2-531/1 (Sénat)
DOC 50 **0813/001 (Chambre)**

Sénat et Chambre des représentants de Belgique

SESSION DE 1999-2000

19 JUILLET 2000

Rapport d'activités 1999 complémentaire du Comité permanent de contrôle des services de renseignements et de sécurité

RAPPORT

FAIT AU NOM DE LA COMMISSION CHARGÉE DU SUIVI DU COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ (Sénat)
ET
DE LA COMMISSION SPÉCIALE CHARGÉE DE L'ACCOMPAGNEMENT PARLEMENTAIRE DU COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE POLICE (Chambre)

PAR M. **HORDIES** (S) ET MME **PELZER-SALANDRA** (Ch)

Ont participé aux travaux de la commission :

Sénat :

Membres : MM. De Decker, président, Dedecker, Mme Lizin, MM. Vandenberghe et Hordies, rapporteur.

Chambre :

Membres : MM. De Croo, président, Coveliers, de Donnéa, De Man, Larcier, Van Den Hove, Van Parijs et Mme Pelzer-Salandra, rapporteuse.

Membres sans droit de vote : MM. Detremmerie et Van Hoorebeke.

2-531/1 (Senaat)
DOC 50 **0813/001 (Kamer)**

Belgische Senaat en Kamer van volksvertegenwoordigers

ZITTING 1999-2000

19 JULI 2000

Aanvullend activiteitenverslag 1999 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

VERSLAG

NAMENS DE COMMISSIE BELAST MET DE BEGELEIDING VAN HET VAST COMITÉ VAN TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN (Senaat)
EN
DE BIJZONDERE COMMISSIE BELAST MET DE PARLEMENTAIRE BEGELEIDING VAN HET VAST COMITÉ VAN TOEZICHT OP DE POLITIEDIENSTEN (Kamer)

UITGEBRACHT DOOR DE HEER **HORDIES** (S) EN MEVROUW **PELZER-SALANDRA** (K)

Aan de werkzaamheden van de commissie hebben deelgenomen :

Senaat :

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

Kamer :

Leden : de heren De Croo, voorzitter, Coveliers, de Donnéa, De Man, Larcier, Van Den Hove, Van Parijs en mevrouw Pelzer-Salandra, rapporteur.

Leden zonder stemrecht : de heren Detremmerie en Van Hoorebeke.

SOMMAIRE

INHOUD

1. EXPOSÉ INTRODUCTIF DU PRÉSIDENT DU COMITÉ R

Le président du Comité R rappelle que le rapport précédent était un rapport de transition.

La relation entre l'autorité de contrôle et les services de renseignement évolue dans le bon sens. Cette situation a permis au Comité R d'améliorer le contrôle et d'avancer dans ses enquêtes.

Le présent rapport est le témoignage de cette nouvelle voie. Sans doute faudra-t-il, dans l'avenir, à travers des cas concrets, essayer de développer une approche plus synthétique et plus globale des problèmes.

Outre les enquêtes qui ont été terminées le dernier trimestre de l'année 1999, le rapport reprend deux enquêtes qui ont été terminées au début de cette année-ci. Pour des raisons différentes, le Comité R a estimé que ces rapports d'enquête devraient être repris dans le présent rapport.

Il s'agit du rapport complémentaire sur la manière dont les services belges de renseignements réagissent face à l'éventualité d'un réseau « Échelon » d'interception de communications, d'une part, et une enquête de contrôle sur les dysfonctionnements éventuels d'un service de la Sûreté de l'État, d'autre part.

Le rapport « Échelon » est l'exemple même d'une enquête qui démontre la complexité de la tâche du Comité R et les dangers auxquels on peut être soumis par l'aspect émotionnel de ce dossier.

À la demande des commissions parlementaires, le Comité R a déjà transmis un premier suivi de ce rapport, qui contient une actualisation des éléments du dossier. En tout cas, le débat sur « Échelon » est loin d'être clos. Pour cette raison, le Comité R continuera à actualiser ce dossier.

Le président croit pouvoir dire qu'en ce qui concerne « Échelon », nous avons dépassé le stade où l'on pouvait simplement s'interroger sur le fait même de l'existence éventuelle d'un tel réseau, étant donné notamment les déclarations de James Woolsey, ancien directeur de la CIA, qui a reconnu la réalité de l'espionnage économique, sans toutefois mentionner la dénomination « Échelon ».

D'autres éléments semblent également confirmer l'existence d'un système global d'interception. C'est ainsi que le commissaire canadien, chargé du contrôle du « Centre de la sécurité des télécommunications (CST) », organisme du ministère de la Défense nationale, dont la mission est de fournir au gouvernement canadien des renseignements électromagnétiques (SIGINT) sur des pays étrangers, donne, dans son dernier rapport 1999-2000 (toujours sans mentionner le terme « Échelon »), des indications qui vont dans le sens de la confirmation de l'existence actuelle d'un

1. INLEIDENDE UITEENZETTING DOOR DE VOORZITTER VAN HET COMITE I

De voorzitter van het Comité I herinnert eraan dat het vorige verslag eigenlijk een overgangsverslag was.

De betrekkingen tussen de controle-instantie en de inlichtingendiensten ontwikkelen zich in gunstige zin. Daardoor kan het Comité I de controle verbeteren en vooruitgang boeken in zijn onderzoeken.

Dit verslag licht deze nieuwe aanpak toe. Wellicht moet in de toekomst via concrete gevallen worden gestreefd naar een meer synthetische en algemene benadering van de problemen.

Behalve de onderzoeken die tijdens het laatste kwartaal van 1999 zijn afgerond, maakt het verslag ook melding van twee onderzoeken die in het begin van dit jaar zijn beëindigd. Om verschillende redenen vond het Comité I dat deze onderzoeksverslagen in dit verslag moesten worden opgenomen.

Het gaat om het aanvullend verslag over de manier waarop de Belgische inlichtingendiensten reageren op het eventuele bestaan van een Echelon-netwerk voor het onderscheppen van communicatie, enerzijds, en een toezichtsonderzoek over de eventuele disfuncties bij een sectie van de Veiligheid van de Staat, anderzijds.

Het Echelon-verslag toont aan hoe complex de taak van het Comité I wel is en welke gevaren kunnen schuilen in de emotionele aspecten van dit dossier.

Op verzoek van de parlementaire commissies heeft het Comité I reeds een eerste aanvulling van dit verslag doorgezonden waarin de elementen van het dossier worden geactualiseerd. Het debat over Echelon is hoe dan ook ver van afgesloten en het Comité I zal dit dossier dus blijven volgen.

De voorzitter vindt dat het stadium waarin het bestaan van Echelon nog in twijfel werd getrokken, voorbij is gezien de verklaringen van James Woolsey, oud-directeur van de CIA, die — weliswaar zonder Echelon uitdrukkelijk te noemen — heeft erkend dat economische spionage werkelijk plaatsvindt.

Ook andere elementen lijken te wijzen op het bestaan van een algemeen interceptiesysteem. De Canadese commissaris belast met de controle op het *Communications Security Establishment* (CSE) — een orgaan van het ministerie van Landsverdediging dat de Canadese regering elektromagnetische inlichtingen (SIGINT) over andere landen verstrekt — geeft in zijn laatste verslag over 1999-2000 aanwijzingen die het bestaan van een algemeen interceptiesysteem lijken te bevestigen (opnieuw zonder Echelon uitdrukkelijk te vermelden). Bij wijze van voorbeeld:

système global d'interception. À titre d'exemple, notons ce passage : « des communications canadiennes peuvent se retrouver dans les fonds de renseignements du CST, car il est techniquement impossible, à l'heure actuelle, de les exclure totalement; .... le CST possède des politiques et des pratiques destinées à assurer la protection et le traitement approprié des communications canadiennes recueillies involontairement ».

Ceci étant, il convient de rappeler que l'enquête du Comité R portait en premier lieu sur la question de savoir quelle était la réaction de nos services de renseignement face à l'éventualité de l'existence d'un tel système d'interceptions des communications. Dans son rapport, le Comité R a déjà fait mention de la réaction des services. Il faut signaler, qu'actuellement, le Comité R s'informe de la manière concrète dont les sources ouvertes concernant « Échelon » ont été analysées et exploitées.

Il ne faut toutefois pas perdre de vue le risque de déboucher dans cette affaire sur une polémique qui pourrait engendrer des effets négatifs. Il faut bien admettre en effet que le problème des interceptions de sécurité, qu'elles soient globales ou ciblées, est souvent évoqué d'une manière émotionnelle et que cette approche légitime et compréhensible, à prendre certes en considération, pourrait également entraîner une peur irraisonnée provoquant à son tour le rejet en bloc de toutes les techniques d'interception et par conséquent le refus d'accorder l'utilisation de celles-ci à nos propres services.

En examinant « Échelon », on se focalise surtout sur les possibilités d'espionnage économique en perdant parfois de vue les autres cibles visées par un tel système et en l'occurrence la lutte contre la criminalité organisée et le terrorisme.

Pour ne pas se limiter aux pays anglo-saxons mis en cause dans la problématique d'« Échelon », on peut souligner qu'en consultant le dernier rapport de l'organisme de contrôle du service d'interceptions français (la Commission nationale de contrôle des interceptions de sécurité, en abrégé CNCIS), on constate qu'en ce qui concerne l'application de la loi française sur les écoutes administratives, les chiffres cités pour l'année 1999 démontrent que les écoutes autorisées (ciblées par définition) en vue de protéger le potentiel économique, ne représentent que 4% du total des écoutes autorisées. Les principales cibles concernées par cette méthode de collecte de renseignements sont avant tout la criminalité organisée, le terrorisme et la sécurité de l'État.

On retrouve la même hiérarchie quant aux sources de préoccupation des services de renseignements anglais lorsque l'on consulte le rapport annuel de l'*« Intelligence and Security Committee »* britannique de 1999.

« het kan gebeuren dat Canadese communicatie terechtkomt in de voorraad inlichtingen van de CSE, want het is technisch nog niet mogelijk om dat helemaal uit te sluiten; ... De CSE is in staat om de bescherming en de behoorlijke behandeling te verzekeren van de onopzettelijk onderschepte Canadese communicatie ».

Het onderzoek van het Comité I ging echter in de eerste plaats over de vraag hoe onze inlichtingendiensten reageren op het mogelijke bestaan van zo'n interceptiesysteem. Het Comité I heeft die reacties reeds beschreven in zijn verslag. Momenteel onderzoekt het Comité I hoe de open bronnen betreffende Échelon concreet zijn geanalyseerd en gebruikt.

Toch mag men niet uit het oog verliezen dat deze zaak een polemiek kan veroorzaken met mogelijk negatieve gevolgen. Het probleem van de algemene of doelgerichte veiligheidsintercepties roept vaak veel emoties op die legitiem en begrijpelijk zijn, maar kunnen uitmonden in een onredelijke angst waarbij alle interceptietechnieken over een kam worden geschoren, wat het gebruik ervan door onze diensten onmogelijk maakt.

Het onderzoek naar Echelon spitst zich vooral toe op de mogelijkheid van economische spionage, waarbij soms uit het oog wordt verloren dat zo'n systeem ook kan worden ingezet in de strijd tegen de georganiseerde criminaliteit en het terrorisme.

Niet alleen de Angelsaksische landen zijn betrokken bij de Echelon-problematiek. Uit het laatste rapport van het Franse *Commission nationale de contrôle des interceptions de sécurité (CNCIS)*, blijkt dat wat de toepassing van de Franse wet op administratieve afluisterpraktijken betreft, de cijfers voor 1999 aantonen dat de toegestane afluisterpraktijken (die per definitie een doelwit hebben) teneinde het economisch potentieel te beschermen, slechts 4% van het totaal van de toegestane afluisterpraktijken uitmaken. Deze vorm van gegevensinzameling heeft als voornaamste doelwit de georganiseerde criminaliteit, het terrorisme en de staatsveiligheid.

Wanneer men het jaarverslag van het Britse *Intelligence and Security Committee* van 1999 raadpleegt, stelt men vast dat de Engelse inlichtingendiensten zich bij voorrang met diezelfde doelwitten bezighouden.

Sans toutefois les minimiser à outrance, cette constatation est sans doute de nature à nuancer quelque peu l'aspect émotionnel que suscite les dangers d'un système du type « Échelon ».

