezien de verklaringen die hierover werden afgelegd en de massale publieke weerklank die deze hebben gehad, wensen wij duidelijkheid te krijgen over dit dossier. Dit voorbeeld toont inderdaad aan hoe gevaarlijk het is met deze materie om te gaan in een rechtsvrije ruimte, waarbij het juridisch kader, de rechten en de verplichtingen en de procedures om zijn rechten te verdedigen, niet duidelijk zijn omlijnd. We moeten waakzaam blijven ten einde misbruiken te vermijden.

Naast het probleem van de juridische bescherming is er ook het probleem van de technische mogelijkheden om ons tegen deze vorm van bespieden – het aftappen van de telecommunicatie – te beschermen. Vorige week werd in de commissie voor de Justitie een interessant debat gevoerd over de installatie van een centrale afluisterkamer om in ons land het aftappen van alle telefoongesprekken mogelijk te maken, uiteraard volgens de voorwaarden die de wet voorschrijft inzake de rol van de onderzoeksrechter. Het risico bestaat dat een systeem zoals echelon gebruik maakt van de technische mogelijkheden die een aftapkamer biedt om alle gevoelige informatie die het voorwerp van aftapping uitmaakt, te registreren. Ik had derhalve graag vernomen of wij over technische middelen beschikken om een dergelijke gang van zaken te verhinderen. Als we niet over een systeem beschikken om de gegevens die het gevolg zijn van de telefoontap te beschermen, nemen wij dan geen onberekend risico aangezien het systeem aanleiding kan geven tot misbruik?

Dat er slechts weinige senatoren zijn die belangstelling hebben voor de bescherming van de fundamentele rechten en vrijheden van de burgers, verwondert mij niet. Nochtans is er op dit vlak een duidelijke rol weggelegd voor de Senaat als reflectiekamer. Ik ben het gewoon geworden dat er weinig politieke interesse is voor grote debatten over fundamentele problemen.

*(Voorzitter: de heer Jean-Marie Happart, ondervoorzitter.)*

Het onderwerp waarover we vandaag discussiëren is alleszins geen *fait divers*. Het gaat over een bespiedingssysteem, een big-brothersysteem dus, dat in een democratische samenleving niet kan worden aanvaard. Het kan immers over de registratie van informatie over allen van ons gaan. Daaraan kan een geheim leven worden gegeven en daarmee kunnen alle mogelijke manipulaties gebeuren. De bescherming van de persoon betreft niet alleen de persoon zelf, maar ook de informatie over de persoon. Die informatie is het verlengde, de essentie, van iedere burger. In een democratie moet in de eerste plaats het parlement de fundamentele rechten en

*(M. Jean-Marie Happart, vice-président, prend place au fauteuil présidentiel.)*

*Le sujet dont nous discutons aujourd'hui n'est pas un fait divers. Il s'agit d'un système d'espionnage, d'un système Big Brother, inacceptable dans une société démocratique. La protection de la personne ne concerne pas seulement la personne même mais aussi l'information sur cette personne. Dans une démocratie, c'est avant tout le parlement qui doit être attentif aux droits et libertés fondamentaux. C'est pourquoi il importe que nous mettions aujourd'hui ces problèmes en évidence et que nous affirmions notre intention d'apporter une réponse aux questions juridiques et aux*

vrijheden in het oog houden. Daarom is het belangrijk dat we die vragen vandaag onderstrepen en de intentie uitspreken om op definitieve wijze zowel de juridische vraagstelling als de vragen in verband met de bescherming te beantwoorden.

***De heer Marc Hordies (ECOLO)***. *– Het Echelonverslag kan u niet onberoerd laten, noch wat zijn verontrustende, noch wat zijn lachwekkende aspecten betreft.*

*Eerst de verontrustende: uw begeleidingscommissie komt tot het besluit dat bevriende landen wel degelijk gesofisticeerde spionageactiviteiten ontplooien en in staat zijn de meeste elektronische berichten die op ons grondgebied worden verzonden, blindelings en naar eigen goeddunken te onderscheppen.*

*Als vertegenwoordigers van het volk zijn wij niet langer in staat om de gevoelige inlichtingen van de Staat te beschermen, noch om de persoonlijke levenssfeer te beschermen of onze bedrijven tegen economische spionage te behoeden. Wij zouden net zo goed kunnen zeggen dat elke brief die in België wordt verzonden, door een vreemde overheid kan worden geopend en dat de inhoud ervan aan derden kan worden meegedeeld. Dat valt des te moeilijker te aanvaarden omdat hierop geen echt democratisch toezicht wordt uitgeoefend, noch door het gerecht, noch door het Parlement.*

*De wet van deze landen voorziet hoogstens in bescherming van hun burgers of ingezetenen, niet van wie in het buitenland verblijft. Zo zou iedereen zijn vreemde buurman kunnen bespioneren en de informatie kunnen uitwisselen met diens land van herkomst of een ander land.*

*U zou kunnen opwerpen dat een en ander van weinig belang is voor wie niets op zijn kerfstok heeft, maar dat ligt niet voor de hand.*

*Daags na 11 september hebben sommigen in een opwelling van medeleven gezegd dat wij allemaal Amerikanen zijn. Nadien heeft de president van de Verenigde Staten een nieuwe kruistocht uitgeroepen: de oorlog van het goed tegen het kwaad, zonder nuances.*

*Sindsdien volgen heel wat andere Staten en staatshoofden, waaronder heel wat minder roemrijke voorvechters van de mensenrechten, zijn voorbeeld en behandelen iedere opposant als een terrorist; zij matigen zich het nagenoeg goddelijke recht aan om in naam van het goede het kwaad te verpletteren en elke andere Staat te verzoeken om mee te vechten tegen hun kwaad.*

*Hoe kan het anders of de Staten en hun geheime diensten ijveren in deze geest zonder nuances tegen de rechten van de mens, die nochtans de grondslag vormen van het hedendaagse Europa.*

*Vanwege mijn gelaatskleur, maar misschien nog meer om wat er zich in mijn achterhoofd afspeelt, zouden sommige weldenkende, maar slechtziende landen mij wel eens in het kamp van het kwaad kunnen indelen, net zoals de nazi's in mijn grootvader, officier bij het verzet in België, een terrorist zagen.*

*Ik heb de val van Allende door toedoen van de CIA en de aanslag op het schip van Greenpeace door de Franse geheime diensten niet verteerd. Ik bespaar u overigens andere questions liées à la protection.*

**M. Marc Hordies (ECOLO)**. – Le rapport Echelon qui vous est présenté par les commissions chargées du suivi et de l'accompagnement des comités R et P doit vous interpeller, tant par ses aspects inquiétants que par ses aspects dérisoires.

L'inquiétude d'abord : votre commission de suivi conclut qu'il existe bien un espionnage sophistiqué de la part de pays amis, capables d'intercepter de façon aveugle la plupart des communications électroniques émises sur notre territoire et d'en tirer les informations comme bon leur semble.

En tant que représentants du peuple, nous ne sommes plus en mesure ni de protéger les informations sensibles de l'État, ni de garantir la protection de la vie privée, ni de prémunir les entreprises de tout espionnage économique.

C'est comme si nous vous annoncions que n'importe quel courrier émis en Belgique pourrait impunément être ouvert par une autorité étrangère et que celle-ci pourrait communiquer son contenu à d'autres. C'est d'autant plus inadmissible que cela se fait sans réel contrôle démocratique, que ce soit par des instances juridictionnelles ou parlementaires.

Tout au plus, la loi de ces pays prévoit de protéger ses citoyens ou résidents à l'étranger. Ainsi, chacun pourrait espionner les citoyens voisins et échanger ensuite les informations avec le pays d'origine ou un autre.

Vous pourriez me rétorquer que cela pourrait ne pas avoir grande importance dès l'instant où l'on n'a rien à se reprocher mais ce n'est pas aussi évident.

Au lendemain du 11 septembre, un élan de compassion bien compréhensible a fait dire à certains que nous étions tous Américains. Plus tard, le Président des États-Unis déclarait une nouvelle croisade : la guerre du bien contre le mal, sans nuances.

Depuis, beaucoup d'autres États ou chefs d'État, dont certains moins glorieux en matière de respect des droits de l'homme, s'engouffrent dans la brèche pour traiter tout opposant de terroriste et s'arrogent le droit quasi divin, au nom du bien, d'écraser le mal, et de demander à chaque autre État de participer à la lutte contre leur mal.

Dans cette nouvelle culture, comment ne pas craindre que des États et leurs services secrets œuvrent, sans nuances, contre les valeurs fondamentales des droits de l'homme, qui ont cependant fondé l'Europe contemporaine ?

Par mon faciès, mais surtout par ce qui se passe derrière, je pourrais être considéré dans certains pays bien pensants, mais mal voyants, comme étant plutôt du côté du mal comme mon grand-père, officier résistant pour la Belgique, terroriste pour les nazis.

Je n'ai pas digéré la chute d'Allende soutenu par la CIA tout comme je n'ai pas digéré l'attentat contre le bateau de Greenpeace par les services secrets français. J'en passe, et des meilleures.

Je ne m'oppose néanmoins pas à la nécessité du

*voorbeelden.*

*Toch verzet ik mij niet tegen het werk van de inlichtingendiensten. Dat werk kan echter maar zin hebben als het onder het toezicht staat van een democratisch systeem dat er de politieke verantwoordelijkheid voor draagt tegenover de burger, een systeem dat de activiteiten van de dienst toespitst op de verdediging van de fundamentele waarden van een democratische rechtsstaat en niet op de ondermijning ervan.*

*Ik zou dus hulde willen brengen aan het Belgische systeem dat voorziet in parlementair toezicht op de inlichtingendiensten. Deze dienst zou moeten worden uitgebreid tot alle andere landen en tot de bescherming van de rechten van de burgers van andere landen die zouden worden bespioneerd. Dat is mijns inziens het beste democratische antwoord op wat een zware disfunctie blijkt te zijn.*

*Na de verontrustende aspecten van het Echelonverslag zou ik nu even willen ingaan op de lachwekkende. Al deze gesofisticeerde apparatuur heeft de aanslagen van 11 september inderdaad niet kunnen beletten.*

*De volgende vragen moeten dus zeker worden gesteld. Als deze middelen niet afdoend zijn, waartoe dienen ze dan? Als ze wel doeltreffend zijn, waarom hebben ze deze slachting dan niet kunnen afwenden?*

*Laten we ons geen technologische illusies maken en laten wij nadenken over het belang dat aan door mensen verstrekte inlichtingen moet worden gehecht.*

*Men heeft overigens terecht gezegd dat sommige antidemocratische, terroristische activiteiten hun doel niet mogen bereiken. Die beogen met name de verzwakking van de democratieën en haar fundamentele principes, waaronder de bescherming van de persoonlijke levenssfeer en de vrijheid van meningsuiting. Wij moeten deze fundamentele principes beschermen en mogen er enkel in geval van nood en onder zeer precieze voorwaarden van afwijken. Er moeten democratische controlemiddelen komen en er moeten democratische bakens worden uitgezet die in verhouding staan tot het gevaar dat eventuele afwijkingen met zich zouden kunnen brengen.*

*In die geest en onder dat voorbehoud sluit ik mij aan bij de aanbevelingen van de begeleidingscommissie.*

*Het voorbehoud dat mij hierbij het nauwst aan het hart ligt, is terug te vinden in artikel 8 en betreft een veel grotere uitwisseling van inlichtingen tussen de verschillende Europese inlichtingendiensten. In de commissie had ik een amendement ingediend dat er toe strekte deze uitwisseling van inlichtingen aan te moedigen, zij het uitsluitend tussen landen die parlementair toezicht uitoefenen op hun inlichtingendiensten en op de eerbiediging van de fundamentele democratische principes.*

*Mijns inziens is dat een minimale waarborg en juist daarom is hij onontbeerlijk. Mag ik u vragen om ook in dezen het voorzorgsprincipe toe te passen, vooral nu partijen die de vrijheid willen fnuiken en vreemdelingenhaat prediken, opnieuw de kop opsteken in heel wat Europese landen en kandidaat-lidstaten?*

renseignement mais j'estime qu'il n'a son sens que s'il est contrôlé par un système démocratique qui en assume la responsabilité politique devant le citoyen, système qui canalise ce service dans le sens de la défense des valeurs fondamentales d'un État démocratique de droit, et non à son détriment.

Je voudrais donc rendre hommage ici au système belge qui prévoit un processus de contrôle parlementaire des services de renseignements.

Ce service devrait être étendu à tous les pays ainsi qu'à la protection des droits des citoyens des autres pays qui seraient espionnés. C'est, à mon sens, la meilleure réponse démocratique à ce qui apparaît comme une grave dérive.

Après avoir cité les aspects inquiétants du rapport Echelon, je voudrais à présent poursuivre sur les aspects dérisoires de ce que nous révèle l'histoire proche. En effet, tous ces appareillages sophistiqués n'ont pu empêcher les attentats du 11 septembre.

Il y a donc bien lieu de se poser ces questions. Ou bien ces moyens sont inefficaces et à quoi dès lors servent-ils, ou bien ils sont efficaces et pourquoi dès lors n'ont-ils pas empêché ce massacre ?

Ne tombons donc pas dans l'illusion technologique et réfléchissons bien à l'importance à accorder aux renseignements humains.

On a dit par ailleurs, à juste titre, qu'il ne fallait pas que certains actes terroristes antidémocratiques atteignent leurs objectifs, à savoir l'affaiblissement des démocraties et de leurs principes fondamentaux. Parmi ceux-ci, il est celui de la protection de la vie privée et de la liberté d'opinion. Il nous revient de protéger ces principes fondamentaux et, en cas de nécessité, d'y déroger dans des cas précis. Il s'agira de mettre les moyens de contrôle et les balises démocratiques à hauteur des dangers que ces éventuelles dérogations comporteraient.

C'est dans cet esprit et avec ces réserves que je souscris aux recommandations de la commission de suivi.

Parmi ces réserves, il en est une qui me tient particulièrement à cœur. Elle est prévue à l'article 8 et concerne un plus grand échange d'informations entre les différents services de renseignements européens. J'avais déposé, en commission, un amendement favorisant ces échanges, mais uniquement entre pays disposant d'un contrôle parlementaire des services de renseignements, afin de veiller au respect des principes fondamentaux démocratiques.

Il s'agit, selon moi, d'une garantie minimale. Et, parce qu'elle est minimale, elle est indispensable. Puis-je donc demander que, dans cette matière également, le principe de précaution soit appliqué, d'autant plus que des partis liberticides et xénophobes renaissent et se développent dans de nombreux pays européens ainsi que dans des pays candidats ?

**De heer Frans Lozie (AGALEV)**. – Ik betreur dat de discussie over Echelon plaatsvond in de beslotenheid van de commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten. Dat die commissie met gesloten deuren vergadert, kan ik begrijpen omwille van de gevoeligheid van de dossiers. Openbaarheid zou de werkzaamheden hypothekeren. Maar meteen nadat een aantal vastellingen over Echelon werden gemaakt, hadden we een openbaar debat moeten krijgen. Dat is er wel geweest in de jaren tachtig toen de Gladio-affaire aan het licht kwam en de inlichtingendiensten in opspraak waren gekomen. Gelukkig geeft het voorliggende verslag ons enig inzicht.

Aangezien ik geen deel uitmaak van voornoemde commissie, zal mijn commentaar beperkt zijn. Het zal wel voor iedereen duidelijk zijn dat het Amerikaans spionagesysteem Echelon een bijzonder gevaarlijk fenomeen is, gevaarlijk voor onze privacy, maar ook voor onze economische belangen. De spionage was immers niet alleen ingegeven door veiligheidsoverwegingen vanwege de Verenigde Staten en de landen die aan de operatie deelnamen, maar ook door economische overwegingen. Echelon is ook gevaarlijk voor de relatie tussen de Verenigde Staten en de Europese Unie. Het is ongehoord dat de Verenigde Staten waarmee Europa een militaire alliantie vormt, om zuiver economische redenen spionageactiviteiten in Europa ontwikkelt zonder dat we daarvan op de hoogte zijn en zonder dat we over de middelen beschikken om het te ontdekken. We moesten het via Amerikaanse bronnen vernemen.

Het fenomeen is ook gevaarlijk voor de relaties binnen de Europese Unie. We stellen immers vast dat bepaalde lidstaten van de Unie aan de operatie hebben meegewerkt. Sommige daarvan zijn bekend, van andere is het niet altijd duidelijk. Ook België is op een bepaald ogenblik genoemd als zijdelingse medewerker.

Ik wil het nog kort hebben over de aanbevelingen in het verslag. In punt 6 wordt terecht gestipuleerd dat het afluisteren met economisch oogmerk tussen de lidstaten van de Europese Unie moet worden verboden. Dat verbod moet echter niet alleen voor de landen van de Europese Unie gelden, maar ook voor alle andere mogendheden die op Europees grondgebied dergelijke activiteiten ontwikkelen. De aanbeveling moet dan ook in die zin worden uitgebreid. Over wat de Verenigde Staten op hun grondgebied doen, kan hun parlement zich dan uitspreken.

Met punt 7 waarin gevraagd wordt een Europese inlichtingendienst op te richten, kan ik akkoord gaan. Het is immers onaanvaardbaar dat we onze eigen situatie alleen kunnen bekijken door de ogen van een vreemde mogendheid, zelfs al gaat het, althans op dit ogenblik, om een militaire bondgenoot. Ervaring uit het verleden leert ons dat we de originele bronnen van de informatie die door de Verenigde Staten over ons land wordt verzameld, niet in handen krijgen, zodat we geen eigen conclusies kunnen trekken. In het beste geval hebben we alleen weet van de conclusies die Verenigde Staten trekken uit de door hun verzamelde informatie.

Ik ben blij dat de Senaat zijn steun gaf aan het Galileo-project, waar de voorzitter van de Senaat een groot voorstander van is. Daardoor zullen we over een eigen instrument beschikken, waarvan we echter gebruik zullen kunnen maken nadat een democratische controle op dat

***M. Frans Lozie (AGALEV)***. *– Je regrette que la discussion sur le système Echelon ait eu lieu au sein de la Commission chargée du suivi du Comité permanent de contrôle des services de renseignements et de sécurité, qui se réunit à huis clos. Ce problème aurait également dû faire l'objet d'un débat public. Heureusement, le présent rapport nous a permis de nous faire une idée de la situation.*

*Comme je ne fais pas partie de la commission de suivi, mon commentaire sera bref. Chacun aura compris que le système américain d'espionnage Echelon est un phénomène particulièrement dangereux pour notre vie privée et pour nos intérêts économiques. Ces pratiques ne sont en effet pas inspirées par des seuls motifs de sécurité mais aussi par des considérations économiques. Echelon est également dangereux pour les relations entre les États-Unis et l'Union européenne. Il est inouï que les États-Unis, avec lesquels l'Europe a conclu une alliance militaire, développent des activités d'espionnage en Europe à des fins exclusivement économiques sans que nous en soyons informés et ayons les moyens de l'être.*

*Ce phénomène est également dangereux pour les relations au sein de l'Union européenne. Nous constatons en effet que certains États membres de l'Union ont pris part à cette opération. Même la Belgique a été citée comme collaboratrice indirecte.*

*Je voudrais également toucher un mot des recommandations formulées dans le rapport. Le point 6 précise à juste titre que tout type d'écoutes à des fins économiques entre États de l'Union doit être interdit. Il convient toutefois d'étendre cette interdiction à toutes les puissances qui développent des activités sur le territoire européen.*

*Je suis d'accord avec le point 7 qui demande la création d'un service de renseignement européen. Il est en effet inacceptable que nous ne puissions examiner notre propre situation qu'à travers les yeux d'une puissance étrangère. Dans le meilleur cas, nous n'avons connaissance que des conclusions que les États-Unis tirent des informations qu'ils ont récoltées.*

*Je suis heureux que le Sénat ait soutenu le projet Galileo. Nous disposerons bientôt de notre propre instrument que nous ne pourrons toutefois utiliser que lorsque son contrôle démocratique aura été organisé au sein de l'Europe.*

*L'engagement que nous prenons de prendre contact avec les parlementaires des autres pays européens et avec le Parlement européen afin de définir un suivi de ce phénomène sous un angle démocratique est pour moi un élément positif. Nous ne pouvons faire ce que nous interdisons à d'autres pays. Le principe de base est qu'il est inacceptable qu'une puissance étrangère collecte systématiquement des informations sur les citoyens, les entreprises et les communications d'un pays sans que les dirigeants de ce pays en soient informés et quel qu'en soit le motif.*

*Je n'ai rien contre les services de renseignement qui tentent de garantir la sécurité des citoyens. Mais je ne puis accepter que des services de sécurité collectent des informations sans que les autorités politiques en soient informées et sans que les objectifs de ces pratiques soient connus.*

*J'espère que nous resterons attentif à ce principe dans les*

systeem binnen Europa is georganiseerd. We mogen uiteraard niet de fouten maken die we andere mogendheden aanwrijven.

Een positief element vind ik het engagement om contact op te nemen met parlementsleden en parlementen van de andere Europese landen en met het Europees Parlement om te kijken hoe we vanuit een democratische invalshoek het fenomeen kunnen blijven opvolgen. Het kan zeker niet de bedoeling zijn om te doen wat we andere landen verbieden. Het uitgangspunt moet zijn dat het onaanvaardbaar is dat een vreemde mogendheid systematisch informatie verzamelt over burgers, ondernemingen en communicatie van een bepaald land zonder medeweten van de politieke leiders van dat land, ongeacht het motief, veiligheid, economische overwegingen, of concurrentievervalsing.

Ik heb niets tegen inlichtingendiensten die de veiligheid van de burgers proberen te garanderen. Ik heb er wel iets tegen dat veiligheidsdiensten informatie verzamelen zonder dat de politieke gezagsdragers daarvan op de hoogte zijn en hun doelstellingen niet kenbaar maken.

Ik hoop dat we bij de activiteiten die we overeenkomstig de aanbevelingen van het rapport in samenwerking met andere parlementen zullen ontwikkelen, die stelregel voor ogen zullen houden.

***Mevrouw Anne-Marie Lizin (PS)**. – In het verslag stelt onze fractie voor een dienst met betrouwbare experts op te richten, wat niet gemakkelijk is voor een land als België. De technologieën die bescherming bieden tegen hackers, zijn inderdaad allemaal in Amerikaanse handen. De minister weet dat we niet gerust zijn in het contract dat zal worden afgesloten met de firma NICE, waarvan alleen de naam sympathiek klinkt. Hoever staat het met het verslag van de Staatsveiligheid, vooraleer de minister een beslissing aan de regering voorlegt? Is het verslag al aangekomen?*

*(De minister knikt ontkennend)*

*We hebben er dus belang bij na te trekken welke weg die verslagen afleggen.*

*We moeten nagaan op welke manier we de deskundigheid van onze experts kunnen natrekken, ook als ze uit het leger komen.*

*Als de diensten van de minister telefonisch toegang krijgen tot alle informatie, is het inderdaad niet interessant een grote dienst op te richten.*

*Moet België de interceptie van boodschappen door de inlichtingendiensten wettelijk regelen? Dat is op dit ogenblik een heikele kwestie. Ik vind van wel, maar we verwachten dat de minister ons zal zeggen op welke manier hij dit wil regelen.*

*Met betrekking tot de antiterroristische maatregelen op ons grondgebied, zei de heer Bruguière gisteren nog dat we het belang daarvan nog maar beginnen te ontdekken. We moeten de Staatsveiligheid beter uitrusten, dat is evident. Dat kan*

*activités que nous développerons à l'avenir.*

**Mme Anne-Marie Lizin (PS)**. – Je vais reprendre quelques considérations inspirées par l'analyse que nous avons faite de cette question dans notre groupe. Nous considérons que ce sujet mérite d'être approfondi et non pas survolé.

Dans le rapport, nous proposons, et notre groupe soutient cette proposition, que soit créé un service doté d'experts fiables. C'est difficile pour un pays comme la Belgique. En effet, je vous rappelle que l'ensemble des technologies de protection contre l'intrusion de *hackers* est déjà dans les mains des Américains. Vous connaissez, parce que nous en avons discuté à huis clos, notre inquiétude quant au contrat en préparation avec la firme NICE dont seul le nom nous paraît sympathique. Qu'en est-il du rapport de la Sûreté de l'État que vous attendiez, monsieur le ministre, avant de proposer une décision au gouvernement ? Vous est-il parvenu neuf jours après son envoi ?

*(Signe de dénégation du ministre)*

Nous avons donc intérêt à vérifier par quels circuits passent ces rapports.

J'en reviens à la difficulté d'obtenir des expertises de qualité. Il importe de s'interroger sur la manière dont nous pourrons vérifier la qualité de nos experts. Je crois que l'on peut en trouver dans les services militaires. Il faut cependant être très attentifs à leur qualité.

Si vous ouvrez à partir de vos propres services téléphoniques la possibilité d'avoir accès à tout, il n'est effectivement pas intéressant de créer un grand service.