Mais au delà de cet aspect, il faut se demander, en ce qui concerne notamment la lutte contre la criminalité et la sécurisation de nos communications, s'il ne faut pas accorder également à nos services la possibilité légale de pratiquer des interceptions de sécurité dans un cadre limité, subsidiaire et contrôlé de manière démocratique (*cf.* les rapports précédents du Comité R).

Selon le Comité R, il s'agit d'un moyen qui tôt ou tard devra être autorisé, sous peine de mettre nos services en difficulté dans le cadre de l'accomplissement des nouvelles missions qui leur ont été conférées par la loi organique des services de renseignement.

Un autre aspect qui est évoqué par le présent rapport est une certaine banalisation des techniques d'interceptions des communications.

Lorsqu'on se rend au Salon international de la sécurité intérieure des États (MILIPOL) on peut constater que toute la technologie de pointe dans ce domaine y est exposée et offerte en vente à un public, certes sélectionné, mais cosmopolite et très nombreux.

Dans le même ordre d'idées et notamment en ce qui concerne la sécurisation des communications, il faut être conscient que la criminalité organisée dispose de moyens financiers illimités qui lui permettent de se procurer du matériel performant répondant aux dernières évolutions de la technique, permettant entre autres le cryptage des communications. Pour nos services de renseignement, davantage limités dans leurs moyens, une telle constatation doit être fort décourageante.

Ensuite, le président du Comité R évoque le problème de la prolifération des services de renseignements privés.

Il se demande si nos services de renseignement sont sensibles à ce problème. Le Comité R voudrait en savoir plus, éventuellement rassembler des chiffres et essayer de mieux cerner, voire d'identifier ces « officines » qui font du renseignement chez nous.

Le Comité R a déjà essayé d'aborder ce problème par le biais des habilitations de sécurité qui seraient, le cas échéant, accordées au personnel de ces entreprises mais apparemment il n'en est tenu aucune comptabilité et il est donc très difficile de recueillir des informations par cette voie sur ces entreprises.

Zonder de gevaren van een systeem van het Echelon-type te willen minimaliseren draagt die vaststelling ongetwijfeld bij tot een nuancering van de emoties die dergelijke mogelijke gevaren hebben uitgelokt.

Los hiervan moet men zich wel afvragen of, onder meer met het oog op de strijd tegen de criminaliteit en het beveiligen van onze communicatie, onze diensten niet wettelijk gemachtigd moeten worden om binnen bepaalde grenzen, op aanvullende wijze en onder democratische controle (zie de vorige verslagen van het Comité I), uit veiligheidsoverwegingen boodschappen te onderscheppen.

Volgens het Comité I gaat het om een middel dat vroeg of laat moet worden toegestaan, wil men onze diensten niet in moeilijkheden brengen bij het vervullen van de nieuwe opdrachten die hun door de wet op de inlichtingendiensten zijn toegekend.

Een ander aspect dat in dit verslag aan bod komt is een vorm van popularisering van de interceptietechnieken.

Op de Internationale Beurs voor de Binnenlandse Veiligheid van Staten (MILIPOL) stelt men vast dat de volledige speerpunttechnologie op dit gebied daar wordt tentoongesteld en te koop aangeboden aan een weliswaar geselecteerd maar kosmopolitisch en zeer breed publiek.

In verband hiermee en met name in verband met de beveiliging van de communicatie moet men er zich bewust van zijn dat de georganiseerde criminaliteit over onbeperkte middelen beschikt die haar in staat stellen zich geavanceerd materiaal aan te schaffen dat de laatste ontwikkelingen van de techniek volgt en dat onder meer de mogelijkheid biedt de communicatie te versleutelen. Voor onze inlichtingendiensten, die beperktere middelen hebben, moet het ontmoedigend zijn dat vast te stellen.

Vervolgens vermeldt de voorzitter van Comité I het probleem van de wildgroei van particuliere inlichtingendiensten.

Hij vraagt zich af of onze inlichtingendiensten zich van dat probleem bewust zijn. Het Comité I wil er ook meer over vernemen, eventueel cijfers verzamelen en dan trachten die « kantoren » die bij ons met inlichtingen bezig zijn, beter in te schatten, eventueel zelfs hun identiteit vast te stellen.

Het Comité I heeft reeds een poging ondernomen om dat probleem aan te pakken door middel van de veiligheidsmachtigingen die in voorkomend geval aan het personeel van die ondernemingen afgegeven zouden worden maar schijnbaar wordt daarvan geen enkele administratie bijgehouden en is het dus zeer moeilijk op die wijze inlichtingen in te winnen over die ondernemingen.

Il est clair que dans ce domaine tout un travail reste à faire. Ce débat est inévitable et est vital pour nos services de renseignements parce qu'il s'agit de la protection des droits de nos citoyens.

Dans le même cadre, M. Delepière se réfère à l'avis que le Comité R a rendu sur la recommandation 1049 du 26 avril du Conseil de l'Europe concernant le contrôle des services de sécurité intérieure dans les États membres du Conseil de l'Europe.

Cette recommandation semble empreinte de bonnes intentions mais fait l'amalgame entre sécurité, renseignements, police et justice. Cette recommandation ne tient pas compte des pays du Conseil de l'Europe qui ont une tradition démocratique et qui ont des législations et des contrôles en la matière.

Le président du Comité R conclut que le Comité R devra, au travers de cas concrets, réaliser des études plus générales dans ces domaines.

Une telle approche n'est cependant pas possible sans une bonne relation avec les services de renseignements.

À ce propos, le Comité R a reçu des signes très positifs : aussi bien la Sûreté de l'État que le SGR ont accepté d'avoir des réunions trimestrielles avec le Comité R, dans le but d'être informés sur leurs activités.

Le président du Comité R signale encore que l'enquête sur un service de la Sûreté de l'État (p. 52 du rapport annuel) a été suivie d'effets, des mesures ont été prises et de nouvelles directives ont été formulées.

En tout cas, le rapport du Comité R n'a pas été contesté et l'utilité du rapport a été reconnue.

Le rapport concernant un ancien informateur (p. 72 du rapport) souligne la nécessité d'une relation entre le Comité R et les autorités judiciaires. Il est nécessaire que cette relation soit mieux élaborée dans le futur.

Le président rappelle que le Comité R n'est compétent que pour exercer un contrôle des deux services de renseignements belges visés par la loi du 18 juillet 1991 organique du contrôle des services de renseignements. *Quid* alors de la protection des droits du citoyen face à des services de renseignements privés ? Ceux-ci échappent au contrôle mis en place.

À propos du renseignement militaire, le Comité R rappelle qu'il y a d'autres services au sein de l'armée qui font du renseignement. Sur ce plan aussi, la logique de la loi organique du contrôle limite celui-ci au SGR. Le Comité R se pose la question de savoir comment il peut éventuellement surmonter ses limites de compétence.

Het is duidelijk dat er op dat vlak nog heel wat werk te verrichten is. Dat debat mag men niet uit de weg gaan en is van vitaal belang voor onze inlichtingendiensten want het gaat om de bescherming van de rechten van onze burgers.

In hetzelfde kader verwijst de heer Delepière naar het advies dat het Comité I uitgebracht heeft over aanbeveling 1409 van 26 april van de Raad van Europa betreffende het toezicht op de binnenlandse veiligheidsdiensten in de lidstaten van de Raad van Europa.

Deze aanbeveling is blijkbaar doortrokken van goede bedoelingen maar verwart veiligheid, inlichtingen, politie en justitie met elkaar. Deze aanbeveling houdt geen rekening met de landen van de Raad van Europa die een democratische traditie hebben en die ter zake over wetten en controles beschikken.

De voorzitter van het Comité I besluit dat het Comité door middel van concrete gevallen meer algemene studies zal moeten verrichten in die domeinen.

Een dergelijke benadering is echter niet mogelijk zonder een goede relatie met de inlichtingendiensten.

In dat verband heeft het Comité I positieve signalen ontvangen : zowel de Veiligheid van de Staat als de ADIV hebben aanvaard om elk kwartaal te vergaderen met het Comité I om elkaar op de hoogte te brengen van hun activiteiten.

De voorzitter van het Comité I meldt ook nog dat het onderzoek aangaande een sectie van de Veiligheid van de Staat (blz. 52 van het jaarverslag) de nodige resultaten heeft gehad : maatregelen zijn genomen en nieuwe richtlijnen zijn opgesteld.

In elk geval wordt het verslag van het Comité I niet betwist en het nut ervan erkend.

Het verslag over een gewezen informant (blz. 75 van het jaarverslag) toont aan dat de relatie tussen het Comité I en de gerechtelijke instanties verbeterd moet worden.

De voorzitter herinnert eraan dat het Comité I enkel bevoegd is voor de controle op de twee Belgische inlichtingendiensten waarvan sprake is in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten. Hoe zit het dan met de bescherming van de rechten van de burger ten aanzien van de privé-inlichtingendiensten ? Die ontsnappen aan de ingevoerde controle.

Het Comité I herinnert eraan dat in het leger ook inlichtingendiensten bestaan. Ook op dat vlak is de controle krachtens de wet tot regeling van het toezicht beperkt tot de ADIV. Het Comité I vraagt zich af hoe het eventueel deze bevoegdheidsbeperkingen kan overschrijden.

Le président du Comité R informe les commissions de suivi que le Comité R a été invité par la Fédération des entreprises de Belgique (FEB) pour éventuellement assister à des rencontres avec les services de renseignement concernant la protection des communications des entreprises. La FEB est très préoccupée par le danger que constituent pour notre potentiel scientifique, économique et industriel, les systèmes d'interception des communications.

Le président du Comité R a organisé un premier contact mardi prochain avec des représentants de la FEB pour s'informer davantage sur la question.

Avec l'accord de la commission de suivi, le Comité R pourrait participer comme observateur aux réunions envisagées. Cela lui permettrait de mieux cerner ce qui se passe dans ce domaine.

Le complément de rapport annuel aborde aussi les nouvelles compétences du Comité R comme organe de recours en matière d'habilitations de sécurité. Le Comité R a particulièrement examiné la plainte d'un particulier dans la perspective de cette nouvelle mission. Il lui est apparu que la nouvelle procédure exigera un devoir de motivation plus strict dans le cadre de la prise en compte du respect des droits de la défense.

2. ÉCHANGE DE VUES

Un membre fait remarquer qu'en ce qui concerne les communications internationales, notre État n'est plus à même de garantir la confidentialité des correspondances. Le problème est donc réel même si l'espionnage économique ne constitue que 3 ou 4% de cette activité.

Ce chiffre est très important lorsque l'espionnage se concentre sur des éléments purement stratégiques.

Par rapport à l'existence du système «Échelon», nous n'avons aucune surveillance légale. Les États-Unis se portent garants pour les citoyens américains mais ne disent pas qu'ils respectent les droits des citoyens dans d'autres pays.

Le même orateur fait d'ailleurs remarquer que le Comité R, à la page 98 de son rapport, écrit: «Encore imprégné du contenu technique de son rapport d'activités 1999 relatif au système planétaire d'interception de communications baptisé «Échelon» dont l'existence a depuis lors été admis par ses utilisateurs ...».

Le Comité R affirme donc clairement l'existence d'Échelon.

Par rapport à cette technologie, l'orateur marque son accord avec la recommandation du Comité R d'envisager la mise sur place d'un service chargé d'apporter une solution à l'ensemble de la problématique de la sécurisation de l'information.

De voorzitter van het Comité deelt de begeleidingscommissies mee dat het Comité I door het Verbond van Belgische ondernemingen (VBO) is uitgenodigd om ontmoetingen bij te wonen met de inlichtingendiensten over de bescherming van de communicatie van de ondernemingen. Het VBO maakt zich zorgen over het gevaar dat de interceptiesystemen kunnen betekenen voor ons wetenschappelijk, economisch en industrieel potentieel.

De voorzitter van het Comité I zal volgende dinsdag een eerste ontmoeting hebben met de vertegenwoordigers van het VBO om meer over de kwestie te vernemen.

Als het de toestemming krijgt van de begeleidingscommissie, kan het Comité I als waarnemer deelnemen aan de geplande vergaderingen. Zo krijgt het een beter beeld van het probleem.

Het aanvullende activiteitenverslag behandelt eveneens de nieuwe bevoegdheden van het Comité I als beroepsorgaan inzake veiligheidsmachtigingen. Het Comité I heeft de klacht onderzocht van een privé-persoon in het kader van deze nieuwe opdracht. Daaruit is gebleken dat bij de nieuwe procedure een strengere motiveringsplicht vereist is met het oog op de eerbiediging van de rechten van de verdediging.

2. GEDACHTEWISSELING

Een lid wijst erop dat de Staat de vertrouwelijkheid van internationale communicaties niet kan garanderen. Het probleem is reëel, al vormt de economische spionage maar 3 of 4% van deze activiteit.

Dat cijfer kan heel belangrijk zijn als de spionage strategische elementen betreft.

Wij hebben geen enkele vorm van wettelijk toezicht op het Echelon-systeem. De Verenigde Staten staan wel borg voor de Amerikaanse burgers, maar beweren niet dat zij de rechten van de burgers van andere landen zullen eerbiedigen.

Dezelfde spreker wijst erop dat het Comité I op blz. 102 van zijn verslag schrijft: «Nog volledig doordrongen van de technische inhoud van zijn activiteitenverslag 1999 over het wereldomvattend systeem voor het intercepteren van communicatie, Echelon genoemd, waarvan de gebruikers het bestaan inmiddels hebben toegegeven ...».

Het Comité I bevestigt dus uitdrukkelijk het bestaan van Echelon.

Spreker is het eens met de aanbeveling van het Comité I om een dienst op te richten die moet zorgen voor een oplossing voor het hele probleem van de beveiliging van informatie.

L'orateur reste, par contre, perplexe quant à l'invitation de la FEB au Comité R. Il voudrait savoir dans quel contexte ces réunions auront lieu.

Un intervenant estime que, si des membres de nos services de renseignements sont invités par la FEB pour réfléchir sur la protection des secrets scientifiques et industriels de notre pays, il est préférable qu'un membre du Comité R soit présent. Cela permet au Parlement de suivre ce qui se passe.

L'intervenant est convaincu que cela se fait partout en Europe. Les entrepreneurs sont obligés de réfléchir sur leur sécurité industrielle. Dans ce cadre, ils font venir les spécialistes des services de renseignements. En tant que parlementaire, il préfère que quelqu'un d'un organe du Parlement soit témoin de ce qui se dit lors de ses réunions.

Un membre s'étonne de la nature des matières qui sont discutées au sein de ces commissions. Au chapitre IV de son rapport, le Comité R signale qu'il a participé à une conférence sur la prolifération des armes chimiques et bactériologiques. Cette activité cadre-t-elle encore avec le contrôle des services de renseignements de notre pays ?

Il apprend également, à son grand étonnement, que le Comité P devrait examiner le Traité Schengen. Il se demande comment on peut faire relever pareilles activités des missions légales confiées aux comités permanents de contrôle.

L'intervenant ne voit pas quel est le lien entre la mission de contrôle légale du Comité R et une conférence au cours de laquelle sont discutés les attentats au gaz sarin dans le métro de Tokyo. Le Comité R a-t-il participé à cette conférence pour vérifier si nos services de renseignements y étaient présents ?

L'intervenant demande au président de la commission de suivi si le Comité R n'est pas en train de jouer lui-même, en l'espèce, le rôle de service de renseignements.

Même l'enquête sur « Échelon » lui semble ne pas ressortir au contrôle des services de renseignements. N'appartient-il pas plutôt aux services de renseignements eux-mêmes de procéder à cette enquête ?

Il est peut-être davantage indiqué que le comité se concentre sur sa véritable mission, qui est de contrôler les services de renseignements. C'est ainsi que ces derniers constituent toujours des dossiers sur des parlementaires, même s'ils ne s'intéressent qu'à leurs activités qui se situent en dehors de leur mission parlementaire.

L'intervenant estime qu'il est davantage indiqué que le Comité R contrôle la manière dont nos services de renseignements suivent des groupes de fondamentalistes.

Overigens is spreker stomverbaasd over de uitnodiging van het Comité I door het VBO. Hij wil weten in welke context deze vergaderingen georganiseerd worden.

Een ander spreker vindt het een goed idee dat een lid van het Comité I aanwezig is wanneer de inlichtingendiensten op verzoek van het VBO discussiëren over de bescherming van de wetenschappelijke en industriële geheimen van dit land. Zo blijft het Parlement ten minste op de hoogte van wat er gebeurt.

Spreker is ervan overtuigd dat dat overal in Europa gebeurt. Alle ondernemers zijn verplicht om zich te bekommeren om de industriële veiligheid. Daarom laten zij specialisten van de inlichtingendiensten komen. Als parlementslid geeft hij er de voorkeur aan dat een orgaan van het Parlement getuige is van wat tijdens deze vergaderingen wordt besproken.

Een lid verbaast zich over de aard van de aangelegenheden die in deze commissies besproken worden. In hoofdstuk IV van zijn verslag vermeldt het Comité I dat het heeft deelgenomen aan een conferentie over de proliferatie van bacteriologische en chemische wapens. Kadert dit nog in het toezicht op de inlichtingendiensten van dit land ?

Tot zijn verbazing hoort hij ook dat het Comité P het Schengenverdrag onder de loep zou moeten nemen. Hij vraagt zich af op welke manier dergelijke activiteiten binnen de wettelijke opdrachten van de vaste comités van toezicht vallen.

Spreker ziet niet in wat het verband is tussen de wettelijke controleopdracht van het Comité I en een conferentie waarop de aanslagen in de metro van Tokio met saringas besproken worden. Heeft het Comité I aan deze conferentie deelgenomen om na te gaan of onze inlichtingendiensten aanwezig waren ?

Aan de voorzitter van de begeleidingscommissie vraagt spreker of het Comité I hier niet zelf de rol van inlichtingendienst aan het spelen is.

Zelfs het onderzoek naar Echelon lijkt hem buiten het bestek van het toezicht op de inlichtingendiensten te vallen. Is het niet eerder een taak van de inlichtingendiensten zelf om dit onderzoek te doen ?

Wellicht is het meer aangewezen dat het Comité I zich toespitst op zijn eigenlijke opdracht : het toezicht op de inlichtingendiensten. Zo worden er door de inlichtingendiensten nog steeds dossiers aangelegd over parlementsleden, zij het over de activiteiten die buiten hun parlementaire opdracht vallen.

Zo lijkt het hem ook veel meer aangewezen dat het Comité I zou toezien op de wijze waarop onze inlichtingendiensten fundamentalistische groeperingen volgen.

Un autre membre rappelle à ce propos l'article premier de la loi organique du contrôle des services de renseignements: «...Le contrôle porte en particulier sur la protection des droits que la Constitution et la loi confèrent aux personnes, ...».

Dans ce cadre, l'enquête sur »Échelon» s'inscrit évidemment dans les missions du Comité R.

Le préopinant estime que l'on peut alors parler de double emploi. Nos services de renseignements sont déjà chargés de protéger nos droits. Il estime qu'il n'appartient pas au Comité R de faire la même chose et qu'il devrait s'occuper d'affaires qui sont plus importantes d'un point de vue politique.

Selon un autre membre, c'est à juste titre que l'on a fait référence à l'article 1er de la loi organique du 18 juillet 1991. Le contrôle externe sur les services de police et de renseignements trouve son origine dans le plan de Pentecôte. Initialement, l'intervenant avait déposé une proposition confiant l'exercice de ce contrôle externe directement au Parlement.

Le Conseil d'État ayant formulé des objections, l'on a en fin de compte opté pour un contrôle exercé par des comités indépendants qui seraient des organes du Parlement.

Le contrôle externe doit permettre de vérifier dans quelle mesure nos services de renseignements remplissent, comme il se doit, leur mission primaire, à savoir la protection du citoyen. Dans ce cadre, les comités de contrôle doivent vérifier si les services de renseignements suivent suffisamment les organisations subversives auxquelles sont associés ou non des parlementaires. Dans le passé également, certains parlementaires ont déjà posé des questions en la matière.

Un membre souligne l'importance des rapports du Comité R sur le système «Échelon». Il s'est avéré que nos deux services de renseignements n'ont pas les moyens de vérifier si le système existe. Cette donnée est très importante et il est tout à fait normal que le Comité R ait mené une enquête.

Le président du Comité R souligne que la principale conclusion du Comité R sur le système Échelon est qu'il faut protéger nos communications. Le Comité a fait preuve d'un certain réalisme et à cet égard il faut tenir compte de l'évolution du dossier depuis le dépôt des premiers rapports.

Il est clair qu'aucun des services concernés, américains, britanniques ou canadiens, ne parle d'Échelon en tant que tel. Tout au plus existent des aveux périphériques. Le directeur de la CIA admet que ces services pratiquent l'espionnage mais ne parle pas d'Échelon.

Le Royaume-Uni ne confirme ni n'infirme l'existence d'Échelon mais reconnaît toutefois la

Een ander lid herinnert in dat verband aan artikel 1 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten: «...Het toezicht heeft in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen waarborgen,...».

Uiteraard behoort het onderzoek naar Echelon dan ook tot de taken van het Comité I.

De vorige spreker meent dat er dan sprake is van dubbel gebruik. Onze inlichtingendiensten hebben reeds een opdracht die erop gericht is om onze rechten te vrijwaren. Hij meent dat het Comité I dit niet nogmaals moet doen en dat het zich met politiek belangrijker zaken zou moeten bezig houden.

Een ander lid meent dat terecht verwezen is naar artikel 1 van de organieke wet van 18 juli 1991. Het extern toezicht op de politie- en inlichtingendiensten vloeit voort uit het Pinksterplan. Oorspronkelijk had spreker een voorstel ingediend waarbij dit extern toezicht rechtstreeks door het Parlement zou worden uitgeoefend.

Ingevolge de bezwaren van de Raad van State is uiteindelijk gekozen voor een toezicht door onafhankelijke comités die organen zijn van het Parlement.

Het extern toezicht moet nagaan in hoeverre onze diensten hun primaire opdracht, de bescherming van de burger, naar behoren vervullen. In die functie moeten zij nagaan of de diensten subversieve organisaties, waarbij al dan niet parlementsleden zijn betrokken, voldoende opvolgen. Ook in het verleden hebben parlementsleden hier reeds vragen over gesteld.

Een lid benadrukt het belang van de verslagen van het Comité I over het Echelon-systeem. Daaruit is gebleken dat onze beide inlichtingendiensten niet de nodige middelen hebben om na te gaan of dit systeem bestaat. Dat is een belangrijk gegeven en het is niet meer dan normaal dat het Comité I een onderzoek heeft ingesteld.

De voorzitter van het Comité I benadrukt dat de voornaamste conclusie van het Comité over het Echelon-systeem is dat onze communicatie beschermd moet worden. Het Comité heeft blijk gegeven van realiteitszin en er moet ook rekening worden gehouden met de ontwikkeling die het dossier sinds de indiening van de eerste verslagen heeft ondergaan.

Geen van de betrokken diensten — de Amerikaanse, Britse of Canadese — vermeldt Echelon als zodanig. Hoogstens is er sprake van onrechtstreekse bekentenissen. De directeur van de CIA geeft toe dat zijn diensten spioneren maar spreekt niet over Echelon.

Het Verenigd Koninkrijk bevestigt noch ontkent het bestaan van Echelon maar beweert dat interceptie

nécessité des interceptions en vue de protéger son potentiel économique.

L'élément le plus récent est le rapport du commissaire canadien qui reconnaît la mission des services de faire des interceptions électromagnétiques de toute sorte de communications. La reconnaissance de l'aspect global du système résulte du fait qu'il reconnaît la difficulté en pratique de protéger la vie privée des citoyens canadiens. Le plus grand problème dans un tel système d'interceptions est que les droits des citoyens ne peuvent être totalement garantis. On essaye donc de limiter au maximum les interceptions involontaires.

Cela montre bien qu'il y a un système global. Une autre grande difficulté provient également de l'énorme quantité d'informations recueillies et de la difficulté d'identifier dans cette masse de données les communications interessantes.

Les experts consultés par le Comité R ont indiqué qu'il n'y a qu'1% des communications téléphoniques internationales qui passent par satellite. On accorde donc probablement une trop grande importance au système. C'est le sens des nuances apportées par le Comité R dans son rapport.

À propos de l'invitation de la FEB, le président du Comité R précise qu'il s'agit d'une réflexion sur l'évaluation des risques des entreprises en Belgique. La FEB voudrait réunir les services de renseignements et certains acteurs du monde des télécommunications (par exemple Belgacom) autour de la table, afin d'identifier les risques et d'examiner les mesures qu'on peut prendre.

Cette invitation était en premier lieu adressée aux services de renseignements. Le Comité R a été invité pour avoir une connaissance de ce qui se passe.