La Belgique doit-elle légiférer sur l'interception de communications par les services de renseignement ? C'est une question qui reste pour l'instant très « chaude ». Nous l'avons mentionnée dans le rapport. Ma conviction personnelle va dans ce sens mais nous attendons de votre part des éléments d'appréciation sur la manière dont cela pourrait

*door een aantal voorzorgsmaatregelen te nemen. Ofwel ijveren we voor een Europees systeem dat de informatie-uitwisseling vergemakkelijkt en stilaan leidt tot gemeenschappelijke regels voor alle landen van de Unie. Spijtig genoeg zal Groot-Brittannië nog lang dwarsliggen. Ofwel gaan we naar strikte regels voor het afluisteren. De machtigingsprocedure mag evenwel niet te zwaar zijn, zodat gevoelige boodschappen kunnen worden onderschept voordat ze uit de communicatiesystemen verdwijnen.*

*Om doeltreffend te zijn moeten onze diensten binnen het half uur kunnen optreden. Inzake pedofilie bijvoorbeeld moeten we bijzonder snel reageren om de bron van de informatie te kunnen achterhalen.*

*In die gevallen mogen we dus geen al te strikte regels opleggen, vooral omdat de CIA en NSA deze regels waarschijnlijk al jaren uit het oog zijn verloren, behalve dan wat de eigen staatsburgers betreft.*

*Het gevaar voor ontsporing bestaat uiteraard. Ik wil dat niet minimaliseren. Ik vind niettemin dat de doeltreffendheid een belangrijk criterium is om de Staatsveiligheid te machtigen boodschappen te onderscheppen.*

*Mijn volgende opmerking heeft betrekking op de providers en speciaal op Microsoft. Het verslag, dat betrekking heeft op Echelon, vermeldt deze kwestie niet. NSA heeft toegang tot alle Microsoft-systemen wereldwijd en dus ook tot de Europese defensie-industrie, de Europese Commissie en de Raad. De heer Solana wordt haast zeker geviseerd, welke bescherming ook is ingebouwd.*

*De monopoliepraktijken van Microsoft werden in de Verenigde Staten al meermaals gehekeld. Het is dan ook geen toeval dat de onderneming haar positie kan behouden. NSA zou deze inlichtingenbron immers niet graag kwijtspelen.*

*Het monopolie van Microsoft ongedaan maken, waardoor meteen ook een einde zou komen aan de samenwerking tussen Microsoft en NSA, zou zeker een goede zaak zijn. Ik vind dat we ons verslag moeten aanvullen met onze informatie over de relaties tussen Microsoft en het Amerikaanse ministerie van Defensie.*

*Magic Lantern is een systeem voor economische spionage dat door het FBI werd ontwikkeld om het werk van de onderzoekers te vergemakkelijken als de versleuteling moeilijk kan worden ontcijferd. Het systeem dient niet om te ontcijferen, maar wel om wachtwoorden en sleutels voor de ontcijfering van boodschappen te onderscheppen. Een aantal parlementsleden heeft het FBI vragen gesteld over de wettelijkheid van dit systeem dat probleemloos toegang verschaft tot de wachtwoorden en werkcodes van de Europese ondernemingen.*

*We vragen niet dat België alleen zou optreden. We mogen niet denken dat ons land hierbij geen belang zou hebben. We willen ons land niet meesleuren in een open oorlog met de Verenigde Staten. We willen niettemin duidelijkheid over de Britse houding terzake, omdat een correcte toepassing van de vrije economische concurrentie aan de grondslag ligt van het lidmaatschap van de Unie. We kunnen hiervan niet afwijken en we hopen dat de regering dit verslag niet alleen ter harte neemt, maar ook belangrijke maatregelen treft.*

*Zo heeft Europa alleen een toekomst als het zijn*

se passer.

Au sujet de toutes les mesures antiterroristes qui se développent sur le territoire, M. Bruguière disait hier encore que nous n'étions qu'au début de la découverte de leur importance. Il est évident que nous devons mieux doter la Sûreté de l'État. Nous devons le faire en prenant un certain nombre de précautions. Soit nous entrons dans un système européen qui facilite la circulation de l'information et aboutit petit à petit à l'établissement de règles valables dans tous les pays de l'Union, mais malheureusement étant donné la présence de la Grande-Bretagne, cela risque de ne pas être possible avant longtemps. Soit nous nous orientons vers l'élaboration de règles strictes qui permettent l'écoute de communications, y compris informatiques. Cependant, la procédure d'autorisation à mettre en place doit être légère de manière à permettre l'interception d'informations qui, lorsqu'elles sont sensibles, n'ont pas une durée de vie très longue au sein des systèmes de communications et risquent donc d'avoir disparu avant d'être interceptées.

Pour être efficace, si nous autorisons l'écoute par nos services, ce que j'estime souhaitable, il faudra rester logique avec la technologie utilisée et permettre d'agir rapidement, dans la demi-heure. Dans le cas de la pédophilie, nous avons appris qu'il fallait aller extrêmement vite pour remonter à la source des informations répréhensibles.

Dans ces cas-là, nous ne devrions pas imposer à nos propres services des règles trop strictes, d'autant plus que, vraisemblablement, la CIA et la NSA auraient quelque peu oublié ces règles depuis de nombreuses années, tout en affichant le respect des mêmes principes vis-à-vis de leurs ressortissants.

Le risque de dérive existe, certes, et je ne veux pas le minimiser mais je voudrais que le volet concernant l'efficacité constitue un des points de référence à l'égard de ce qui sera autorisé en matière d'actions d'écoute par la Sûreté de l'État.

Ma remarque suivante porte sur les *providers*, plus particulièrement sur Microsoft, dont il n'a pas été question dans le rapport parce que celui-ci était consacré à Echelon. Il faut savoir que la NSA peut avoir accès à tous les systèmes Microsoft implantés dans le monde entier : remonter à l'intérieur d'un réseau, prendre connaissance des informations, tant dans une banque que dans une entreprise européenne de défense, voire à l'intérieur des services de la Communauté européenne, de la Commission et du Conseil. M. Solana doit certainement être une des cibles de ce type d'écoutes, quelles que soient les protections prévues.

Il faut également savoir que les pratiques monopolistiques de la firme Microsoft ont été dénoncées à maintes reprises aux États-Unis : de nombreuses plaintes ont été déposées en la matière. Ce n'est pas un hasard si l'ensemble du système reste aux mains de cette entreprise : la NSA ne se privera pas aisément de cette source de renseignements.

Si l'on pouvait faire cesser cette collaboration entre Microsoft et la NSA, en cassant le monopole, ce serait certainement utile. Selon moi, nous devrions compléter notre rapport par les informations dont nous disposons quant aux relations entre Microsoft et le ministère américain de la Défense.

*energiebehoeften kan bepalen en in staat is zijn olie- en aardgasbelangen te beschermen. Dat kan alleen via een breed opgevat Europees systeem.*

*De dienst die we in België willen oprichten, bestaat al in de Verenigde Staten: het gaat om de in 1997 opgerichte National infrastructure protection.*

*In deze nieuwe dienst werken 120 experts in een centrum voor de bescherming van de computersystemen en moeten 200 specialisten, verspreid over alle FBI-districten, inlichtingen vergaren ingeval van buitenlandse inmenging.*

*Een dergelijke structuur willen we ook oprichten.*

*De Amerikanen hebben het gevaar al lang begrepen. Met deze nieuwe dienst tonen ze aan dat ze ook beseffen dat anderen zich aanpassen aan de technologische evolutie.*

*Wij hebben geen 120 personen nodig, maar wel een dienst met betrouwbare experts met een aangepaste bezoldiging.*

*Welke Belgische ondernemingen zouden we kunnen beschermen? Solvay, UCB, Kredietbank, Tessenderlo, Interbrew? Maar wat doen we dan met General Motors, Ford of Volvo? Aan wie moeten we informatie verstrekken?*

*Het moet dus gaan om een Europese dienst. Ik heb samen met enkele specialisten verschillende technieken bestudeerd. Als de technologische evolutie zich verder doorzet, geeft dit onderzoek aanleiding tot ongerustheid omwille van onze passiviteit.*

*Zelfs het Witte Huis heeft een White House Cyberspace Security adviser. Ik weet niet of de eerste minister een dergelijke adviseur heeft, maar hij moet zich omringen met mensen die hem de gepaste technologische conclusies kunnen voorleggen.*

*Kortom, onze fractie vindt dat een operationele en betrouwbare dienst nodig is ter versterking van de Staatsveiligheid, zodat de gaten in de Belgische kaas in dit opzicht kunnen worden opgevuld.*

Deux mots encore à propos d'un système intéressant appelé *Magic Lantern* et longuement explicité dans une édition du *Figaro* l'année dernière. Ce système permet de faire de l'espionnage économique et a été développé par le FBI pour faciliter le travail des enquêteurs lorsque le cryptage est devenu trop difficile à casser : il s'agit non plus d'une pratique de décryptage mais d'interception des mots de passe et des clés utilisées pour crypter les messages. Certains parlementaires américains ont interrogé le FBI à ce sujet et cette pratique, qui ne devrait pas dépasser le cadre légal et permet d'avoir accès, sans la moindre difficulté, aux mots de passe et aux différents codes de travail des entreprises européennes.

Nous ne souhaitons pas que la Belgique fasse cavalier seul en la matière. Il s'agit, en l'occurrence, d'une opinion politique. Ce serait rêver de penser que notre pays aurait le moindre intérêt à agir de la sorte. Nous ne voulons pas vous entraîner dans une guerre ouverte avec les États-Unis. Cependant, nous voulons clarifier le comportement britannique en la matière dans la mesure où le *fair competition*, c'est-à-dire le fait d'être correct dans la compétition économique, doit être un élément de base du comportement à l'intérieur de l'UE où il y a d'importantes zones à protéger. Nous ne pouvons dès lors pas nous détourner de cette obligation et nous espérons que cela incitera le gouvernement non seulement à prendre ce rapport au sérieux mais également à prévoir d'importantes mesures.

On peut imaginer que l'avenir de l'Europe se situera dans sa capacité de définir ses intérêts énergétiques pétroliers, surtout si on arrive à appliquer la décision du gouvernement de fermer les centrales nucléaires entre 2015 et 2025.

Le temps presse pour savoir comment nous allons protéger nos intérêts pétroliers et gaziers.

En réfléchissant, il est évident que la dimension de la protection de nos intérêts énergétiques futurs dépendra de notre capacité d'organiser correctement un système européen d'envergure.

Le service que nous vous proposons de créer en Belgique existe aux États-Unis : c'est le *National infrastructure protection* mis en place en 1997. Il n'est donc pas si ancien si l'on pense que l'accord entre les États-Unis et l'Angleterre date de 1948.

Imaginez la création d'un nouveau service : 120 experts qui s'occupent d'un centre de protection des systèmes informatiques et 200 spécialistes qui travaillent dans tous les districts du FBI et qui sont chargés de la collecte de renseignements en cas d'intrusion du territoire américain.

Cette structure devrait être la référence de ce que nous souhaitons créer.

Les Américains ont depuis longtemps compris le danger et, en créant ce nouveau service en 1997, ils démontrent qu'ils ont aussi compris que d'autres s'adaptent à la qualité technologique de ce qui est en train de se produire au niveau mondial.

Sans avoir besoin d'un service de 120 personnes, il nous faut un service d'experts fiables, dont les rémunérations devront être adaptées dans un cadre spécifique.

Si l'on imagine que l'on mènerait une politique qui protégeât nos entreprises, quelles seraient les entreprises que nous devrions considérer comme belges ? Solvay, l'Union chimique, la Kredietbank, Tessenderlo, Interbrew ? Mais que faire de General Motors, de Ford ou de Volvo ? À qui donner les informations sur ces matières.

L'efficacité au niveau belge ne peut justifier un tel type de service qui doit être à vocation européenne avec des questions techniques auxquelles il conviendra de répondre.

Nous pourrions encore approfondir diverses techniques. J'ai pris le temps de le faire avec un certain nombre de spécialistes que je remercie. Cependant, si l'évolution technologique continue, elle constitue une source d'inquiétudes par rapport à notre passivité.

Même la Maison Blanche a créé un *White House Cyberspace Security adviser*. Je ne sais pas si le Premier ministre en a un, mais je pense que chaque premier ministre devrait s'entourer des éléments capables de lui donner les conclusions détaillées que la technologie qui nous entoure exige.

Voilà ce que nous souhaitions vous dire au nom de notre groupe : il faut un service renforçant la Sûreté de l'État, opérationnel et fiable, pour que l'aspect « État gruyère » de la Belgique puisse être géré, au moins en cette matière.

***De heer Georges Dallemagne (PSC)**. – Ik dank de rapporteurs voor hun voortreffelijk verslag. Gezien de ernst van de inlichtingen over verschillende gesofisticeerde systemen om Staten, ondernemingen en burgers af te luisteren, was dit werk noodzakelijk. Vandaag bevestigt men het bestaan van die systemen. Er werd aangetoond dat inbreuken werden gepleegd op een hele reeks nationale en internationale wettelijke bepalingen: de bescherming van de persoonlijke levenssfeer, het Europees Verdrag tot bescherming van de rechten van de mens en sommige artikelen van het Verdrag betreffende de Europese Unie. Het gaat dus om een bijzonder ernstige zaak die het wankele evenwicht van onze democratieën kan verstoren en sommige van hun fundamentele waarden en steunpijlers aantast. Bovendien ontstaat daardoor onenigheid over het begrip bevriend land, bondgenoot, partner in het kader van de Europese Unie of van andere internationale organisaties. Die onenigheid zou aanleiding kunnen geven tot een verslechtering van onze onderlinge relaties.*

*Deze problemen verdienen mijns inziens een krachtige reactie. Ik heb dus met belangstelling kennis genomen van de aanbevelingen van het verslag. Toch blijf ik wat in de kou staan. Hoofdprobleem vandaag is zo snel mogelijk afrekenen met die spionagesystemen. De heer Hordies heeft verklaard dat de bevolking, de ondernemingen en de Staat moeten worden gewaarschuwd. Wij zouden ons in een vlucht vooruit kunnen gooien: zij bespioneren ons, laten wij ze dus ook maar bespioneren en contraspionagesystemen opzetten.*

*De aanbevelingen gaan in de richting van het opzetten van eigen beschermings-, afluister- en onderscheppingssystemen via een betere coördinatie op Europees niveau.*

*Ik zou graag hebben dat er inspanningen worden gedaan om te achterhalen hoe wij het patrimonium, het onderzoek en de producten van onze ondernemingen in Luik, in Gent of elders beter tegen spionage kunnen beschermen.*

**M. Georges Dallemagne (PSC)**. – Je voudrais tout d'abord remercier les auteurs du rapport pour la qualité de leur travail. Je pense qu'il s'agissait d'un travail nécessaire étant donné la gravité des informations qui circulaient à propos de divers systèmes sophistiqués d'écoute des États, des entreprises et des citoyens. Leur existence est à présent confirmée. Des infractions à toute une série de dispositions légales nationales et internationales, qu'il s'agisse de la protection de la vie privée, de la convention européenne de sauvegarde des droits de l'homme ou encore de certains articles du traité de l'Union européenne, sont désormais établies. Il s'agit donc d'une affaire particulièrement grave, qui fragilise l'équilibre de nos démocraties, qui met à mal certaines valeurs fondamentales et certains dispositifs sur lesquels nos démocraties sont basées. Par ailleurs, cela jette un trouble important sur ce que peut encore signifier la notion de pays ami, de pays allié, de partenaire dans le cadre de l'Union européenne ou d'autres organisations internationales. Ce trouble pourrait être à l'origine d'une détérioration des relations qui peuvent exister entre nous.