M. Delepière souligne que le Comité R n'assiste pas à des séminaires dans un but qui dépasse ses missions légales. Pour effectuer un contrôle, et savoir si les droits des citoyens sont bien protégés, le Comité R essaie de s'informer sur les risques existants. Cela lui permet d'interpeller nos services de renseignements.

À la conférence sur la prolifération des armes chimiques et bactériologiques, il n'y avait pas de représentants de nos services. Il y avait un public très divers (médecins, professeur, etc.). Assister à une telle conférence permet au Comité R de vérifier si nos services de renseignements sont attentifs à ces dangers. Le principe de précaution nous impose d'interroger nos services sur leur pratique en la matière, l'évaluation du risque, la capacité d'appréhender cette menace.

Une autre conférence portait sur la protection du potentiel économique et scientifique. Cela a permis au Comité R de charger le service d'enquêtes d'examiner ce que nos services font sur ce point.

nodig is om zijn economisch potentieel te beschermen.

Het meest recente element komt uit een verslag van de Canadese commissaris die toegeeft dat de diensten tot taak hebben om elektromagnetische intercepties uit te voeren van alle soorten communicatie. Hij geeft toe dat het in de praktijk moeilijk is om de persoonlijke levenssfeer van de Canadezen te beschermen, waardoor hij in feite bevestigt dat het om een wereldwijd systeem gaat. Het grote probleem met zo'n interceptiesysteem is dat de rechten van de burger niet volledig gewaarborgd zijn. Men tracht het aantal onopzettelijke intercepties zoveel mogelijk te beperken.

Dat toont goed aan dat er een wereldwijd systeem is. Een andere grote moeilijkheid schuilt in de enorme massa verzamelde informatie, waardoor het moeilijk wordt de interessante communicaties eruit te pikken.

De deskundigen die het Comité I heeft geraadpleegd, zeggen dat slecht 1% van het internationale telefoonverkeer via satelliet gaat. Wellicht hecht men te veel belang aan het systeem. Daarom brengt het Comité I in zijn verslag nuances aan.

Wat de uitnodiging van het VBO betreft, verduidelijkt de voorzitter van het Comité I dat getracht wordt de risico's voor Belgische ondernemingen te evalueren. Het VBO wil de inlichtingendiensten en bepaalde personen uit de telecommunicatiesector (bijvoorbeeld Belgacom) samen rond de tafel brengen om deze risico's te identificeren en na te gaan welke maatregelen kunnen worden genomen.

Deze uitnodiging was in de eerste plaats tot de inlichtingendiensten gericht; het Comité I is uitgenodigd opdat het op de hoogte is van wat er gebeurt.

De heer Delepière benadrukt dat het Comité I zijn boekje niet te buiten gaat door deel te nemen aan seminaries. Om controle te kunnen uitoefenen en te weten of de rechten van de burgers goed beschermd zijn, wil het Comité I zich informeren over de bestaande risico's. Alleen op die manier kan het de inlichtingendiensten eventueel tot de orde roepen.

Bij de conferentie over de proliferatie van chemische en bacteriologische wapens waren geen vertegenwoordigers van onze diensten aanwezig. Er was een zeer uiteenlopend publiek (artsen, professoren, enz.). Door het bijwonen van zo'n conferentie kan het Comité I nagaan of onze inlichtingendiensten oog hebben voor deze gevaren. Het voorzorgsbeginsel wil dat we de diensten ondervragen over hun beleid ter zake, de beoordeling van het risico, het vermogen om deze dreiging op te vangen.

Een andere conferentie ging over de bescherming van het economisch en wetenschappelijk potentieel. Zo kon het Comité I de Dienst enquêtes opdragen om na te gaan wat onze diensten op dat vlak uitvoeren.

De telles activités du Comité R n'ont donc pas une finalité opérationnelle mais visent uniquement à permettre un contrôle efficace, à vérifier si le citoyen est protégé et à déterminer si nos services sont efficaces. Tout cela permet au Comité R de sensibiliser nos services à prendre des mesures plus appropriées.

Un membre demande si la FEB a également invité des services de renseignements privès.

Le président du Comité R répond que cela n'est pas le cas. Le seul but de la FEB est de mieux appréhender le problème. Le Comité R a demandé plus d'in for mations sur cette initiative. Dès qu'il disposera d'informations plus précises, il en donnera connaissance au président de la commission de suivi.

Le président du Comité P souligne le fait que le Comité P ne s'est jamais proposé d'évaluer l'accord de Schengen. Il est toutefois important d'être conscient de la réalité. Lorsque l'on parle de traite d'êtres humains et que l'on constate qu'un groupe de clandestins albanais, intercepté à Bruxelles, est accompagné d'un gendarme italien, on doit vérifier ce qui se passe.

La même conclusion s'impose lorsqu'un agent de police belge est arrêté à l'étranger.

Tant le Comité P que le Comité R participent à des conférences. Les comités permanents de contrôle n'ont rien à voir avec les services de renseignements mais si les comités ne suivent pas certaines évolutions, le contrôle devient sourd et aveugle. Les deux comités doivent donc disposer des éléments et des informations nécessaires pour remplir leur tâche comme il se doit.

Un sénateur partage ce point de vue et estime qu'il est évident que le Comité R s'occupe d'Échelon. Nos services de renseignements admettent qu'ils ne disposent pas de la capacité nécessaire pour s'informer sur Échelon, *a fortiori* qu'ils ne peuvent pas offrir une protection adéquate contre ce système. Le même problème se pose d'ailleurs au niveau européen. Aussi pense-t-il qu'en tant qu'organe de contrôle, le Comité R doit informer le Parlement lorsqu'il s'avère que les services de renseignements ne sont pas en mesure de faire face à ces problèmes. C'est là une de leurs missions de contrôles essentielles.

En ce qui concerne les dossiers qui ont été constitués à l'égard de parlementaires, le président du Comité R confirme que des enquêtes ont déjà été faites précédemment sur ce sujet. Il rappelle que, lors de la précédente législature, le Comité R était chargé de faire une évaluation annuelle de ces dossiers.

Par rapport aux enquêtes relatives à certaines formes d'intégrisme religieux, le Comité R a plusieurs enquêtes en cours.

Deze activiteiten van het Comité I hebben dus geen operationeel doel maar strekken ertoe een efficiënte controle mogelijk te maken, na te gaan of de burger beschermd is en of onze diensten doeltreffend zijn. Zo kan het Comité I onze diensten ertoe aanzetten om meer aangepaste maatregelen te nemen.

Een lid vraagt of het VBO ook de privé-inlichtingendiensten heeft uitgenodigd.

De voorzitter van het Comité I antwoordt ontkennend. Het VBO wil alleen het probleem beter begrijpen. Het Comité I heeft meer informatie gevraagd over dit initiatief. Zodra hij deze informatie heeft, zal hij ze aan de voorzitter van de begeleidingscommissie meedelen.

De voorzitter van het Comité P vestigt de aandacht op het feit dat het Comité P nooit voorgesteld heeft om Schengen te evalueren. Het is evenwel belangrijk om oog te hebben voor de realiteit. Wanneer men over mensenhandel spreekt, en moet vaststellen dat een groep Albanese illegalen in Brussel wordt onderschept, waarbij blijkt dat ze worden geleid door een Italiaanse carabiniero, dan moet men nagaan wat er aan de hand is.

Een zelfde conclusie dringt zich op wanneer een Belgische politieman in het buitenland wordt gearresteerd.

Zowel het Comité P als het Comité I nemen deel aan conferenties. De vaste comités van toezicht staan buiten de diensten maar als de comités bepaalde ontwikkelingen niet volgen, dan is het toezicht blind en doof. Beide comités moeten dus over de nodige elementen en informatie beschikken om hun taak naar behoren te vervullen.

Een senator treedt deze zienswijze bij en vindt het vanzelfsprekend dat het Comité I zich met Echelon bezighoudt. Onze inlichtingendiensten geven toe dat zij niet over de capaciteit beschikken om iets over Echelon te weten te komen, laat staat dat zij een afdoende bescherming kunnen bieden. Dit probleem bestaat trouwens evengoed op Europees niveau. Hij meent dan ook dat het Comité I, als toezichtsorgaan, het Parlement moet informeren als blijkt dat de diensten deze problemen niet aankunnen. Dit behoort tot de essentie van hun toezichtsopdracht.

Wat de dossiers over de parlementsleden betreft, bevestigt de voorzitter van het Comité I dat in dit verband reeds eerder onderzoek is verricht. Tijdens de vorige zittingsperiode moest het Comité I een jaarlijkse evaluatie maken van die dossiers.

Daarnaast voert het Comité I onderzoeken uit naar bepaalde vormen van religieus fundamentalisme.

Un sénateur propose d'examiner le suivi des dossiers, constitués par la Sûreté de l'État sur les parlementaires, lors d'une prochaine réunion.

Le président du Comité R annonce que le Comité R transmettra prochainement une nouvelle mise à jour du dossier « Échelon » aux présidents des deux commissions.

Un sénateur s'interroge sur les raisons pour lesquelles le système « Échelon » a été rendu public, alors qu'il existait depuis longtemps. Quelle est la manipulation politique et volontaire derrière tout cela ?

Il se demande si le but final n'est pas une déstabilisation de l'Union européenne. En prenant connaissance du dossier Échelon, il se peut que ce soit une manœuvre pour diviser les Anglais des autres membres de l'Union, ce qui affaiblirait tout projet de défense européen.

Le système Échelon touche à la fois à la souveraineté et à la sécurité des États, à la sécurité des intérêts économiques et à la liberté des citoyens.

*
* *

Les commissions de suivi rappellent qu'elles ont décidé de faire elles-mêmes un rapport sur le système « Échelon ». Mme Lizin (Sénat) et M. Van Parijs (Chambre) ont été designés comme rapporteurs.

Le présent rapport est approuvé à l'unanimité des membres présents.

Les rapporteurs, *Les présidents,*
Marc HORDIES. Armand DE DECKER.
Géraldine PELZER-SALANDRA. Herman DE CROO.

Een senator stelt voor om tijdens een volgende vergadering de dossiers te onderzoeken die de Veiligheid van de Staat over de parlementsleden heeft aangelegd.

De voorzitter van Comité I kondigt aan dat de nieuwe ontwikkelingen in het Echelon-dossier binnen afzienbare tijd aan de voorzitters van de twee commissies zullen worden meegedeeld.

Een senator vraagt zich af waarom het Echelonsysteem nu pas aan het licht is gekomen, terwijl het al een hele tijd bestaat. Welke politieke machinaties zitten daar achter ?

Hij vraagt zich af of het uiteindelijke doel niet de ontwrichting van de Europese Unie is. Misschien is het de bedoeling onenigheid te zaaien tussen het Verenigd Koninkrijk en de andere lidstaten om zo stokken in de wielen te steken van het Europees defensieproject.

Het Echelon-systeem raakt aan de soevereiniteit en de veiligheid van de Staten, aan de beveiliging van de economische belangen en aan de vrijheid van de burgers.

*
* *

De begeleidingscommissies herinneren eraan dat zij zelf een verslag zullen opstellen over het Echelonsysteem. Mevrouw Lizin (Senaat) en de heer Van Parijs (Kamer) zijn aangewezen als rapporteurs.

Dit verslag is eenparig goedgekeurd door de aanwezige leden.

De rapporteurs, *De voorzitters,*
Marc HORDIES. Armand DE DECKER.
Géraldine PELZER-SALANDRA. Herman DE CROO.

3. ANNEXE : RAPPORT D'ACTIVITÉS 1999 COMPLÉMENTAIRE DU COMITÉ R

PRÉAMBULE

À monsieur le Président du Sénat,

À monsieur le Président de la Chambre des représentants,

À monsieur le ministre de la Justice,

À monsieur le ministre de la Défense nationale,

Messieurs les Présidents,

Messieurs les ministres,

Le 14 février 2000, les Commissions réunies de la Chambre des représentants et du Sénat, respectivement chargées du suivi des Comités permanent P et R, approuvaient le rapport d'activité 1999 du Comité permanent R couvrant la période du 1er août 1998 au 30 septembre 1999. Ce rapport avait été déposé à l'attention des Présidents de la Chambre des représentants et du Sénat, le premier jour de la session ordinaire des deux assemblées, soit le 12 octobre 1999, comme le prescrit l'article 35 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

À l'occasion de l'approbation des rapports généraux d'activités des Comités permanents P et R, il fut proposé de faire coïncider dorénavant la période couverte par ces rapports avec l'année civile.

En attendant la modification formelle dans ce sens des articles 11, 1º, et 35, 1º, de la loi précitée, il fut demandé aux deux Comités d'établir, pour avril 2000, un complément de rapport couvrant le dernier trimestre de 1999.

Le présent rapport répond à cette demande en reprenant notamment le compte rendu des enquêtes de contrôle terminées et transmises au cours de cette période au Comité permanent R par son Service d'enquêtes. Le Comité R a également estimé opportun d'y joindre le texte de deux enquêtes clôturées au début de l'année 2000, dont le « rapport complémentaire sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau « Échelon » d'interception des communications ».

Il est important de rappeler les raisons pour lesquelles les enquêtes publiées dans le présent rapport sont rédigées en termes généraux. Conformément aux dispositions du chapitre IV du règlement d'ordre intérieur du Comité R publié au *Moniteur belge* du 7 octobre 1994, les membres du Comité R ont, en

3. BIJLAGE : AANVULLEND ACTIVITEITENVERSLAG 1999 VAN HET COMITÉ I

VOORWOORD

Aan de heer Voorzitter van de Senaat,

Aan de heer Voorzitter van de Kamer van volksvertegenwoordigers,

Aan de heer minister van Justitie,

Aan de heer minister van Landsverdediging,

Geachte heren Voorzitters en ministers,

Op 14 februari 2000 keurden de Verenigde Commissies van de Kamer van volksvertegenwoordigers en van de Senaat, respectievelijk gelast met de begeleiding van de Vaste Comités P en I, het activiteitenverslag 1999 goed van het Vast Comité I dat de periode van 1 augustus 1998 tot 30 september 1999 besloeg. Dit rapport werd ter attentie van de Voorzitters van de Kamer van volksvertegenwoordigers en van de Senaat ingediend op de eerste dag van de gewone zitting van de twee vergaderingen, namelijk op 12 oktober 1999, zoals voorgeschreven in artikel 35 van de wet van 18 juli 1991 houdende het toezicht op de politie- en inlichtingendiensten.

Ter gelegenheid van de goedkeuring van de algemene activiteitenverslagen van de Vaste Comités P en I, werd voorgesteld om in de toekomst de referteperiode van deze rapporten te doen samenvallen met het burgerlijk jaar.

In afwachting van een formele wijziging in deze zin van de artikelen 11, 1º, en 35, 1º, van voornoemde wet, werd aan beide Comités gevraagd om voor april 2000 een aanvullend verslag op te stellen dat de laatste trimester van 1999 zou beslaan.

Het hiernavolgend verslag beantwoordt aan dit verzoek en herneemt onderdeel de verslagen van de toezichtsonderzoeken die in deze periode door zijn Dienst Enquêtes werden afgesloten en doorgezonden aan het Vast Comité I. Het Comité I achtte het eveneens opportuun om hierbij twee toezichtsonderzoeken toe te voegen die in het begin van het jaar 2000 werden afgesloten, waaronder het aanvullend verslag over de wijze waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een netwerk « Echelon » genaamd, voor het onderscheppen van communicaties.

Het is van belang om hierbij te herinneren aan de redenen waarom de gepubliceerde onderzoeken in dit rapport in algemene termen zijn opgesteld. Overeenkomstig de bepaling van hoofdstuk IV van het huishoudelijk reglement van het Comité I (gepubliceerd in het *Belgisch Staatsblad* van 7 oktober 1994), zien de

effet, veillé de cette façon à permettre une large diffusion des résultats d'enquêtes de contrôle, sans mention de situations particulières et sans identification nominale des personnes (article 79, alinéa 2).

Ce faisant, le Comité permanent R a également tenu compte des autres impératifs stipulés dans le règlement d'ordre intérieur, à savoir: le préjudice qui pourrait être fait au bon fonctionnement des services de renseignements nationaux et étrangers, la protection de la vie privée et la préservation de l'intégrité physique des personnes, la coopération internationale entre différents services, le droit des plaignants de connaître la suite qui a été réservée à leur plainte, le droit des citoyens de s'assurer du bon fonctionnement des services de renseignement (article 66, alinéa 5).

Enfin, les avis des ministres concernés par les textes destinés à la publication ont chaque fois été sollicités pour tous les rapports relatifs à des enquêtes de contrôle, conformément à l'article 37 de la loi organique du contrôle des services de renseignements.

Ce rapport comprend aussi les commentaires formulés par le Comité permanent R, à la demande de monsieur le ministre de la Justice, à l'égard de la Recommandation 1402 (1999) sur le contrôle des services de sécurité intérieure dans les États membres du Conseil de l'Europe, émise le 26 avril 1999 par l'Assemblée parlementaire dudit Conseil.

Il faut mentionner également qu'au cours de la période considérée neuf nouvelles enquêtes de contrôle ont été ouvertes à l'initiative du Comité permanent R sur les activités des deux services de renseignement visés par la loi organique précitée, portant à 14 le total des enquêtes encore en cours au 31 décembre. Du 1er octobre au 31 décembre 1999, le Comité R a tenu 11 réunions.

Le Comité R a également eu, au cours de cette période, des contacts avec l'Autorité Nationale de sécurité concernant les dispositions légales de la loi du 11 décembre 1998 instituant notamment le Comité R en qualité d'organe de recours en matière d'habilitation de sécurité. Ces dispositions entrent en vigueur le 1er juin 2000.

Le 26 novembre 1999 étaient installés les nouveaux membres du Comité permanent de contrôle des services de police. Parmi ces membres, il faut mentionner la présence de madame Danielle Cailloux qui faisait partie jusqu'à cette date du Comité permanent R.

Ce dernier fonctionne depuis lors avec trois membres à temps plein, de façon transitoire, puisqu'il faut rappeler que la loi du 1er avril 1999 modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements a notamment

leden van het Comité I er inderdaad op toe om op deze wijze een ruime verspreiding van de resultaten van de toezichtsonderzoeken te bereiken zonder evenwel melding te maken van de bijzonderheden van de situaties en van de namen van personen (artikel 79, lid 2).

Hierdoor houdt het Comité I ook rekening met de andere vereisten gesteld in het huishoudelijk reglement, zijnde het nadeel dat zou kunnen toegebracht worden aan de goede werking van de nationale en buitenlandse inlichtingendiensten, de bescherming van de persoonlijke levenssfeer en de vrijwaring van de fysieke integriteit van personen, de internationale samenwerking tussen de verschillende diensten, het recht van de indieners van een klacht om kennis te nemen van het gevolg dat gegeven werd aan hun klacht en het recht van de burgers om zich te vergewissen van de goede werking van de inlichtingendiensten (artikel 66, lid 5).

Uiteindelijk werd telkens van elk verslag van de toezichtsonderzoeken het advies van de betrokken ministers gevraagd overeenkomstig artikel 37 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten.

Dit verslag bevat eveneens de commentaren opgesteld door het Vast Comité I op verzoek van de minister van Justitie betreffende de Aanbeveling 1402 (1999) op de controle op de binnenlandse veiligheidsdiensten van de lidstaten van de Raad van Europa, zoals uitgebracht op 26 april 1999 door de Algemene Vergadering van voornoemde Raad.

Hierbij moet vermeld dat in de loop van deze periode negen nieuwe onderzoeken werden ingesteld op initiatief van het Comité I aangaande de activiteiten van de twee inlichtingendiensten die vallen onder de voornoemde wet, wat het totaal van lopende onderzoeken op 31 december 1999 op veertien brengt. Vanaf 1 oktober 1999 tot 31 december 1999 hield het Comité I elf vergaderingen.

Het Comité I heeft tijdens deze periode eveneens contacten gehad met de Nationale Veiligheidsoverheid betreffende de bepalingen van de wet van 11 december 1998, die het Comité I aanstelt als beroepsorgaan inzake veiligheidsmachtigingen. Deze bepalingen gaan van kracht vanaf 1 juni 2000.

Op 26 november 1999 werden de nieuwe leden van het Vast Comité van toezicht op de politiediensten geïnstalleerd. Bij deze leden moet men de aanwezigheid van mevrouw Danielle Cailloux vermelden die tot dan deel uitmaakte van het Vast Comité I.

Dit laatste is sindsdien dus werkzaam met drie voltijdse leden, en dit bij wijze van overgang. Immers bracht de wet van 1 april 1999 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, het aantal vaste leden

ramené le nombre des membres effectifs du Comité permanent R de cinq à trois, dont deux membres non permanents, le président exerçant seul son mandat à plein temps.

Il convient enfin de souligner l'excellence des relations qui se sont établies entre les deux Comités de contrôle P et R. Celles-ci se sont notamment manifestées lors de l'organisation commune de la conférence sur : « The recent developments in the field of open source intelligence in North-America » présentée par monsieur Robert Steele, le 14 avril dernier au siège des Comités P et R.

Nous vous prions de croire, messieurs les Présidents, messieurs les ministres, en l'assurance de notre haute considération.

Bruxelles, le 8 mai 2000

Jean-Claude DELEPIÈRE
Président

Gérald VANDE WALLE
Conseiller

Jean-Louis PRIGNON
Conseiller

Wouter DE RIDDER
Greffier

van het Comité I van vijf tot drie waarvan twee leden niet voltijds, enkel de voorzitter oefent zijn opdracht voltijds uit.

Tot slot is het passend de uitstekende verstandhouding die zich tussen de twee toezichtscomités P en I heeft ontwikkeld, te onderlijnen. Deze werd onder meer aangetoond ter gelegenheid van de gemeenschappelijke organisatie van de conferentie over « The recent developments in the field of open source intelligence in North-America » die werd gegeven door de heer Robert Steele op 14 april jongstleden op de zetel van de Vaste Comités P en I.

Met de meeste hoogachting,

Brussel, 8 mei 2000

Jean-Claude DELEPIÈRE
Voorzitter

Gérald VANDE WALLE
Raadsheer

Jean-Louis PRIGNON
Raadsheer

Wouter DE RIDDER
Griffier

SOMMAIRE

INHOUD

TITRE I

LESSERVICESDERENSEIGNEMENTSBELGES

LES ENQUÊTES

A. À LA REQUÊTE DU PARLEMENT

CHAPITRE 1

RAPPORT COMPLÉMENTAIRE SUR LA MANIÈRE DONT LES SERVICES BELGES DE RENSEIGNEMENT RÉAGISSENT FACE À L'ÉVENTUALITÉ D'UN RÉSEAU «ÉCHELON» D'INTERCEPTION DES COMMUNICATIONS

1. Introduction

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

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

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

Le 31 janvier 2000, les commissions permanentes de la Chambre des représentants et du Sénat, respectivement chargées du suivi des Comités permanents P et R, se sont réunies pour examiner le rapport annuel d'activités de ce dernier, incluant l'enquête que le Comité R a consacré à la manière dont «les services

TITEL I

DE BELGISCHE INLICHTINGENDIENSTEN

DE TOEZICHTSONDERZOEKEN

A. OP VERZOEK VAN HET PARLEMENT

HOOFDSTUK 1

AANVULLEND VERSLAG OVER DE WIJZE WAAROP DE BELGISCHE INLICHTINGENDIENSTEN REAGEREN OP HET EVENTUEEL BESTAAN VAN EEN NETWERK «ECHELON» GENAAMD, VOOR HET ONDERSCHEPPEN VAN COMMUNICATIES

1. Inleiding

Het is aangewezen eraan te herinneren dat, op algemene wijze, het Vast Comité I zich in het verleden reeds gebogen heeft over de bescherming van informatica- en communicatiesystemen. In dit kader deed het in 1994 de aanbeveling dat een officieel organisme zou gelast worden met de ontwikkeling en de uitvoering van een globale veiligheidspolitiek van het geheel van de informatiesystemen van de openbare dienst.

Men kan in dezelfde gedachtengang de studie en het onderzoek uitgevoerd in 1998 vermelden over de deelname van de Belgische inlichtingendiensten, in het bijzonder SGR, aan programma's voor inlichtingensatellieten. De belangstelling van het Comité I voor deze materie kwam tegemoet aan een politieke bekommernis die onder andere geconcretiseerd werd in de regeringsverklaring van 28 juni 1995 die uitdrukking gaf aan de wens van dit land om «actief bij te dragen tot de uitwerking van een Europese veiligheidsarchitectuur die beoogt de stabiliteit van het Europese continent te bevorderen en nieuwe kloven te voorkomen» (activiteitenverslag 1998 — blz. 173 en volgende).