Je pense qu'il faut pouvoir réagir fermement par rapport à l'ensemble de ces problèmes. J'ai donc pris connaissance avec intérêt des recommandations du rapport. Toutefois, je reste un peu sur ma faim. Le problème principal auquel nous sommes aujourd'hui confrontés est de mettre rapidement un terme à ces systèmes d'espionnage. M. Hordies a déclaré qu'il fallait mettre la population, les entreprises et l'État en garde. Nous pourrions nous lancer dans une fuite en avant : ils nous espionnent, espionnons-les à notre tour, mettons en place des systèmes de contre-mesures.

Les recommandations tendent à faire valoir que nous pourrions créer nos propres systèmes de protection et nos propres systèmes d'écoute et de renseignement à travers une meilleure coordination à l'échelon de l'Union européenne.

En ce qui me concerne, j'aimerais que nous nous efforcions

*De aanbevelingen van de commissie op dat vlak zijn nogal bondig. Ik hoop dat de regering ons wat meer uitgewerkte voorstellen zal kunnen doen. Mevrouw Lizin had het over de oprichting van een dienst om de Staatsveiligheid te versterken. Ik steun die idee en wil er nog aan toevoegen dat er ook een dienst ten behoeve van de bedrijven en de burgers moet worden opgericht.*

*Ik kom nu tot een ander punt. Aangezien er sprake is van inbreuken op een reeks wettelijke bepalingen – ik weet niet of het nodig is het juridisch arsenaal uit te breiden – moeten wij de regering horen over de mogelijke sancties, vervolgingen, klachten. Wij zijn blijkbaar bereid ons daarvoor in te zetten. Ik heb gehoord dat onze voorzitter zich in de media ongerust maakt over het bestaan van afluistersystemen. Wij moeten concrete daden stellen in het kader van de bestaande wetgeving. Ik zal nauwgezet toekijken op de voorstellen van de regering.*

*Ik had soms de indruk dat men wat te voorzichtig was. In de eerste aanbeveling werd voorgesteld politieke en juridische vragen te stellen. Men moet wat duidelijker zijn over de initiatieven die moeten worden genomen.*

*De Europese Unie heeft de plicht haar belangen en waarden met de gepaste instrumenten te beschermen, maar men moet zich hoeden voor een vlucht vooruit waarbij elke grootmacht of coalitie van grootmachten zich van afluister- en contraspionagesystemen voorziet.*

***De heer Armand De Decker (PRL-FDF-MCC)**. – Als voorzitter van de Commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingendiensten wil ik mijn analyse mededelen na twee jaar werkzaamheden.*

*Dit debat geeft een bijzonder goed beeld van de wereld die we nu binnengaan en die helemaal niet meer lijkt op de wereld die we kenden net na de tweede wereldoorlog. De huidige technologieën bestaan en zullen niet ongedaan worden gemaakt. De samenleving moet zich dus aanpassen. We moeten de nodige juridische en technische middelen vinden om de rechten en de vrijheden van de burgers in deze nieuwe context te beschermen.*

*Dit verslag heeft onze begeleidingscommissie bijzonder veel geleerd over de problematiek van de inlichtingendiensten waarop wij toezicht moeten uitoefenen. In Europa en de wereld hebben maar heel weinig landen een democratische controle op hun inlichtingendiensten. De Verenigde Staten hebben dat wel. In Frankrijk geschiedt de controle uitsluitend door de regering, zonder enige inbreng van het parlement.*

*Door onze naoorlogse geschiedenis waren wij ons er wel van bewust dat de grootmachten hun belangen zo veel mogelijk wilden vrijwaren in het kader van de Oost-Westrivaliteit en dat ze dus belangrijke inlichtingendiensten en -systemen hadden uitgebouwd.*

*Nu hebben we echter vernomen dat ook veel kleinere en bevriende landen beschikken over afluistersystemen die ze gebruiken, niet alleen om hun strategische belangen te verdedigen, maar ook om veel algemenere informatie te*

de vérifier dans quelle mesure nous pourrions mieux protéger le patrimoine, les recherches et les produits de nos entreprises, à Liège, à Gand ou ailleurs, vis-à-vis de l'espionnage.

Les recommandations de la commission me semblent relativement sommaires sur ce plan et j'espère que le gouvernement pourra nous présenter des propositions plus élaborées. Mme Lizin a évoqué la création d'un service qui permettrait de renforcer la Sûreté de l'État. Je souscris à cette idée, en ajoutant qu'il faut aussi mettre en place un service au bénéfice des entreprises et des citoyens.

J'en viens à un autre élément. Puisqu'il y a infraction à une série de dispositions légales – j'ignore s'il est nécessaire d'augmenter cet arsenal juridique aujourd'hui –, nous devons entendre le gouvernement sur les possibilités de sanctions, de poursuites, de plaintes. Il semble que nous ayons la volonté de nous mobiliser ; j'ai entendu notre président s'inquiéter dans les médias de l'existence de ces systèmes d'écoute. Nous devons poser des actes concrets dans le cadre du droit existant. Je serai attentif aux propositions du gouvernement.

J'ai parfois eu l'impression d'un excès de prudence. La première recommandation proposait de poser les questions politiques et juridiques. Il s'agit d'être un peu plus clair sur les initiatives à prendre.

Il incombe à l'Union européenne d'utiliser les outils nécessaires à la protection de ses intérêts et de ses valeurs, mais il faut se garder d'une fuite en avant où chaque grande puissance ou groupement de puissances se doterait de moyens d'écoute et de contre-mesures. J'espère que nous opterons pour des dispositifs qui permettront de protéger la vie privée, les intérêts des entreprises et les valeurs de nos États.

**M. Armand De Decker (PRL-FDF-MCC)**. – Il n'est pas courant pour moi de prendre la parole dans cet hémicycle, mais comme j'ai eu le privilège de présider le Comité de suivi du Comité permanent de contrôle des services de renseignement sur ce sujet et que je pense y avoir joué un rôle significatif, tout comme nos collègues, il me paraît important de vous exprimer mon analyse à l'issue de ces deux années de travail.

Ce débat est excessivement révélateur du monde dans lequel nous entrons et qui ne ressemble absolument plus à ce que nous avons connu dans l'après-deuxième guerre mondiale. Les technologies actuelles sont bien là ; on ne les « désinventera » pas. Il faut que nos sociétés s'y adaptent et que nous trouvions les moyens juridiques et techniques de protéger les droits et libertés des citoyens, dans ce contexte nouveau.

Ce rapport que nous avons établi a été extrêmement instructif pour notre commission du suivi. Le fait de nous y atteler nous a considérablement armés par rapport à l'ensemble de la problématique du renseignement que nous avons, dans notre pays, le privilège de contrôler. Il faut savoir que très peu de pays en Europe et dans le monde disposent d'un contrôle démocratique sur leurs services de renseignement. C'est le cas aux États-Unis, mais ce ne l'est pas en France où le contrôle est exclusivement exercé par le gouvernement, sans aucune dimension parlementaire.

Ce fut très instructif pour nous et cela nous a surtout considérablement ouvert les yeux sur les agissements des

*verkrijgen.*

*We hebben het hierbij uitsluitend over globale afluistersystemen, niet over gerichte administratieve telefoontaps die het gerecht in ons land, en de inlichtingendiensten in andere landen, mogen uitvoeren in het kader van onderzoeken, de bestrijding van banditisme of terrorisme, enzovoort.*

*Het gaat om globale afluistersystemen die heel wat landen in staat stellen satellietgesprekken over de hele wereld te beluisteren. Echelon is zeker niet het enige systeem dat in staat is tot dergelijke intercepties.*

*Het gebruik dat sommigen willen maken de satellieten, die vooral voor communicatie worden gebruikt, is juridisch niet duidelijk geregeld. De komende jaren zal zich waarschijnlijk een ruim toepassingsgebied van internationaal publiek recht ontwikkelen.*

*We zullen uiteraard moeten nagaan in welke mate een internationale wetgeving op het opvangen van informatie via satelliet in de praktijk mogelijk is. Het gaat om berichten via GSM, fax en e-mail, en ook om totale afluistersystemen voor informatie die via onderzeese communicatiekabels wordt doorgestuurd. Dat is wel een veel ouder systeem, maar het bestaat nog en het wordt nog gemoderniseerd.*

*Die inlichtingendiensten werden meestal tijdens de koude oorlog opgericht. Vandaag worden ze ingeschakeld bij de bestrijding van banditisme en terrorisme, maar waarschijnlijk ook voor economische spionage. Dat gebeurt zelfs tussen bondgenoten en bevriende staten.*

*In het verslag wijzen we erop dat het Echelon-systeem waarschijnlijk bestaat. De heer Dallemagne spoort ons aan iets te doen om die praktijken te doen ophouden. Hij lijkt niet te beseffen dat een Amerikaanse afluisterdienst over evenveel middelen en personeelsleden beschikt als het hele Belgische leger. We moeten niet geloven dat wij de Verenigde Staten, via diplomatiek overleg, kunnen overtuigen om daarmee te stoppen.*

*Mevrouw Lizin legt zeer sterk de nadruk op het Echelon-systeem en op de betrokkenheid van Europese landen bij activiteiten van de Verenigde Staten via dit systeem.*

*Wat ik het meest nieuw, ongewoon en ergerlijk vind, is dat landen van de Europese Unie, die bevriende Staten, bondgenoten en partners in die Unie zijn, over globale afluistersystemen beschikken die de hele wereld bestrijken. Dat is het geval voor Frankrijk, Duitsland en Groot-Brittannië. Maar ook kleinere landen, zoals Nederland en Denemarken hebben globale afluistersystemen, ook al zijn die eenvoudiger.*

*Wij leven dus in een Europese Unie waarin sommige van onze beste politieke vrienden, bondgenoten en partners dagelijks luisteren naar en inlichtingen inwinnen over wat hun vrienden en partners doen. Dat is een even belangrijk element van ons verslag als de conclusie dat het Echelon-systeem waarschijnlijk bestaat. Ik dacht wel dat de Verenigde Staten een belangrijk systeem hadden. Maar vóór we deze werkzaamheden aanvatten, wist ik niet dat onze partners van de Europese Unie over zulke uitgebreide systemen beschikten, die duizenden personen tewerkstellen en macrocomputers gebruiken die werken met sleutelwoorden en die enorm veel*

États.

Nous avions, par la force même de notre histoire de l'après-deuxième guerre mondiale, conscience que les grandes puissances agissaient au mieux de leurs intérêts dans le cadre de la rivalité Est-Ouest et que ces grandes puissances s'étaient donc dotées de systèmes et services de renseignements importants.

Ce que nous avons en revanche appris ici, c'est que des pays beaucoup plus modestes et amis se dotaient, eux aussi, de systèmes d'écoute globale et s'en servaient, non seulement dans le cadre de la défense de leurs intérêts stratégiques mais aussi dans une volonté de renseignement beaucoup plus générale.

De quoi s'agit-il ? Peut-être cela n'a-t-il pas été suffisamment précisé, même si madame Lizin en a parlé au début de son rapport. Nous parlons exclusivement des systèmes d'écoute globale et ne nous intéressons pas aux écoutes administratives ponctuelles que, dans notre pays, la justice, dans d'autres pays, les services de renseignements peuvent effectuer dans le cadre d'enquêtes, de lutte contre le banditisme ou le terrorisme, etc.

Il s'agit de systèmes d'écoute globale permettant à de nombreux pays d'écouter les communications par satellites de la planète entière et de mettre sur pied, à cette fin, des services d'importance évidemment variable. Il ne faut pas croire qu'Echelon soit le seul système capable de telles interceptions.

Ceci m'amène à rappeler que le statut juridique des satellites, utilisés notamment pour les communications, n'est pas très clairement défini quant à l'usage que les uns et les autres peuvent décider d'en faire. La matière n'est pas réglée et il subsiste là un vaste champ de droit international public qui se développera probablement dans les années à venir.

Évidemment, il faudra voir dans quelle mesure le respect d'une éventuelle législation internationale sur le captage des informations passant par satellites pourra se réaliser dans la pratique. Il s'agit essentiellement des messages passant par GSM, par fax et par *e-mail* mais aussi des écoutes globales des informations passant par câbles sous-marins, système certes beaucoup plus ancien mais existant toujours et se modernisant.

Ces services ont été créés, la plupart du temps, pendant la guerre froide. Aujourd'hui, ils servent bien sûr à des fins légitimes de lutte contre le grand banditisme et le terrorisme mais probablement aussi à l'espionnage économique. Ces pratiques se développent même entre alliés et amis.

Nous révélons ici que le système Echelon existe probablement. Il est d'une importance considérable. Lorsque monsieur Dallemagne nous exhorte à faire quelque chose pour que ces pratiques cessent, il semble ignorer qu'un service d'écoute américain dispose à lui seul d'un budget égal à celui de toute l'armée belge et emploie 40.000 personnes, soit autant que l'ensemble de l'armée belge. Il ne faut pas croire que nous parviendrons demain, par une simple négociation diplomatique, à convaincre les États-Unis d'arrêter ce genre de systèmes.

Sur un point, ma sensibilité se différencie quelque peu de celle de madame Lizin qui insiste très profondément sur le

*informatie kunnen vergaren.*

*Voor mij is dit, net als voor de heren Vandenberghe en Hordies, een politiek probleem. Wat moeten wij doen? De opdracht van de Veiligheid van de Staat is vastgelegd in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, meer bepaald in artikel 7, §1, waar hij als volgt wordt omschreven: "het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige 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". Onze Veiligheid van de Staat kan die wettelijk opdracht niet uitvoeren met betrekking tot de globale afluisterpraktijken vanuit talrijke landen.*

*Dat is de politieke conclusie ten gronde die we moeten trekken. We moeten de regering vragen hoe volgens haar op deze technologische evolutie moet worden gereageerd. Aangezien het huidig wettelijk kader de Veiligheid van de Staat niet de technologische middelen geeft waarmee ze kan nagaan wie ons afluistert, wanneer, waarom en waarover, moeten wij ons hierover bezinnen en ons land een systeem geven dat het beschermt tegen en inlicht over de afluisterpraktijken waarvan het het voorwerp is.*

*Ons land, dat onderdak biedt aan de Atlantische alliantie, de Europese Unie en duizenden internationale instellingen van diverse omvang, heeft zeker geen cultuur inzake inlichtingen en veiligheid. Wij moeten onze bedrijven, besturen, ministeriële kabinetten, landgenoten die meewerken aan gevoelige wetenschappelijke onderwerpen dan ook een echte inlichtingen- en veiligheidscultuur inprenten.*

*Op dat gebied beschikken wij over troeven, want onze universiteiten behoren tot de meest gerenommeerde op het gebied van de encryptiesystemen.*

*Ook de Europese Unie moet zich over het probleem bezinnen. Ons verslag is vrijmoediger dan dat van het Europees parlement omdat wij niet over een globaal afluistersysteem beschikken en alleen onze militaire inlichtingendienst in het buitenland gesprekken mag afluisteren met het oog op de bescherming van onze militaire belangen. Ons land is dan ook vrijer om, via dit verslag, denksporen aan te wijzen voor de toekomst van Europa op dit gebied. De Europese Unie heeft belangrijke staatkundige bevoegdheden en beheert een gemeenschappelijke munt. Het is niet normaal dat ze nog niet beschikt over een systeem waarmee ze haar belangen kan beschermen. Ons land zou de reflectie daarover binnen de Europese Unie kunnen aanzwengelen. Hetzelfde probleem rijst, op een andere wijze, binnen de Atlantische Alliantie. Ook daar zouden we onze partners in alle openheid en sereniteit kunnen aanspreken over Echelon en de Britse betrokkenheid daarbij.*

*Ons verslag heeft ertoe bijgedragen dat de democratie en het parlement zich bewust werden van dit belangrijke probleem. Als het verslag wordt aangenomen, zullen we in de Senaat een colloquium organiseren. We zullen alle in de Europese Unie bestaande parlementaire controlecommissies op de inlichtingendiensten uitnodigen om samen met ons na te*

système Echelon et sur la complicité de pays européens, la Grande-Bretagne et d'autres dans le passé, à la démarche des États-Unis via ce système.

Ce qui m'est apparu le plus nouveau, le plus inusité et le plus choquant est de découvrir que des pays de l'Union européenne, amis et alliés, partenaires dans cette Union, disposaient de systèmes d'écoute globaux parcourant la planète. C'est le cas de la France, l'Allemagne et la Grande-Bretagne. Mais des pays plus petits, comme les Pays-Bas et le Danemark, ont également des systèmes d'écoute globaux, même s'ils sont plus modestes.

Nous vivons donc dans une Union européenne où certains de nos meilleurs amis politiques, alliés et partenaires, écoutent et se renseignent quotidiennement sur ce que font leurs amis et partenaires. C'est un élément au moins aussi important de notre rapport que la conclusion que le système Echelon existe probablement. J'imaginais bien que les États-Unis avaient un système important, mais je ne savais pas, avant d'avoir entamé ce travail, que nos partenaires au sein de l'Union européenne disposaient de systèmes aussi développés, utilisant des milliers de personnes et des systèmes de macro-ordinateurs fonctionnant avec des mots clés et parvenant à recueillir énormément de renseignements.

Pour moi, comme pour M. Vandenberghe et M. Hordies, la question est politique. Que devons-nous faire ? La mission de la Sûreté de l'État est définie par la loi, dans l'article 7 §1er, et consiste à « rechercher, analyser, 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 ». Par rapport aux écoutes globales qui se font au départ de très nombreux pays de par le monde, notre Sûreté de l'État n'est pas en mesure de remplir cette mission légale.

C'est une conclusion politique de fond que nous devons poser aujourd'hui et nous devons interroger le gouvernement quant à la vision qui est la sienne de la réponse à apporter à cette évolution technologique. Étant donné que le cadre légal actuel ne donne pas à la Sûreté de l'État les moyens technologiques permettant de vérifier qui nous écoute, à quel moment, dans quel but, sur quel objet, je pense qu'il est indispensable que nous menions une réflexion à ce sujet et que nous dotions notre pays d'un système de veille et de renseignements sur les écoutes dont nous faisons l'objet.

Notre pays, qui accueille l'Alliance atlantique, l'Union européenne ainsi que des milliers d'institutions internationales de tailles diverses n'a indiscutablement pas suffisamment une culture du renseignement et de la sécurité. Il est de notre devoir, dans le monde dans lequel nous vivons aujourd'hui, d'inculquer à nos entreprises, à nos administrations, à nos cabinets ministériels, à nos concitoyens qui travaillent sur des sujets scientifiques sensibles une sérieuse et réelle culture du renseignement et de la sécurité.

Nous avons d'ailleurs à cet égard des atouts, puisque nos universités sont parmi les plus réputées dans les différentes technologies de cryptage. Cela me paraît important.

Deuxièmement, une réflexion doit avoir lieu au niveau de l'Union européenne. Le rapport que nous avons préparé ici a

*denken over deze problematiek. We zullen de parlementen van de landen die nog niet beschikken over een parlementair controlesysteem uitnodigen om onze werkzaamheden bij te wonen, zodat ze daar ervaring uit kunnen putten en de mentaliteit daarover in hun eigen land kan rijpen.*

*Het verslag over Echelon toont aan dat deze zaak niet zuiver Amerikaans of Angelsaksisch is. Ze is fundamenteel Europees en wat de principes betreft, is dit probleem even ernstig tussen de partners van de Europese Unie als tussen de partners van de Atlantische Alliantie. Wat onze beste vrienden en bondgenoten binnen de Europese Unie doen, is juridisch, politiek en moreel even betwistbaar als wat de Angelsaksen doen via Echelon.*

**De heer Marc Verwilghen**, minister van Justitie. – Ik zal mijn betoog in twee delen opsplitsen. Eerst wil ik een meer algemene beschouwing geven over het Echelon-netwerk en in een tweede deel zal ik ingaan op het verslag, de aanbevelingen en de conclusies die eruit moeten worden getrokken en het standpunt van de regering dienaangaande toelichten.

Nog geen anderhalf jaar geleden heeft de Senaat een wetsontwerp goedgekeurd met betrekking tot de informaticacriminaliteit. We hebben er ons toen, op basis van enkele aanbevelingen van de Raad van Europa en van proefondervindelijke waarnemingen in onze eigen samenleving, rekenschap van gegeven dat het in bepaalde omstandigheden mogelijk is binnen te dringen in andermans

la particularité d'être plus franc que celui du Parlement européen pour la bonne et simple raison que notre pays ne dispose pas de système d'écoute global et que parmi nos services, seul le service de renseignement militaire dispose de l'autorisation d'écouter à l'étranger dans un but de protection de nos intérêts militaires. Notre pays, qui a donc les mains plus libres que d'autres dans l'Union européenne, a été capable, à travers ce rapport, de proposer des pistes plus utiles à l'avenir de l'Europe dans ce domaine. Je pense en effet qu'il est indispensable de mesurer aujourd'hui que l'Union européenne détient des compétences de nature étatique d'une très grande importance et gère aujourd'hui une monnaie commune. Il est assez anormal qu'une Union européenne qui a des compétences d'une telle importance ne se soit pas encore dotée d'un système de protection qui lui permette de protéger des intérêts aussi importants. Notre pays pourrait peut-être jouer le rôle d'instigateur d'une réflexion à ce sujet au sein de l'Union européenne. Le même problème se pose, mais différemment, au sein de l'Alliance atlantique, dans la mesure où la question d'Echelon et du partenariat britannique dans Echelon pourrait très bien être posée politiquement et diplomatiquement, mais en toute franchise et sérénité, à nos partenaires autour de la table de l'Alliance atlantique.

Enfin, l'intérêt de notre rapport a été de participer au développement d'une prise de conscience démocratique et parlementaire progressive dans ce domaine très important. Nous essayerons de remplir notre rôle en organisant un colloque au Sénat, si ce dernier vote le rapport. Nous inviterons toutes les commissions parlementaires de contrôle des services de renseignement de l'Union européenne qui existent à venir réfléchir sur ces sujets avec nous. Nous inviterons les Parlements des pays qui n'ont pas de système de contrôle parlementaire à assister à nos travaux et à en retirer une certaine expérience qui sera probablement de nature à faire évoluer les mentalités et les esprits dans leurs propres pays.

Monsieur le ministre, ce qui m'importe, c'est que le rapport Echelon révèle que la matière n'est pas exclusivement américaine ni anglo-saxonne, que ce domaine est fondamentalement européen et qu'au niveau des principes, ce problème est aussi grave entre partenaires de l'Union européenne qu'entre les partenaires de l'Alliance atlantique. Ce que font nos meilleurs amis et alliés au sein de l'Union européenne est, aux plans juridique, politique et moral, aussi critiquable que ce que font, à travers Echelon, les anglo-saxons.

***M. Marc Verwilghen**, ministre de la Justice. – Je commencerai par quelques considérations générales relatives au réseau Echelon pour m'attarder ensuite sur le rapport et la position du gouvernement.*

*Il y a moins d'un an et demi, le Sénat a adopté un projet de loi relatif à la criminalité informatique. Nous nous sommes rendus compte que des intrus pouvaient s'introduire dans des systèmes informatiques. Le progrès technologique ne garantit donc pas toujours la confidentialité des systèmes.*

*Ayant constaté les carences de notre droit pénal, nous avons introduit les concepts de hacking, tagging et sabotage de données. La Belgique fut le premier pays du Conseil de l'Europe à intégrer de telles règles dans son droit national. Ce faisant, nous avons compris que pour être vraiment*

informaticasysteem. Deze vergelijking geeft duidelijk aan dat in de technische vooruitgang niet altijd de zekerheid wordt ingebouwd dat anderen er niet in kunnen binnendringen.

Toen we vaststelden dat het eigen strafrecht tekortschoot, hebben we een aantal nieuwe definities en tenlasteleggingen ingevoerd zoals *hacking*, *tagging* en datasabotage. België was hiermee het eerste land binnen de Raad van Europa dat dergelijke regels in zijn nationaal recht opnam. Tegelijk hebben we ingezien dat we, om echt performant te kunnen optreden, een stap verder moesten gaan en dat op internationaal vlak een brede consensus tot stand moest worden gebracht. We hoopten dat ook de andere leden van de Raad van Europa een gelijkaardig initiatief zouden nemen.

Natuurlijk moeten we er ook rekening mee houden dat wat zich in de individuele sector tussen fysieke personen en rechtspersonen afspeelt ook een maatschappelijke dimensie heeft. Dit leidt ons onmiddellijk tot de relaties tussen continenten en tussen verschillende landen.

Dit alles maakt het debat van vandaag een beetje onwezenlijk: het is abstract, maar zonder dat we het beseffen kan het tegelijkertijd ook zeer concreet zijn. We dreigen dan ook verwikkeld te raken in een strijd die te vergelijken is met de strijd van David tegen Goliath of van Don Quichote die we terugvinden in de werken van Cervantes en Telemann. Anderzijds mogen we niet het onmogelijke vragen. Enige realiteitszin is geboden; dit hebben sommige sprekers duidelijk laten blijken.

Afluisteren heeft niet zozeer te maken met de nieuwsgierigheid die de mensen eigen is, maar vooral met de wens om kennis te verwerven over de intenties van de ander. Kennis is immers macht.