Het bestaan van een «Echelon»-netwerk dat werd opgezet door onder meer de Verenigde Staten en Groot-Brittannië met als doel alle Europese burgelijke telecommunicaties te onderscheppen werd aan het licht gebracht in september 1998 door een verslag bestemd voor het Europees Parlement. De verspreiding van dit verslag door de media wekte de belangstelling van bepaalde regeringen, de Franse in het bijzonder, evenals deze van het Belgisch Parlement.

Op 31 januari 2000 vergaderden de vaste begeleidingscommissies van de Kamer van volksvertegenwoordigers en van de Senaat, respectievelijk verantwoordelijk voor de opvolging van de Vaste Comités P en I, om het jaarlijks activiteitenverslag van dit laatste te onderzoeken met inbegrip van het onderzoek dat

belges de renseignements réagissent face à l'éventualité d'un système américain «Échelon» d'interception des communications téléphoniques et fax en Belgique».

Cette enquête avait été ouverte sur l'initiative de membres du Parlement fédéral. Ces derniers posaient également la question suivante: «Nos services cherchent-ils à établir l'existence du système Échelon, et le cas échéant, à protéger les entreprises et les citoyens belges contre ces interceptions?»

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

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

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

Le Service général du renseignement et de la sécurité avait considéré quant à lui l'existence du système «Échelon» comme un fait acquis. Bien qu'ayant ciblé «les menaces auxquelles se voit confrontée notre société de l'information et de la communication, dont «Échelon» n'est qu'une illustration», le SGR n'effectuait cependant pas de recherche active sur ce réseau, se fondant, d'une part, sur le fait que la défense du potentiel scientifique et économique n'est

(1) Depuis la clôture, en août 1999, de ce premier rapport d'enquête du Comité R, l'existence du réseau Échelon a été confirmée sur la base d'éléments que l'on trouvera repris et développés dans le rapport des experts mandatés par le Comité (voir p. 13 et suivantes).

het Comité I wijdde aan «de wijze waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België».

Dit onderzoek werd geopend op initiatief van het federaal Parlement. Hieraan werd eveneens de volgende vraag verbonden: «Proberen onze diensten bewijzen te verzamelen over het bestaan van dit systeem en, indien het zou bestaan, onze Belgische ondernemingen en burgers tegen deze intercepties te beschermen?»

Uit de conclusies van het eerste rapport(1) blijkt dat de Belgische inlichtingendiensten globaal genomen negatief op deze vragen antwoordden daarbij vooral het feit inroepend dat zij niet over de technische middelen beschikten die hen in staat zouden stellen om zelf het bestaan van het «Echelon-systeem» vast te stellen. Hun kennis over het onderwerp is dus uitsluitend gebaseerd op gegevens afkomstig uit de consultatie van open bronnen.

De Veiligheid van de Staat was dus niet bij machte om het bestaan van praktijken van intercepteren van telecommunicaties te bevestigen. Deze dienst verklaarde zich geconfronteerd te worden met een gebrek aan middelen zowel op het vlak van personeel als op materieel vlak. Haar onderzoeksmiddelen stelden haar dus niet in staat om het bestaan van het «Echelon-systeem» te bevestigen.

De organieke wet van 30 november 1998 op de inlichtingendiensten kent echter een bijzondere opdracht toe aan de Veiligheid van de Staat. In zijn artikel 7: «het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefineerd door het ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefineerd door de Koning op voorstel van het ministerieel Comité, bedreigd of zou kunnen bedreigen.»

De Algemene Dienst inlichtingen en veiligheid beschouwde wat haar betreft, dat het bestaan van het Echelon-systeem een vaststaand feit was. Hoewel gericht op «de bedreigingen waarmee onze informatie- en communicatiemaatschappij geconfronteerd wordt en waarvan Echelon enkel een illustratie is», heeft SGR nochtans geen actief onderzoek uitgevoerd naar dit netwerk zich beroepend enerzijds op het feit dat de verdediging van het wetenschappelijk en eco-

(1) Sinds het afsluiten in augustus 1999, van het eerste onderzoeksrapport van het Comité I werd het bestaan van het Echelon-netwerk bevestigd op basis van gegevens hernomen en uitgewerkt in het verslag van de deskundigen aangeduid door het Comité I.

pas une des compétences qui lui est attribuée par la nouvelle loi organique du 30 novembre 1998 sur les services de renseignements et, d'autre part, sur les restrictions légales qui lui sont imposées en matière de captage des radiocommunications.

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

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

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

2. Procédure

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

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

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

nomisch potentieel niet tot de bevoegdheden behoort die haar worden toegekend door de nieuwe organieke wet van 30 november 1998 op de inlichtingendiensten en, anderzijds op de wettelijke beperkingen die haar worden opgelegd wat betreft de interceptie van radiocommunicaties.

Volgens de bepalingen van de organieke wet, heeft SGR een opdracht ondernomen ter bescherming van de informatica- en communicatiesystemen van de militaire informatie- en communicatiesystemen evenals van degene die door het ministerie van Landsverdediging worden beheerd. Een uitbreiding van een dergelijke opdracht aan belangen andere dan militaire, wordt niet expliciet vermeld in de wet. Zonder enige twijfel kan men dit soort opdracht onderbrengen onder de verdediging van het wetenschappelijk of economisch potentieel, wat de bevoegdheid is van de Veiligheid van de Staat. Toch heeft SGR, vertegenwoordigd bij het College van inlichtingen en veiligheid, voorgesteld om bij te dragen zowel tot de conceptie van federale structuren als tot de uitwerking van een algemene politiek inzake de beveiliging van de informatica-netwerken.

Het algemeen activiteitenverslag 1999 van het Vast Comité I bevattende de eerste resultaten van het onderzoek aangaande de Echelon-problematiek, werd op 14 februari 2000 goedgekeurd door de Verenigde Commissies van de Kamer van volksvertegenwoordigers en van de Senaat, belast met de respektievelijke opvolging van de Vaste Comités P en I.

De Vaste Begeleidingscommissies hebben bovendien aan het Comité I de opdracht toevertrouwd om zijn onderzoeken verder te zetten in deze materie en hun het huidig aanvullend verslag voor midden maart 2000 te bezorgen.

2. Procedure

Door middel van de brief d.d. 17 februari 2000 heeft de voorzitter van het Comité I aan mevrouw Timmermans, administrateur-generaal a.i. van de Veiligheid van de Staat en aan generaal-majoor Michaux, chef van SGR, geïnformeerd dat de Vaste Begeleidingscommissies verzocht hadden om het onderzoek over het Echelon-netwerk verder te zetten.

Op 21 februari 2000 ontving het Comité I de brief van de voorzitter van de Senaat gedateerd op 14 februari 2000 met de bevestiging van dit verzoek in de volgende termen : « de begeleidingscommissies hebben duidelijk de wens geuit dat het Comité I het onderzoek over het Echelon-systeem zou verderzetten en, zich zou informeren in dit verband inzake de arrestatie van de Franse majoor « Bunel » teneinde te bepalen of de gegevens die geleid hebben tot zijn arrestatie, afkomstig zijn van een elektronisch bewakingssysteem. »

Op 22 februari 2000 besloot het Comité I als volgt :

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

— le professeur Yves Poullet, docteur en droit et directeur du Centre de recherche informatique et droit des Facultés Universitaires Notre Dame de la Paix à Namur et membre de la Commission de protection de la vie privée;

ainsi que son collaborateur,

— M. Jean-Marc Dinant, maître et doctorant en informatique, auteurs de plusieurs travaux de recherche sur le thème de la vie privée et de la sécurité des données personnelles sur Internet.

2. d'ouvrir une seconde enquête « sur la manière dont les services de renseignement ont participé à la découverte d'une affaire d'espionnage » et de charger le Service d'enquêtes de cette seconde investigation (1).

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

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

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

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

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

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

1. het onderzoek naar het Echelon-systeem zelf verder te zetten en zich hierbij te laten assisteren overeenkomstig artikel 48, § 3, van de wet van 18 juli 1991 houdende toezicht op de politie- en inlichtingendiensten, door twee experten te weten :

— Professor Yves Poullet, doctor in de rechten en directeur van het Centre de recherche informatique et droit des Facultés Universitaires Notre Dame de la Paix à Namur en lid van de Commissie ter bescherming van de persoonlijke levenssfeer;

evenals van zijn medewerker,

— Meester Jean-Marc Dinant, doctorandus in de informatica, schrijver van meerdere onderzoeksverslagen over het thema van de persoonlijke levenssfeer en de beveiliging van de persoonlijke gegevens op Internet.

2º om een tweede onderzoek te openen « over de wijze waarop de inlichtingendiensten deelgenomen hebben aan de ontdekking van een spionagezaak » en de dienst Enquêtes te belasten met dit tweede onderzoek (1).

Het contract bepaalde de opdracht van de experten en de eedaflegging volgens de formule van artikel 48, § 3, van de wet houdende toezicht op de politie- en inlichtingendiensten van 18 juli 1991. Het werd getekend door de experten en door de voorzitter van het Vast Comité I op 23 februari 2000.

De leden van het Comité I hebben de vergadering van de Commissie vrijheden en rechten van de burgers, Justitie en Binnenlandse Zaken van het Europees Parlement, die doorging op 22 en 23 februari 2000 te Brussel, bijgewoond. De heer Dinant heeft eveneens de vergadering van 23 februari 2000 bijgewoond tijdens dewelke de heer Duncam Campbell, schrijver van het rapport over het « Echelon-netwerk » werd gehoord.

De leden van het Comité I hebben mevrouw Godelieve Timmermans, administrateur-generaal a.i. van de Veiligheid van de Staat gehoord op donderdag 2 maart 2000. Deze heeft enkele preciseringen aangebracht aan haar verklaringen door middel van een brief van 6 maart 2000.

Op 3 maart 2000 ging het Comité I over tot het verhoor van generaal-majoor Michaux, chef van SGR.

De verslagen van deze verhoren werden opgenomen in het huidig rapport en werden opgesteld, rekening houdend met de bemerkingen die schriftelijk werden gemaakt door de verhoorde personen.

(1) Gezien de huidige stand van het onderzoek kan men reeds stellen dat noch de Veiligheid van de Staat noch SGR in de mogelijkheid zijn het bestaan van eender welk elektronisch bewakingssysteem te bevestigen dat aan de oorsprong zou liggen van de ontdekking van de strafbare activiteiten van majoor Bunel.

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

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

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

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

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

3. Quelques dernières manifestations de l'intérêt parlementaire concernant la problématique de l'existence d'un réseau «Échelon»

3.1. L'intérêt du Parlement européen

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

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

Le but des auditions prévues à cette occasion était de passer en revue les questions sensibles de la stratégie de l'Union européenne, qu'elle agisse dans le cadre de ses compétences communautaires et, en particulier celui de la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci (*JO* L 281 du 23 novembre 1995 p. 31) ou dans celui d'autres politiques et formes de coopération (IIe pilier: politique étrangère et de sécurité commune, IIIe pilier: coopération policière et judiciaire en matière pénale).

La réunion du mercredi 23 février était notamment consacrée aux «atteintes à la protection des données en dehors de la coopération judiciaire et policière: le

De experten aangewezen door het Comité I hebben hun verslag neergelegd op 7 maart 2000.

Op 9 maart 2000 werd een werkvergadering gehouden die het Comité I de gelegenheid bood een gedachtewisseling te hebben met de experten, de heren Poullet en Dinant.

Op 10 maart 2000 richtte de voorzitter van het Comité I een kantschrift aan het hoofd van de dienst Enquêtes vragende dat er met urgentie zou overgegaan worden tot het onderzoek betreffende «de arrestatie van de Franse majoor Bunel, teneinde na te gaan of de elementen die geleid hebben tot zijn arrestatie afkomstig waren van een elektronisch bewakingssysteem» (zie hierboven).

Dezelfde dag werd deze enquête genotifieerd door het hoofd van de dienst Enquêtes aan de ministers van Justitie en Landsverdediging overeenkomstig artikel 43, eerste lid, van de wet van 18 juli 1991.

Huidig rapport werd goedgekeurd door het Comité I op 13 maart 2000.

3. Enkele navolgende uitingen van de parlementaire belangstelling inzake de problematiek van het bestaan van een «Echelon-netwerk»

3.1. De belangstelling van het Europees Parlement

Het Verdrag van Amsterdam versterkte de verplichting van de Europese Unie om de bescherming van de persoonlijke gegevens in het kader van het fundamenteel recht op de bescherming van de persoonlijke levenssfeer te vrijwaren (artikel 8 van het Europees Verdrag voor de Rechten van de Mens zoals hernomen door artikel 6 van het Unie-Verdrag).