*In 1998 werden in de Kamer en in de Senaat verschillende parlementaire vragen gesteld. Dit verslag is in zekere zin de concrete uitwerking van de antwoorden op die vragen.*

*Door een aantal gebeurtenissen die zich de jongste tijd hebben voorgedaan zien we de zaken vandaag enigszins anders. Ik denk onder meer aan de aanslagen van 11 september 2001 die de inlichtingendiensten niet konden voorkomen.*

*In eigen land was er het veelbesproken faillissement van Lernaut & Hauspie en het vermeende verband met het Echelon-systeem.*

*We bevinden ons dus in een heel bijzondere situatie.*

Meer zelfs, we moeten er ons rekenschap van geven dat technisch wel veel, maar toch niet alles mogelijk is. Dat is een eerste uitgangspunt. Dat we niets mogen uitsluiten en van de veronderstelling moeten uitgaan dat niet alles kan en dat de doelstellingen niet altijd even nobel zijn, is een tweede uitgangspunt.

In die omstandigheden moet men zich ervoor hoeden te snel in complottheorieën terecht te komen. Ik begrijp dan ook de opmerking van bepaalde sprekers met betrekking tot uitspraken van de eerste burger van ons land.

Dit toont de waarde aan van *freedom of speech*. Ik ben zelf te lang parlementslid om de waarde daarvan niet te onderkennen. Met *freedom of speech* bedoel ik de vrijheid om

*performants, nous devions franchir une étape supplémentaire en essayant d'atteindre un large consensus au plan international. Nous espérions que les autres membres du Conseil de l'Europe prendraient une initiative semblable.*

*Nous ne devons évidemment pas oublier que les interactions entre les personnes physiques et morales comportent également une dimension sociétale. Ceci nous amène aux relations entre continents et entre différents pays.*

*Tout ceci rend le présent débat apparemment abstrait, même s'il peut se révéler très concret. Nous risquons d'être impliqués dans un combat comparable à celui de David contre Goliath. Nous ne pouvons cependant pas demander l'impossible. Il faut être réaliste, comme l'ont expliqué certains orateurs.*

*Les systèmes d'écoute ne sont pas tant liés à la curiosité de l'homme qu'à la volonté de connaître les intentions d'autrui. En effet, savoir, c'est pouvoir.*

En 1998, plusieurs questions parlementaires ont été posées tant à la Chambre qu'au Sénat. Elles nous ont amené des informations dont le rapport actuel constitue en quelque sorte la concrétisation.

Aujourd'hui, nous voyons les choses autrement à cause des événements qui ont, entre-temps, secoué l'actualité. À commencer par les attentats du 11 septembre 2001 et l'échec des services de renseignements.

Sur le plan national, citons la faillite retentissante de Lernaut & Hauspie et les liens que l'on a fait, à tort ou à raison, avec le système Echelon.

C'est dire que nous nous trouvons dans une situation à tout le moins particulière.

*Nous devons être conscients que les possibilités techniques sont larges, mais pas infinies. En outre, tout n'est pas permis. Tous les objectifs ne sont pas aussi nobles les uns que les autres.*

*Nous devons dès lors nous garder d'évoquer de quelconques théories de complot. Je comprends dès lors les remarques de certains orateurs relatives aux déclarations du premier citoyen de notre pays.*

*Ceci prouve la valeur de la liberté d'expression. J'entends par là la liberté d'exprimer son opinion pour autant qu'on puisse prouver ses déclarations ou que l'on puisse en tout cas avancer des éléments qui en constituent la réflexion pour*

zijn mening te kunnen uiten, waarbij men zijn uitspraken uiteraard hard moet kunnen maken of alleszins elementen moet kunnen aanhalen die er op zijn minst de reflectie naar de toekomst van vormen.

Na deze algemene inleiding wil ik namens de regering de rapporteurs feliciteren met hun uitstekend verslag. Het is een goed gedocumenteerd geheel geworden, dat het bestaan van het Echelon-netwerk vanuit diverse oogpunten heeft benaderd, wat de mogelijkheid biedt de omvang en de mogelijke dreiging van het systeem beter in te schatten en in een ruimer perspectief te plaatsen. De regering wenst hierop eerst dieper in te gaan alvorens de aanbevelingen van naderbij te bekijken.

De regering gaat ervan uit dat, op basis van open bronnen en van verschillende onderzoeksrapporten dienaangaande, blijkt dat het Echelon-interceptiesysteem wel degelijk bestaat. Hierover mag geen onduidelijkheid bestaan. Met andere woorden, de regering deelt de stelling die ook in het verslag wordt verdedigd, met name dat het het Parlement toekomt de afweging te maken van de waarachtigheid van bepaalde gegevens, die overigens vergaande gevolgen kunnen hebben voor de verhouding met andere landen, om een juridische kwalificatie te geven aan deze feiten en er de politieke gevolgen aan te geven.

Desondanks moet ook worden geprobeerd de omvang en de mogelijke dreiging van dit systeem te evalueren. Hierbij merkt de regering op dat, indien zo'n systeem operationeel is, er moet worden van uitgegaan dat de gebruikte technieken niet alleen openstaan voor deze of gene overheden die ze gebruiken, maar eveneens dat ze kunnen worden gebruikt of misbruikt door om het even wie.

Bovendien moeten we ervan uitgaan dat er andere systemen of middelen bestaan die dezelfde mogelijkheden hebben als die aan Echelon worden toegeschreven. Misschien is Echelon geen uniek systeem. We zeggen dat hier met des te meer nadruk omdat uit rechtsvergelijkende studies blijkt dat ten minste 35 landen over een *communications intelligence system* beschikken dat nagenoeg gelijkaardige inspanningen aankan als Echelon.

Zoals het rapport verder benadrukt moet ook de capaciteit van zo'n interceptiesysteem worden gerelativeerd, niet alleen wegens de explosie van het aantal communicaties dat eruit voortvloeit, maar ook wegens de verschillende ontwikkelingen die het onderscheppen van communicatie ernstig bemoeilijken. Niet voor niets wordt er zo vaak gesproken over *firewalls* om systemen te beveiligen. Zo performant als men is in het ontwikkelen van een algemeen afluistersysteem, zo performant kan men ook zijn in het bedenken van veiligheidssleutels die dat moeten beletten.

*In deze ruimere context heeft de regering een aantal vragen die ook aan bod komen in de aanbevelingen van de commissie.*

*Een eerste vraag, waarnaar ook verwezen wordt in de eerste aanbeveling van de commissie, is of het raadzaam is politieke en/of juridische stappen te ondernemen tegen het Echelon-netwerk. Voorheen vond de regering het, rekening houdend met de omstandigheden, niet opportuun een klacht in te dienen bij het Europees Hof voor de Rechten van de Mens tegen de lidstaten die betrokken zijn bij het Echelonsysteem.*

*l'avenir.*

*Après cette introduction, je souhaiterais, au nom du gouvernement, féliciter les rapporteurs pour leur excellent rapport. Il s'agit d'un travail bien documenté qui envisage l'existence du réseau Echelon de plusieurs points de vue, ce qui permet de mieux en évaluer l'étendue et la dangerosité et de le placer dans une perspective plus large.*

*Le gouvernement se rallie sans équivoque à la thèse de l'existence du système d'interception Echelon. Autrement dit, le gouvernement partage l'opinion, défendue dans le rapport, selon laquelle il revient au Parlement de peser la véracité de certaines données, qui peuvent du reste avoir des conséquences importantes sur les relations avec les autres pays, afin de conférer une qualification juridique à ces faits et de leur donner des suites politiques.*

*Néanmoins, nous devons tenter d'évaluer l'étendue et la dangerosité de ce système. Le gouvernement fait remarquer que, si ce système est opérationnel, il faut être conscient de ce que les techniques utilisées ne sont pas seulement accessibles aux autorités officielles qui les emploient, mais qu'elles peuvent être utilisées, parfois à des fins illégales, par n'importe qui.*

*Par ailleurs, il existe d'autres systèmes qui offrent les mêmes possibilités que celles qui sont attribuées à Echelon. Echelon n'est peut-être pas un système unique. Nous insistons d'autant plus sur ce point que des études de droit comparé font apparaître qu'au moins 35 pays disposent d'un communications intelligence system semblable à Echelon.*

*Comme l'indique le rapport, il convient de relativiser la capacité de tels systèmes d'interception, non seulement en raison de l'explosion du nombre de communications qui en découle, mais aussi à cause des différents développements qui rendent beaucoup plus difficile l'interception de communications. Ce n'est pas pour rien que l'on parle tant des firewalls pour sécuriser les systèmes. On peut être aussi performant dans le développement de systèmes d'écoute générale que dans la conception de codes de sécurité qui doivent empêcher ces écoutes.*

Dans ce contexte plus large, le gouvernement se pose une série de questions. Elles sont également évoquées dans les recommandations de la commission. Je ne serai pas long à ce sujet car la longueur d'un débat n'est pas un gage de qualité. En se basant sur les recommandations, il est parfaitement possible de prendre position.

Tout d'abord, est-il opportun d'agir politiquement et/ou juridiquement, sous quelque forme que ce soit, face au réseau Echelon ? Cette question est abordée dans la première recommandation de la commission. Précédemment, le

*De regering zal wel meewerken aan eventuele politieke initiatieven op het Europese niveau, die ze zinvol acht. Ze onderstreept nogmaals dat het moet gaan om een gezamenlijk initiatief, dat moeilijk te realiseren is wegens de passieve houding van een aantal lidstaten. Realisme noopt ons ertoe te beseffen dat een gerechtelijke klacht wellicht wordt geseponeerd of niet tot het gewenste resultaat zal leiden. Op politiek vlak kan er evenwel meer bereikt worden.*

*Een gemeenschappelijk normatief juridisch initiatief lijkt evenmin veel slaagkansen te bieden. Ofschoon dit de beste oplossing zou zijn, is een Europese reglementering die economische spionage en afluisterpraktijken tussen de lidstaten verbiedt, alsnog uitgesloten. Er zijn momenteel wel een aantal gezamenlijke initiatieven van bijstand en uitwisseling van informatie, maar de werking van de inlichtingendiensten is nog steeds een nationale materie. Dat geldt a fortiori voor het al dan niet toegelaten van afluisterpraktijken. De regering zal haar positie bepalen naargelang van de voorgestelde initiatieven. We willen een harmonisatie op Europees niveau, maar aangezien het om een juridische materie gaat in de derde pijler, is er alleen vooruitgang mogelijk bij eenparigheid. We zijn ons ervan bewust dat dit grote problemen kan veroorzaken. Zodra er in de zogenaamde JBZ-Raad van de EU sprake is van informatica, wordt door steeds dezelfde landen obstructie gevoerd: Duitsland, Frankrijk en het Verenigd Koninkrijk staan dan meteen en heel radicaal op de rem.*

Een tweede vraag betreft het in kaart brengen van de dreiging die uitgaat van verschillende interceptiesystemen of -technieken. Dit is vooral een taak voor de inlichtingendiensten en de regering heeft daarvoor onlangs initiatieven genomen. Eind vorig jaar heeft de Ministerraad een wetsontwerp goedgekeurd om de goed afgebakende afluistermogelijkheden van de Algemene Dienst Inlichtingen en Veiligheid van de krijgsmacht aan te passen aan de nieuwe communicatievormen en -technologieën. De Raad van State gaf hierover een erg genuanceerd advies dat de werkgroep op het ogenblik verder onderzoekt. Het is onze bedoeling op dit terrein een stap vooruit te doen.

In verband met de Veiligheid van de Staat heeft de werkgroep een voorbereidende nota opgesteld over de bescherming van het wetenschappelijk en economisch potentieel van het land. Deze nota is intussen door het College voor inlichting en veiligheid goedgekeurd en zal onmiddellijk na het paasreces aan het ministerieel comité – dat wordt voorgezeten door de premier, maar waarin ook Justitie, Binnenlandse Zaken,

gouvernement avait déjà considéré, avec un certain réalisme, qu'il n'était pas opportun, dans la situation actuelle, de déposer une plainte auprès de la Cour européenne des droits de l'homme, contre les États membres qui seraient impliqués dans le système Echelon. Le gouvernement ne se tiendra pas à l'écart d'éventuelles initiatives politiques au niveau européen, initiatives qu'il juge sensées. Il souligne cependant une fois de plus qu'il devrait s'agir d'une initiative commune. Mais elle est difficile à réaliser compte tenu de l'attitude passive d'un certain nombre d'États membres. Nous les connaissons ; ils ont d'ailleurs été cités. Donc, dans une première approche juridique, nous sommes suffisamment réalistes pour savoir que l'introduction d'une action pourrait nous amener à un non-lieu ou à une réaction ne correspondant pas au but que nous voulons atteindre. Par contre, sur le plan politique, nous pouvons faire plus.

Une action normative juridique commune ne semble pas avoir plus de chances d'aboutir. En aucun cas, une réglementation européenne visant à interdire, entre les États membres, l'espionnage et les pratiques d'écoute à des fins économiques n'est envisageable à l'heure actuelle, bien qu'elle constituerait la meilleure solution. À ce jour, le fonctionnement des services de renseignements est encore une matière nationale, indépendante d'une série d'initiatives communes d'assistance et d'échange d'informations. Cela vaut a fortiori pour l'admissibilité des pratiques d'écoute qui, comme le souligne le rapport, constituent également une compétence nationale. Il va de soi que le gouvernement continuera à suivre cette affaire et qu'il déterminera sa position en fonction des initiatives proposées. Nous voudrions obtenir une harmonisation à l'échelle européenne. Mais il est difficile de progresser pour la simple raison qu'il s'agit d'une matière juridique, que nous nous trouvons dans le troisième pilier et que, dans ce pilier, il est exclu d'obtenir un résultat sauf en cas d'uniformité. Nous nous rendons compte que cela pourrait engendrer de gros problèmes. D'ailleurs, je veux souligner que, dès que les ministres de la Justice abordent, lors des fameux JAI de l'Union européenne, le sujet de l'informatique, ce sont les mêmes pays qui font obstruction : l'Allemagne, la France et le Royaume-Uni sont les premiers à enfoncer la pédale de frein. Ils le font de façon très visible et, croyez-moi, cela sent le caoutchouc !

*Une deuxième question concerne la description de la menace que font peser les différents systèmes et techniques d'interception. Cette mission incombe principalement aux services de renseignements. Le gouvernement a récemment pris des initiatives en ce sens. À la fin de l'année dernière, le Conseil des ministres a adopté un projet de loi visant à adapter les possibilités d'écoute du Service général de renseignement et de sécurité de l'armée aux nouvelles formes et technologies de communication. Le Conseil d'État a rendu un avis très nuancé que le groupe de travail est en train d'examiner. Nous avons l'intention d'avancer dans cette matière.*

*En ce qui concerne la Sûreté de l'État, le groupe de travail a rédigé une note préparatoire relative à la protection du potentiel scientifique et économique du pays. Cette note a été approuvée par le Collège du renseignement et de la sécurité et sera soumise immédiatement après les vacances de Pâques au comité ministériel présidé par le premier ministre mais où sont représentés les départements de la Justice, de l'Intérieur,*

Buitenlandse Zaken en Landsverdediging vertegenwoordigd zijn – worden voorgelegd. Deze nota zal de basis vormen voor concrete maatregelen op basis van de analyse van de verschillende bedreigingen tegen de belangrijkste sectoren. Voor de volledigheid van het debat voeg ik eraan toe dat de Veiligheid van de Staat twee dingen moet krijgen, zeker nu ze heeft moeten toegeven dat ze niet in staat is een afdoend antwoord te geven op de vraag of Echelon al dan niet bestaat en hoe ze de strijd ermee aanbindt. Voor mij blijft één ding duidelijk, maar ik spreek uit eigen naam. Ik heb de regering een voorstel gedaan dat de inlichtingendiensten de mogelijkheid moet geven om administratief over te gaan tot telefoontap. Dit voorstel vloeit voort uit mijn contacten met de andere inlichtingendiensten in Europa, die, zoals u weet, verenigd zijn in de fameuze *Groupe de Berne*. Deze groep is overigens ruimer dan de Europese Unie aangezien ook Noorwegen en Zwitserland er deel van uitmaken. Al deze landen vinden dat er een uniform systeem van afluisteren op administratieve gronden moet komen. De Veiligheid van de Staat heeft die mogelijkheid niet. De wetgever wenste ze in 1992 en 1998 niet in de wet op te nemen. Als we van de Veiligheid van de Staat in de Europese context een moderne dienst willen maken, moet daarin verandering komen. Een tweede probleem is natuurlijk dat van een goede bemanning van een dergelijke dienst. Zoals u weet is deze dienst onderworpen aan de lineaire maatregel van de aanwervingsstop die de regering op een bepaald ogenblik nam.

*(Voorzitter: de heer Armand De Decker.)*

Het college dat ik daarnet vernoemde, heeft tijdens een recente vergadering ook een grondige analyse laten uitvoeren over de wijze waarop de inlichtingendiensten de hun toevertrouwde opdrachten uitvoeren. Hier sluit ik aan bij de discussie van daarnet. Er moeten ongetwijfeld meer inspanningen worden geleverd om op basis van een degelijke kosten-batenanalyse en met het oog op goed afgelijnde doelstellingen, bepaalde aanpassingen te verwezenlijken.

Uiteraard zal de centrale dienst voor de informatiebeveiliging, waarover in de vijfde aanbeveling wordt gesproken, mee moeten worden opgenomen. Dat dit een moeilijke opgave wordt, hoeft geen betoog. Daarvoor is niet alleen een goede kosten-batenanalyse nodig, maar moet ook de vraag worden beantwoord wat we precies moeten beveiligen, hoever we daarin willen gaan en hoeveel geld we daarvoor veil hebben. Hierbij moet ook rekening worden gehouden met de zeer snel evoluerende technologieën en al wat daarmee te maken heeft.

Eenzelfde redenering kan worden gevolgd voor de elektronische bewakingspost en voor de wettelijke technieken inzake het opsporen, afluisteren en onderscheppen van berichten. Beide elementen hangen voor een stuk samen. De regering bespreekt op het ogenblik een wetsontwerp terzake. Zoals reeds tijdens de bespreking in de commissie voor de Justitie werd gezegd, moeten we de nodige waarborgen inbouwen – zodat we niet vervallen in de fouten die we anderen verwijten – en moeten we ook aandacht besteden aan de informatie-uitwisseling met andere diensten, zoals de gerechtelijke diensten. Hoewel de regering niet twijfelt aan het nut van zo'n preventie-instrument, wijst ze er toch op dat daar niet alle heil van mag worden verwacht.

*des Affaires étrangères et de la Défense. Cette note constituera la base des mesures concrètes fondées sur l'analyse des différentes menaces qui pèsent sur les principaux secteurs.*

*J'ajouterai que la Sûreté de l'État doit obtenir deux avancées, surtout depuis qu'elle a dû admettre qu'elle n'était pas à même de savoir si Echelon existait ou non et qu'elle ne savait pas comment lutter contre ce système. Je parle ici en mon nom propre. Premièrement, j'ai proposé au gouvernement de donner aux services de renseignements la possibilité de procéder à des écoutes téléphoniques administratives. Cette proposition découle de mes contacts avec les autres services secrets européens réunis au sein du fameux Groupe de Berne. Tous ces pays s'accordent à reconnaître la nécessité d'un système uniforme d'écoute administrative. En 1992 et 1998, le législateur a refusé d'accorder cette possibilité à la Sûreté de l'État. Si nous voulons faire de celle-ci un service moderne dans le contexte européen, cette situation doit changer. Deuxièmement, un tel service soit évidemment pouvoir compter sur des effectifs suffisants. Or, ce service est soumis à la mesure linéaire de blocage des recrutements prise en son temps par le gouvernement.*

*(M. Armand De Decker, président, prend place au fauteuil présidentiel.)*

*Le collège que je viens de citer a récemment fait analyser la manière dont les services de renseignements exécutent leurs missions. Des efforts doivent indubitablement être fournis en vue de procéder à des aménagements fondés sur une analyse coût-efficacité et visant à réaliser des objectifs bien définis.*

*Il va de soi que le service central de sécurisation de l'information dont il est question dans la cinquième recommandation devra également être concerné. Il est inutile de préciser que cela ne sera pas simple. Une bonne analyse coût-efficacité ne suffira pas, il faudra aussi préciser ce que nous voulons sécuriser, dans quelle mesure et de quels moyens financiers nous disposons pour ce faire. Nous devons également tenir compte de la rapidité d'évolution des technologies et de tout ce qui y est lié.*

*Le même raisonnement peut s'appliquer au poste de surveillance électronique et aux techniques légales de recherche, d'écoute et d'interception d'informations. Ces deux éléments sont en partie liés. Le gouvernement est en train de discuter un projet de loi relatif à cette matière. Nous devons prévoir les garanties nécessaires et être attentifs à l'échange d'informations avec les autres services, tels les services judiciaires. Bien que le gouvernement ne doute pas de la nécessité de cet instrument de prévention, il insiste sur le fait qu'il ne faut pas en attendre des miracles.*

*De bescherming van zowel burgers als ondernemingen is een prioriteit. De regering vindt dat de overheid moet nadenken over de manier waarop ze haar burgers en bedrijven kan beschermen tegen de afluisterpraktijken van sommige mogendheden of groepen die de markt willen verstoren.*

*Dat is een essentieel punt in de nota over de bescherming van het wetenschappelijk en economisch potentieel. In dit verband verwijs ik naar het protocol dat onlangs tussen het VBO en de Veiligheid van de Staat werd gesloten. Dat bewijst dat het voor bedrijven perfect mogelijk is de nodige inlichtingen door te geven aan de Staatsveiligheid, zodat deze zwakke plekken kan opsporen en kan reageren.*

*Een vierde probleem houdt verband met de Europese samenwerking. Ik verwijs naar de conclusies van de Raad JBZ na de gebeurtenissen van 11 september, meer bepaald op 20 september 2001. Er werd een besluit genomen over de oprichting van een Europese inlichtingendienst of over andere initiatieven voor de uitwisseling van informatie tussen de inlichtingendiensten, zoals in de aanbevelingen 7 en 8 wordt gevraagd.*

*Ik geeft toe dat het besluit tot een bijzonder geval beperkt blijft en dat het toepassingsgebied zou moeten worden uitgebreid. De discussie ligt echter moeilijk omdat in deze materie unanimiteit vereist is.*

*De ministers hebben gekozen voor een doorgedreven uitwisseling van informatie tussen de inlichtingendiensten, in afwachting van de eventuele oprichting van een Europese inlichtingendienst. Toch moeten nog vele juridische en institutionele obstakels worden opgeruimd. Zoals in het voorlopige STOA-verslag staat, behoort de wetgeving betreffende de inlichtingendiensten nog altijd tot de exclusieve bevoegdheid van de lidstaten. Dat is een reden te meer om ons bewust te worden van de complexiteit van de problematiek.*

De regering zal bij de evaluatie van de werking van de inlichtingendiensten uiteraard rekening houden met de aanbevelingen van de commissie. De gebeurtenissen van 11 september hebben de commissie – en ook andere diensten trouwens – voor een moeilijke periode geplaatst. Deze ervaring zal bij de evaluatie mede worden verwerkt. Verder dient een beveiligingsbeleid goed te worden omlijnd en voorzien van de nodige waarborgen.

De regering is zich ook bewust van de grenzen van de beveiligingsmogelijkheden en pleit voor een zeker realisme, zoals ik in het begin van mijn uiteenzetting reeds heb verduidelijkt. Er moet goed afgewogen worden welke de prioriteiten zijn in dit beleidsdomein en hoe de samenwerking tussen de verschillende betrokken diensten optimaal kan worden uitgebouwd.

De regering blijft ook voorstander van een Europese aanpak, ook al loopt daar lang niet alles even vlot als ze zou willen. België zal in ieder geval blijven ijveren om op de ingeslagen weg verder te gaan.

Het verslag maakt ook duidelijk dat de burgers en de bedrijven bewust moeten worden van de bedreigingen die

La question de la protection tant des citoyens que des entreprises est une question prioritaire. Le gouvernement estime que l'autorité doit également réfléchir à la manière dont elle peut protéger ses citoyens et ses entreprises des pratiques d'écoute de certaines puissances ou de certains groupes, qui peuvent aussi vouloir fausser les marchés.

C'est un point essentiel qui figure dans la note relative à la protection du potentiel scientifique et économique. À cet égard, je renvoie au protocole conclu très récemment entre la FEB et la Sûreté de l'État qui démontre qu'il est parfaitement possible aux entreprises de donner les informations nécessaires à la Sûreté de l'État pour détecter les points faibles et pour réagir.

Une quatrième problématique concerne la coopération européenne. Je renverrai aux conclusions du conseil JAI qui s'est tenu après les événements du 11 septembre, plus exactement le 20 septembre 2001. Une décision y a été prise quant à la création d'un service de renseignement européen ou à la mise en œuvre d'autres initiatives en matière d'informations entre services de renseignements tel que prévu dans les recommandations 7 et 8.

J'admets que la décision est limitée à un cas particulier et qu'il conviendrait d'élargir le champ couvert. Mais le débat est difficile car l'unanimité est requise en cette matière. Mais dès qu'un accord sera obtenu sur un point, nous pourrons continuer à avancer.

Les ministres ont en effet opté pour un échange d'informations très poussé entre les différents services de renseignements, anticipant la création éventuelle d'un service européen de renseignement. Néanmoins, il convient de signaler que de nombreux obstacles juridiques et institutionnels doivent encore être franchis. Je ne désespère pas. Comme le mentionne le rapport provisoire de la STOA, la législation concernant les services de renseignements appartient encore aujourd'hui à la sphère des compétences exclusives des États membres. Une raison de plus de se rendre compte de la difficulté de la question.

*Lors de l'évaluation du fonctionnement des services de renseignements, le gouvernement tiendra évidemment compte des recommandations de la commission, influencée par les événements du 11 septembre. La politique de sécurité doit être bien définie et pourvue des garanties nécessaires.*

*Conscient des limites des possibilités de sécurisation, le gouvernement plaide pour un certain réalisme. Il convient de bien définir les priorités et d'examiner la façon d'optimaliser la collaboration entre les différents services.*

*Le gouvernement reste partisan d'une approche européenne, même si celle-ci ne se déroule pas toujours aussi bien qu'il le voudrait.*

*Le rapport indique très clairement que les citoyens et les entreprises doivent être conscients des menaces liées aux nouveaux modes de communication.*

*Je remercie le Sénat de la manière dont il a mené et enrichi ce débat. Malheureusement, l'intérêt suscité par ce dossier n'est toujours pas proportionnel à son importance. C'est d'autant plus regrettable que les présentes recommandations sont fondamentales. Il me suffit de me référer au rapport de la commission du Sénat, dans lequel je peux lire que la*

gepaard gaan met de moderne communicatiemiddelen. De aanbevelingen van het verslag hieromtrent zijn niet mis te verstaan.