Op 22 en 23 februari 2000 vergaderden de commissie Vrijheden en Rechten van de burgers, Justitie en Binnenlandse Zaken van het Europees Parlement te Brussel over het thema «De Europese Unie en de bescherming van de gegevens».

Het doel van deze hoorzittingen die bij deze gelegenheid werden georganiseerd, was het overschouwen van de netelige kwesties van de strategie van de Europese Unie waar zij handelde enerzijds in het kader van haar gemeenschapsbevoegdheden en in het bijzonder van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en van de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, en anderzijds van andere politieke domeinen en vormen van samenwerking (IIe pijler: buitenlandse politiek en gemeenschappelijke veiligheid, IIIe pijler: politionele en gerechtelijke samenwerking in strafzaken).

De vergadering van woensdag 23 februari was in het bijzonder gewijd aan «inbreuken op de bescherming van de gegevens buiten de gerechtelijke en poli-

problème des interceptions des télécommunications (Échelon)». M. Duncan Campbell, auteur de l'étude commandée par le Parlement européen, y a présenté son rapport sur la problématique des interceptions des télécommunications et des conditions institutionnelles, politiques et opérationnelles qui les rendent possibles.

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

3.2. L'intérêt des parlementaires belges

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

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

3.3. L'intérêt de l'Assemblée Nationale française

Selon le compte rendu nº 27 de la commission de la Défense nationale et des Forces armées du mardi 29 février 2000 (http://www.assemblee-nationale.fr), son président Paul Quilès, après avoir fait référence au débat engagé dans plusieurs Parlements étrangers et au Parlement européen, ainsi que dans le public, sur le réseau dit «Échelon», a souligné qu'il appartenait à la Commission de la Défense de mener une enquête sur un système d'interception des communications dans le monde qui, en raison de son caractère d'organisation en réseau très étendu, de sa reconversion partielle vers l'espionnage industriel et de la participation d'un État membre de l'Union européenne, n'était pas sans poser de questions pour la sécurité du pays et la politique de défense, en particulier au moment où une politique européenne commune de sécurité et de défense était instituée.

Il a alors proposé la nomination d'un rapporteur d'information sur «les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale» en associant aux activités de ce

tionele samenwerking: het probleem van de intercepties van telecommunicaties (Echelon)». De heer Duncan Campbell, auteur van de door het Europees Parlement bevolen studie, stelde er zijn rapport voor inzake de intercepties van telecommunicaties en de institutionele, politieke en operationele voorwaarden.

Ingevolge de bespreking van dit rapport, hebben de vertegenwoordigers van de politieke groep van de «Groenen» van het Europees Parlement de procedurele stappen ondernomen om een onderzoekscommissie op te richten.

3.2. De belangstelling van de Belgische parlementsleden

Behalve de parlementaire initiatieven die aan de oorsprong liggen van de oorspronkelijke enquête over het Echelon-systeem, is het nuttig op te merken dat, sedert de recente onthullingen over het Echelonnetwerk in de media verschenen, het onderwerp in ons land aanleiding heeft gegeven tot een versterking van de belangstelling van de vertegenwoordigers van de natie voor dit onderwerp dat zowel gevoelig als zorgwekkend is in meerdere betekenissen.

De aanvulling van het onderzoek die het voorwerp is van huidig rapport, evenals de vragen gesteld door meerdere parlementsleden (zie *Beknopt Verslag* van de openbare vergadering van de Commissie voor de Buitenlandse betrekkingen van 22 februari 2000 — BV 50 — COM 130) zijn hiervan het voorbeeld.

3.3. De belangstelling van de Franse Assemblée Nationale

Volgens het verslag nr. 27 van de commissie Landsverdediging en Strijdkrachten van dinsdag 29 februari 2000 (ref. http://www.assemblee-nationale.fr/) onderlijnde voorzitter Paul Quilès, na verwezen te hebben naar het debat dat aangegaan werd in meerdere buitenlandse Parlementen en in het Europees Parlement alsook in het publiek aangaande het netwerk «Echelon» genaamd, dat het aan de Commissie Landsverdediging toekwam om een onderzoek in te stellen over een interceptiesysteem voor communicaties in de hele wereld die, ingevolge zijn zeer uitgestrekte netwerkstructuur, de gedeeltelijke omvorming naar industriële spionage en de deelname van een lidstaat van de Europese Unie, vragen oproept over de veiligheid van het land en zijn defensiepolitiek, in het bijzonder op het ogenblik waarop een gemeenschappelijk Europees beleid inzake veiligheid en defensie wordt ingesteld.

Hij heeft hierop de benoeming voorgesteld van een informatieverslaggever over «de elektronische bewakings- en interceptiesystemen die de nationale veiligheid in het gedrang kunnen brengen» en de activitei-

rapporteur un groupe de travail dans lequel chaque groupe politique désignerait un représentant.

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

3.4. L'intérêt du Congrès américain

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

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

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

3.5. L'intérêt du Parlement britannique

Outre les questions parlementaires citées dans le rapport des experts (*cf.* point 1.2 de leur rapport), le Comité permanent R a pris connaissance du rapport annuel de l'*« Intelligence and security committee »*(1) déposé par le premier ministre devant le Parlement britannique le 25 novembre 1999. Ce rapport indique les quatre priorités actuelles des services de renseignement du Royaume Uni, à savoir :

— le renseignement comme appui aux missions de maintien de la paix des Forces armées,

— la prolifération des armes de destruction massive,

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

ten van deze verslaggever te verbinden met een werkgroep waarvoor elke politieke groep een vertegenwoordiger zou aanwijzen.

Deze Commissie keurde, unaniem, dit voorstel goed en benoemde de heer Arthur Paecht als informatieverslaggever over « de elektronische bewakings- en interceptiesystemen die de nationale veiligheid kunnen in het gedrang brengen ».

3.4. De belangstelling van het Amerikaans Congres

In zijn rapport van 1999 wees het Comité I op een bepaling van de « Intelligence Authorisation Act for Fiscal Year 2000 » die de Director of Central intelligence, de Director of the National Security, en de Attorney General opdroeg om aan de parlementaire commissies, binnen de 60 dagen na afkondiging van deze wet, een rapport voor te leggen in twee versies (geclassificeerd en niet geclassificeerd) « describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance ».

Volgens de editie van 26 augustus 1999 van het Franse tijdschrift « *le Monde du Renseignement* » is deze bepaling de vertaling van de vrees van het Amerikaans Congres dat de grondwettelijke rechten van de Amerikaanse burgers zouden bedreigd zijn door het Echelon-netwerk.

Het Comité I heeft gepoogd de niet-geclassificeerde versie van dit rapport te verkrijgen. Vandaag is blijkbaar enkel de geclassificeerde versie neergelegd bij het Amerikaans Congres. Het Comité I heeft dus geen kennis kunnen nemen van dit niet-geclassificeerde document, maar het zal niet nalaten de evolutie van dit dossier bij het Amerikaans Congres op te volgen.

3.5. De belangstelling van het Britse Parlement

Behalve de parlementaire vragen vermeld in het expertenverslag (*cf.* punt 1.2 van hun verslag) heeft het Comité I kennis genomen van het jaarrapport van het « Intelligence and security committee »(1) dat door de eerste minister aan het Britse parlement werd voorgelegd op 25 november 1999. Dit verslag duidt vier actuele prioriteiten aan van de Britse inlichtingendiensten :

— inlichtingen als hulpmiddel bij de vredesmissies van de Strijdkrachten;

— de proliferatie van massa-vernietigingswapens;

(1) « The Intelligence and security » opgericht door de « the Intelligence Services Act 1994 » oefent de parlementaire controle uit over de Britse inlichtingendiensten; zie activiteitenverslag 1998 van het Comité I, blz. 2 tot 47).

— les attaques terroristes et la croissance du crime organisé,

— le rapport souligne également ... la menace croissante de l'espionnage économique.

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

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

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

4. Le point de la question sur les éventuelles initiatives entreprises par les services de renseignement depuis la clôture du rapport d'enquête précédent, le 5 août 1999

4.1. L'audition de Mme Timmermans, administrateur général a.i. de la Sûreté de l'État

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

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

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

— de terroristische aanslagen en de stijging van de georganiseerde criminaliteit;

— het rapport onderlijnt eveneens de toenemende bedreiging van de economische spionage.

Het «Committee» wijdt een hoofdstuk van zijn verslag aan de werking van het GCHQ (General Communication Headquarter), dat volgens het Campbell-rapport de operationele Britse dienst zou zijn die deelneemt aan het «Echelon-netwerk». Er wordt vermeld dat het GCHQ een belangrijke rol heeft gespeeld in de strijd tegen de georganiseerde criminaliteit en inlichtingen verschafte ter ondersteuning van de vredesmissies van de Strijdkrachten. Deze inlichtingen werden aan de regering, de geallieerde militaire commando's en de NATO verschaft. Het «Committee» roept op tot een grotere budgettaire gestrengheid vanwege de GCHQ.

Het is niet zonder belang aan te stippen dat inzake cryptografie, het «Committee» de wens van de regering goedkeurt om te legiferen inzake elektronische handel en cryptografie teneinde de produktie van sleutels die de ontcijfering van boodschappen kunnen toelaten, te kunnen bevelen.

Het rapport van het «Committee» (waarvan de presentatie van bepaalde passages aantoont dat zeker een deel van de inhoud niet publiek werd gemaakt) maakt geen enkele melding van het bestaan van een Echelon-systeem dat gericht zou zijn op economische spionage-operaties.

4. De stand van zaken over eventuele initiatieven die genomen zouden zijn door onze inlichtingendiensten na het afsluiten van het vorig onderzoeksverslag d.d. 5 augustus 1999

4.1. Het verhoor van mevrouw Timmermans, administrateur-generaal a.i. van de Veiligheid van de Staat

Op donderdag 2 maart 2000 hoorden de leden van het Comité I, mevrouw Timmermans, administrateur-generaal a.i. van de Veiligheid van de Staat. Deze bracht enige preciseringen aan aan haar verklaringen door haar schrijven van 6 maart 2000. Huidig verslag houdt rekening met deze preciseringen.

Het Comité I vroeg of sedert het indienen van het eerste rapport van het Comité I in 1999, de Veiligheid van de Staat gepoogd heeft om zich verder te informeren over het Echelon-systeem.

Mevrouw Timmermans antwoordt hierop negatief. Zij kan enkel bevestigen wat de vorige administrateur-generaal van de Veiligheid van de Staat verklaarde tegenover het Comité I ten tijde van het eerste onderzoek, zijnde:

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

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

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

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

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

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

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

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

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

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

— dat de Veiligheid van de Staat het bestaan van het systeem « Echelon » enkel kende door middel van diverse persartikelen. Enkele informele pogingen die zij sedertdien ondernomen had bij haar buitenlandse correspondenten, hadden geen resultaat opgeleverd;

— dat de bescherming van het economisch en wetenschappelijk potentieel, zijnde het vermoedelijk doelwit van het systeem « Echelon », toen niet behoorde tot de opdrachten van de Veiligheid van de Staat;

— dat de dienst zowel qua personeel als wat materieel betreft, onvoldoende middelen had teneinde de werkelijkheid van het bestaan van het Echelon-systeem na te gaan; geen enkel agent van de Veiligheid van de Staat beschikt over dergelijke technische bekwaamheden om deze bedreiging te analyseren;

— dat de Veiligheid van de Staat niet overgaat tot het inwinnen van inlichtingen door middel van sattelieten en dat zij geen enkele toegang had tot dit type van informatiebron;

— dat de Veiligheid van de Staat trouwens geen enkele wettelijke mogelijkheid had om over te gaan tot interceptie van communicaties en het afluisteren via satellieten; deze situatie was trouwens nadelig voor de Veiligheid van de Staat in haar betrekkingen met buitenlandse diensten die wel over dergelijke mogelijkheden beschikken;

— dat het bestaan van het « Echelon »-systeem dus voor de Veiligheid van de Staat onmogelijk aan te tonen was;

— behoudens de mededeling van voornoemde elementen aan de minister van Justitie om deze toe te laten op parlementaire interpellaties te antwoorden, heeft de Veiligheid van de Staat nooit enig rapport of nota over het Echelon-systeem opgesteld.