Ik dank de Senaat voor de wijze waarop hij dit debat heeft gevoerd en voor de verrijking die hij heeft toegevoegd. Jammer genoeg is de belangstelling voor dit dossier, net als in het verleden vaak, ook vandaag niet evenredig met het belang ervan. Dat is des te treuriger omdat de aanbevelingen die hier ter sprake komen, bijzonder diepgaand zijn. Ik hoef hiervoor maar te verwijzen naar het verslag van de Senaatscommissie zelf, waarin ik lees: "De problematiek in kwestie roept een aantal fundamentele vragen op: onafhankelijkheid, zelfbeschikkingsrecht en veiligheid van de soevereine staten, respect voor het privé-leven van de burger, internationale gewaarborgde vrije handel en ten slotte de bescherming van het wetenschappelijk en industrieel patrimonium van een land." Voor mij mocht daar ook bij staan: internationaal gewaarborgde rechten van de individuen. Alleen als we deze uitgangspunten vasthouden en als we daarvoor ook internationale goodwill kunnen creëren, kunnen we problemen als dat van Echelon het hoofd bieden. *(Applaus)*

– **De bespreking is gesloten.**

– **De stemming over de besluiten en de aanbevelingen van de begeleidingscommissies heeft later plaats.**

*problématique en question « soulève des questions fondamentales sur l'indépendance, le droit à l'autodétermination et la sécurité des États souverains, les 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. »*

*En ce qui me concerne, on peut y ajouter : les droits des individus, garantis sur le plan international. C'est seulement en nous en tenant à ces conclusions et en suscitant la volonté au niveau international que nous pourrons résoudre des problèmes comme celui d'Echelon. (Applaudissements)*

– **La discussion est close.**

– **Il sera procédé ultérieurement au vote sur les conclusions et les recommandations des commissions de suivi.**

## Wetsontwerp ertoe strekkende het Belgische recht in overeenstemming te brengen met het Verdrag tegen foltering en andere wrede, onmenselijke of onterende behandeling of bestraffing, aangenomen te New York op 10 december 1984 (Stuk 2-1020) (Evocatieprocedure)

### *Algemene bespreking*

**De voorzitter**. – De heer Vandenberghe verwijst naar zijn schriftelijk verslag.

– **De algemene bespreking is gesloten.**

### *Artikelsgewijze bespreking*

*(Voor de tekst aangenomen door de commissie voor de Justitie, zie stuk 2-1020/4.)*

**De voorzitter**. – Artikel 5 luidt:

In Boek II, Titel VIII, Hoofdstuk I, van hetzelfde Wetboek wordt een Afdeling V ingevoegd die bestaat uit de artikelen 417*bis* tot 417*quinquies*, luidende:

"Afdeling V – Foltering, onmenselijke behandeling en onterende behandeling.

Art. 417*bis*. – Voor de toepassing van deze afdeling wordt verstaan onder:

1º foltering: elke opzettelijke onmenselijke behandeling die […] hevige pijn of ernstig en vreselijk lichamelijk of geestelijk lijden veroorzaakt;

2º onmenselijke behandeling: elke behandeling waardoor een persoon opzettelijk ernstig geestelijk of lichamelijk leed

## Projet de loi de mise en conformité du droit belge avec la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, adoptée à New York le 10 décembre 1984 (Doc. 2-1020) (Procédure d'évocation)

### *Discussion générale*

**M. le président**. – M. Vandenberghe se réfère à son rapport écrit.

– **La discussion générale est close.**

### *Discussion des articles*

*(Pour le texte adopté par la commission de la Justice, voir document 2-1020/4.)*

**M. le président**. – L'article 5 est ainsi libellé :

Il est inséré dans le Livre II, Titre VIII, Chapitre I$^{er}$, du même Code, une Section V comprenant les articles 417*bis* à 417*quinquies*, rédigée comme suit :

« Section V – De la torture, du traitement inhumain et du traitement dégradant.

Art. 417*bis*. – Pour l'application de la présente section, l'on entend par :

1º torture : tout traitement inhumain délibéré qui provoque une douleur […] aiguë ou de très graves et cruelles souffrances, physiques ou mentales ;

2º traitement inhumain : tout traitement par lequel de graves souffrances mentales ou physiques sont intentionnellement

wordt toegebracht, onder meer om van hem inlichtingen te verkrijgen of bekentenissen af te dwingen of om hem te straffen, of om druk op hem of op derden uit te oefenen, of hem of derden te intimideren;

3º onterende behandeling: elke handeling die in de ogen van het slachtoffer of van derden een ernstige krenking of aantasting van de menselijke waardigheid uitmaakt.

Art. 417*ter*. – Hij die een persoon aan foltering onderwerpt, wordt gestraft met opsluiting van tien jaar tot vijftien jaar.

Het misdrijf bedoeld in het eerste lid wordt gestraft met opsluiting van vijftien jaar tot twintig jaar als het is gepleegd:

1º door een openbaar officier of ambtenaar, drager of agent van de openbare macht die handelt naar aanleiding van de uitoefening van zijn bediening;

2º op een persoon die ten gevolge van zwangerschap, een ziekte, dan wel een lichamelijk of een geestelijk gebrek of onvolwaardigheid of wegens een precaire toestand bijzonder kwetsbaar is;

3º op een minderjarige […]; of

4º wanneer de handeling een ongeneeslijk lijkende ziekte, hetzij een blijvende fysieke of psychische ongeschiktheid, hetzij het volledig verlies van een orgaan of van het gebruik van een orgaan, hetzij een zware verminking heeft veroorzaakt.

Het misdrijf bedoeld in het eerste lid wordt gestraft met opsluiting van twintig jaar tot dertig jaar als:

1º het is gepleegd op een minderjarige of op een persoon die uit hoofde van zijn lichaams- of geestestoestand niet bij machte is om in zijn onderhoud te voorzien, door de vader, de moeder of door andere bloedverwanten in de opgaande lijn, door enig andere persoon die gezag over hem heeft of die hem onder zijn bewaring heeft, of door iedere meerderjarige persoon die occasioneel of gewoonlijk met het slachtoffer samenleeft; of

2º de dood heeft veroorzaakt, en gepleegd is zonder het oogmerk om te doden.

Het bevel van een meerdere of van een gezag kan het misdrijf bedoeld in het eerste lid niet verantwoorden.

Art. 417*quater*. – Hij die een persoon aan een onmenselijke behandeling onderwerpt, wordt gestraft met opsluiting van vijf jaar tot tien jaar.

Het misdrijf bedoeld in het eerste lid wordt gestraft met opsluiting van tien jaar tot vijftien jaar als het is gepleegd:

1º door een openbaar officier of ambtenaar, drager of agent van de openbare macht die handelt naar aanleiding van de uitoefening van zijn bediening;

2º op een persoon die ten gevolge van zwangerschap, een ziekte, dan wel een lichamelijk of een geestelijk gebrek of onvolwaardigheid of wegens een precaire toestand bijzonder kwetsbaar is;

3º op een minderjarige […]; of

4º wanneer de handeling een ongeneeslijk lijkende ziekte, hetzij een blijvende fysieke of psychische ongeschiktheid,

infligées à une personne, notamment dans le but d'obtenir d'elle des renseignements ou des aveux, de la punir, de faire pression sur elle ou d'intimider cette personne ou des tiers ;

3º traitement dégradant : tout acte qui cause à celui qui y est soumis, aux yeux d'autrui ou aux siens, une humiliation ou un avilissement graves.

Art. 417*ter*. – Quiconque soumettra une personne à la torture sera puni de la réclusion de dix ans à quinze ans.

L'infraction visée à l'alinéa premier sera punie de la réclusion de quinze ans à vingt ans lorsqu'elle aura été commise :

1º par un officier ou un fonctionnaire public, un dépositaire ou un agent de la force publique agissant à l'occasion de l'exercice de ses fonctions ;

2º envers une personne particulièrement vulnérable en raison d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale ou en raison d'une situation précaire ;

3º envers un mineur […] ; ou

4º lorsque l'acte a causé une maladie paraissant incurable, une incapacité permanente physique ou psychique, la perte complète d'un organe ou de l'usage […] d'un organe, ou une mutilation grave.

L'infraction visée à l'alinéa premier sera punie de vingt ans à trente ans de réclusion lorsque :

1º elle aura été commise envers un mineur ou envers une personne qui, en raison de son état physique ou mental, n'était pas à même de pourvoir à son entretien, par ses père, mère ou autres ascendants, toute autre personne ayant autorité sur lui ou en ayant la garde, ou toute personne majeure qui cohabite occasionnellement ou habituellement avec la victime ; ou

2º elle aura causé la mort et aura été commise sans intention de la donner.

L'ordre d'un supérieur ou d'une autorité ne peut justifier l'infraction prévue à l'alinéa premier.

Art. 417*quater*. – Quiconque soumettra une personne à un traitement inhumain sera puni de réclusion de cinq ans à dix ans.

L'infraction visée à l'alinéa premier sera punie de dix ans à quinze ans de réclusion lorsqu'elle aura été commise :

1º par un officier ou un fonctionnaire public, un dépositaire ou un agent de la force publique agissant à l'occasion de l'exercice de ses fonctions ;

2º envers une personne particulièrement vulnérable en raison d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale ou en raison d'une situation précaire ;

3º envers un mineur […] ; ou

4º lorsque l'acte a causé une maladie paraissant incurable, une incapacité permanente physique ou psychique, la perte

hetzij het volledig verlies van een orgaan of van het gebruik van een orgaan, hetzij een zware verminking heeft veroorzaakt.

Het misdrijf bedoeld in het eerste lid wordt gestraft met opsluiting van vijftien jaar tot twintig jaar als:

1º het is gepleegd op een minderjarige of op een persoon die uit hoofde van zijn lichaams- of geestestoestand niet bij machte is om in zijn onderhoud te voorzien, door de vader, de moeder of door andere bloedverwanten in de opgaande lijn, door enig andere persoon die gezag over hem heeft of die hem onder zijn bewaring heeft, of door iedere meerderjarige persoon die occasioneel of gewoonlijk met het slachtoffer samenleeft; of

2º de dood heeft veroorzaakt en gepleegd is zonder het oogmerk te doden.

Het bevel van een meerdere of van een gezag kunnen het misdrijf bedoeld in het eerste lid niet verantwoorden.

Art. 417*quinquies*. – Hij die een persoon aan een onterende behandeling onderwerpt, wordt gestraft met gevangenisstraf van vijftien dagen tot twee jaar en met geldboete van 50 EUR tot 300 EUR of met een van die straffen alleen".

Op dit artikel heeft de heer Vandenberghe c.s. amendement 5 ingediend (zie stuk 2-1020/2) dat luidt:

In het voorgestelde artikel 417*ter*, laatste lid, het woord "verantwoorden" vervangen door het woord "*rechtvaardigen*".

– **De stemming over het amendement wordt aangehouden.**

– **De aangehouden stemming en de stemming over het wetsontwerp in zijn geheel hebben later plaats.**

**De voorzitter**. – De agenda van deze vergadering is afgewerkt.

De volgende vergaderingen vinden plaats donderdag 21 maart 2002 om 10 uur en om 15 uur.

*(De vergadering wordt gesloten om 17.05 uur.)*

## Berichten van verhindering

Afwezig met bericht van verhindering: de heer Colla, met opdracht in het buitenland en de heren Geens en Vandenbroeke, wegens andere plichten.

– **Voor kennisgeving aangenomen.**

complète d'un organe ou de l'usage […] d'un organe, ou une mutilation grave.

L'infraction visée à l'alinéa premier sera punie de quinze ans à vingt ans de réclusion lorsque :

1º elle aura été commise envers un mineur ou envers une personne qui, en raison de son état physique ou mental, n'était pas à même de pourvoir à son entretien, par ses père, mère ou autres ascendants, toute autre personne ayant autorité sur lui ou en ayant la garde, ou toute personne majeure qui cohabite occasionnellement ou habituellement avec la victime ; ou

2º elle aura causé la mort et aura été commise sans intention de la donner.

L'ordre d'un supérieur ou d'une autorité ne peut justifier l'infraction prévue à l'alinéa premier.

Art. 417*quinquies*. – Quiconque soumettra une personne à un traitement dégradant sera puni d'un emprisonnement de quinze jours à deux ans et d'une amende de 50 EUR à 300 EUR ou d'une de ces peines seulement. »

À cet article, M. Vandenberghe et consorts proposent l'amendement nº 5 (voir document 2-1020/2) ainsi libellé :

Dans le texte néerlandais de l'article 417*ter*, dernier alinéa, proposé, remplacer le mot « verantwoorden » par le mot « *rechtvaardigen* ».

– **Le vote sur l'amendement est réservé.**

– **Il sera procédé ultérieurement au vote réservé ainsi qu'au vote sur l'ensemble du projet de loi.**

**M. le président**. – L'ordre du jour de la présente séance est ainsi épuisé.

Les prochaines séances auront lieu le jeudi 21 mars 2002 à 10 h et à 15 h.

*(La séance est levée à 17 h 05.)*

## Excusés

M. Colla, en mission à l'étranger, ainsi que MM. Geens et Vandenbroeke, pour d'autres devoirs, demandent d'excuser leur absence à la présente séance.

– **Pris pour information.**