Mevrouw Timmermans heeft eveneens bevestigd dat de Veiligheid van de Staat nooit voorheen enige discussie met de Algemene Dienst Inlichtingen en Veiligheid van de Strijdkrachten en evenmin trouwens met enig andere Europese inlichtingendienst heeft gehad. Mevrouw Timmermans verbindt er zich evenwel toe, gelet op de recente ontwikkelingen inzake Echelon, om de buitenlandse correspondenten te bevragen inzake het bestaan van het Echelon-systeem.

Wat de economische doelwitten betreft die door het Echelon-systeem geviseerd zouden zijn, verduidelijkt mevrouw Timmermans dat haar dienst nog geen instructies ontving van het ministerieel Comité voor de Inlichtingen inzake de bescherming van het wetenschappelijk en economisch potentieel.

De Veiligheid van de Staat zal voorstellen formuleren en voorleggen aan het ministerieel Comité voor de Inlichtingen.

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

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

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

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

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

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

4.2. L'audition du général-major Michaux, chef du SGR

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

Momenteel, werken slechts twee agenten op dit onderwerp binnen de Veiligheid van de Staat.

Deze materie blijkt trouwens enkel de bescherming van de strikt nationale belangen te betreffen. Volgens mevrouw Timmermans bestaat er dus geen enkele informatie-uitwisseling van welke aard dan ook tussen Europese inlichtingendiensten waar de «cloisonnering» regel blijft in dit domein.

Ondervraagd over de eventuele kennis van de Veiligheid van de Staat over het bestaan van «Opidium», verklaart mevrouw Timmermans dat er haar niets meer bekend is dan wat de open bronnen hierover vermelden. Zij meent bovendien dat het bestaan van een dergelijk systeem moet beschouwd worden als een antwoord op de Amerikaanse praktijken.

Mevrouw Timmermans verklaarde eveneens dat, in tegenstelling tot SGR, de Veiligheid van de Staat geen enkele technische of wettelijke bevoegdheid heeft om zich in te laten met problemen van de veiligheid van communicaties.

Ondervraagd over de mogelijkheid om in de toekomst onderzoeksmiddelen zoals het gemeenschappelijk exploiteren van open bronnen met SGR of het beroep doen op experten inzake bijzondere opdrachten, maakt mevrouw Timmermans enig voorbehoud. Wat de experten aangaat bestaat het enig alternatief dat openstaat voor de Veiligheid van de Staat er in, hetzij het recruteren van nieuwe statutaire agenten, hetzij het aanwerven van contractuele agenten van niveau 1. Maar, de aanwervingen zijn steeds onderworpen aan budgettaire beperkingen en meer bepaald aan het advies van de inspecteur van Financiën: een uitbreiding van 25 éénheden voor de buitendiensten, gevraagd in het kader van de budgettaire controle, werd recent verworpen.

Wat de ILETS-ontmoetingen (International Law Enforcement Telecommunications Seminar) aangaat waarvan eveneens sprake is in het STOA-rapport, bevestigt mevrouw Timmermans dat een afdelingscommissaris van de Veiligheid van de Staat wel degelijk deelgenomen heeft aan enkele van deze vergaderingen die sedert 1997 op initiatief van het Amerikaanse FBI werden georganiseerd. Namen eveneens deel aan deze vergaderingen, vertegenwoordigers van de rijkswacht, van de APSD, evenals een vertegenwoordiger van het kabinet van de minister van Justitie. Het voorwerp van deze ontmoetingen was de harmonisatie van de standaarden inzake intercepties in Europa en Amerika.

4.2. Het verhoor van generaal-majoor Michaux, chef van SGR

De leden van het Comité I hebben generaal-majoor Michaux, chef van SGR, verhoord op vrijdag 3 maart 2000.

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

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

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

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

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

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

Le SGR a également pris l'initiative de porter le sujet de la sécurité informatique et de la cryptologie à l'ordre du jour du Collège du renseignement et de la sécurité.

Ce collège a désigné des experts chargés de déposer un rapport au Comité ministériel du renseignement et de la sécurité.

Le SGR a formulé aux membres du Collège du renseignement et de la sécurité la proposition de créer une agence fédérale pour la protection de l'information, chargée de la politique du chiffrement en Belgique.

Cette proposition est encore à l'étude à ce jour.

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

De voorzitter van het Comité I vraagt aan generaal Michaux of, sedert het indienen van het rapport van het Comité I in 1999, SGR getracht heeft om zich verder te informeren over dit onderwerp.

Generaal Michaux antwoordt dat SGR het Echelon-systeem niet volgt. De dreiging die uitgaat van Echelon situeert zich voornamelijk op het niveau van de economische, politieke en juridische orde, materies die buiten de bevoegdheden van SGR vallen. Zou het gaan om een militair spionagesysteem, wat wel degelijk de bevoegdheid is van SGR, dan verleent deze dienst geen prioriteit aan de spionage uitgaande van geallieerden van België. In deze materie blijven andere landen veel meer bedreigender activiteiten te vertonen voor de Belgische militaire belangen.

SGR beschikt niet over technische of menselijke middelen die noodzakelijk zijn om het bestaan van het Echelon-netwerk te ontleden. Volgens generaal Michaux zou het volgen van een technisch systeem zoals « Echelon » trouwens illegaal zijn in België, gelet op het ontbreken in dit land van een wetgeving inzake veiligheidsintercepties.

Dit betekent niet dat SGR in deze materie inactief gebleven is.

SGR werkt vanuit de veronderstelling dat intercepties van communicaties wel degelijk bestaan en ongeacht het land dat ze uitvoert men er zich tegen moet weren. SGR meent eveneens dat eender welk informatica-vercijfering vatbaar is om verbroken te worden.

Als verantwoordelijke voor de veiligheid van de communicaties van de Strijdkrachten, heeft SGR verschillende regels uitgewerkt met als doel het vrijwaren van de vertrouwelijkheid van geclassificeerde gegevens die door telecommunicatie of informaticanetwerken worden verzonden of behandeld.

SGR heeft eveneens het initiatief genomen om het onderwerp van de informaticaveiligheid en de cryptologie aan de orde te brengen in het College van de inlichtingen en veiligheid.

Dit college heeft deskundigen aangewezen om een rapport neer te leggen aan het ministerieel Comité voor de inlichtingen en de veiligheid.

SGR heeft aan de leden van het College voor inlichtingen en veiligheid het voorstel gedaan om een federaal agentschap voor de bescherming van de informatie op te richten dat gelast zou worden met de vercijferingspolitiek in België.

Dit voorstel is nog steeds ter studie.

Wat hen betreft is SGR de idee genegen om een federaal agentschap op te richten voor de bescherming van de informatie hetzij om een bestaand organisme te gelasten met dit beleid inzake vercijfering in België. België heeft trouwens eminente specialisten in de cryptografie.

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

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

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

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

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

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

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

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

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

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

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

À ce propos, le général Michaux souligne le caractère peu attractif du statut financier offert aux informaticiens des Forces armées et à ceux de la fonction

SGR volgt van zeer nabij de ontwikkeling van de wetgeving inzake cryptografie in België. Het probleem van de cryptografie is evenwel zeer complex, gezien het zich situeert op het kruispunt van verschillende uiteenlopende belangen :

— de economische belangen die op het spel staan zijn enorm, om zich te ontwikkelen moet de Internethandel noodzakelijk veilig zijn, het heeft dus nood aan een sterk vercijferingssysteem;

— criminele organisaties gebruiken eveneens overvloedig internet ook zij hebben nood aan een sterk vercijferingssysteem;

— verschillende ondernemingen ontwikkelen cryptografische systemen die zij vrij op de markt willen brengen;

— daarentegen hebben politie- en inlichtingendiensten geen belang aan de verspreiding van sterke vercijferingssystemen.

Deze uiteenlopende belangen geven in de VS aanleiding tot hevige gevechten om invloed tussen de NSA en de lobby van internetgebruikers.

Het Comité I vraagt eveneens aan generaal Michaux of SGR de Echelonbedreiging als plausibel beschouwd en of hij kennis heeft van het bestaan van andere buitenlandse (Russische, Franse, Zwitserse, ...) afluisternetwerken.

Generaal Michaux antwoordt dat hij geen andere kennis heeft van interceptienetwerken dan door open bronnen waarin men informatie terugvindt maar ook desinformatie. SGR beschouwt de bedreiging komende van grote landen als plausibel en past dus het principe van de voorzorg toe.

De voorzitter vraagt of er informatie uitgewisseld tussen SGR en de Veiligheid van de Staat en, op een meer algemene wijze, tussen de Europese inlichtingendiensten inzake Echelon of enig ander onderwerp van economische spionage.

Generaal Michaux antwoordt dat er geen informatie-oorlog bestaat tussen de twee Belgische inlichtingendiensten. Alles wat SGR verneemt en dat interessant is voor de Veiligheid van de Staat, wordt aan deze dienst doorgezonden.

Vooraleer het voorstel te doen tot de oprichting van een federaal agentschap ter bescherming van de informatie aan het College van inlichtingen en veiligheid, heeft de voorganger van de huidige chef van SGR hierover gesproken met de administrateur-generaal van de Veiligheid van de Staat. Tussen informatici van beide diensten vonden periodieke vergaderingen plaats.

Wat dit betreft onderlijnt generaal Michaux het weinig aantrekkelijk karakter van het financieel statuut dat geboden wordt aan informatici van de

publique en général. Les salaires offerts par les firmes privées sont bien plus avantageux et certains informaticiens quittent les Forces armées pour des motifs financiers évidents. La mise en place du système informatique du SGR en subit les conséquences.

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

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

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

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

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

5. Le rapport des experts désignés par le Comité permanent R

Le Comité a estimé, vu l'ampleur de la problématique posée par le réseau «Échelon» et l'urgence d'en poursuivre une approche dynamique, de ne pas se contenter d'élaborer une synthèse des informations

Strijdkrachten en van de openbare dienst in het algemeen. De salarissen die aangeboden worden door private ondernemingen zijn veel voordeliger en bepaalde informatici verlaten de Strijdkrachten om evidente financiële motieven. De uitbouw van een informaticasysteem van SGR ondervindt hiervan trouwens de gevolgen.

Generaal Michaux signaleert anderzijds dat sedert de werken van de Ruanda-commissie, SGR zijn bilaterale verhoudingen met andere militaire of externe diensten van Europese landen heeft aangehaald, deze diensten gaan over tot regelmatige uitwisseling van gemeenschappelijke belangstellingspunten, maar er wordt nooit gesproken over economische spionage. Natuurlijk wordt niet alles uitgewisseld, men houdt sommige gegevens voor zich in functie van de eigen nationale belangen. Een regel is ook dat men niets zegt over zijn contacten met derde diensten. Indien het niet makkelijk is om een Europees leger op te bouwen, dan zal het nog moeilijker zijn om een gemeenschappelijke Europese inlichtingendienst op te richten.

Tenslotte moet men betreuren dat, uitgezonderd de wapensector verbonden aan Landsverdediging, de andere Belgische ondernemingen zeer weinig gevoelig zijn voor economische intelligence.

Generaal Michaux kent niemand die door zijn beroep of door zijn voormalig toebehoren aan een inlichtingendienst een directe persoonlijke kennis zou verworven hebben van het Echelon-systeem. Men moet zich trouwens hoeden voor «onthullingen» van de zogenaamde gewezen leden van de inlichtingendiensten die de pers halen. Het is gepast om steeds de verklaringen te onderzoeken in het licht van de omstandigheden die het vertrek van deze personen bij hun dienst hebben voorafgegaan.

Ondervraagd over de ILETS-ontmoetingen, verklaart generaal Michaux dat SGR niet aan deze vergaderingen deelneemt.

De voorzitter vraagt of SGR overweegt om beroep te doen op externe specialisten of deskundigen voor materies waar deze niet beschikt over bevoegd personeel. Generaal Michaux antwoordt dat SGR hieraan reeds gedacht heeft en deze mogelijkheid overweegt voor punctuele samenwerkingen. In afwachting, heeft SGR recent nieuwe analisten aangeworven die momenteel gevormd worden. Ook levert SGR momenteel een bijzondere inspanning om deze analisten te vormen.

5. Het rapport van de deskundigen aangewezen door het Vast Comité I

Het Comité I heeft geoordeeld, gelet op de omvang van het gestelde probleem van het Echelon-netwerk en de dringendheid om er een dynamische benadering aan te kunnen geven, om zich niet te vergenoegen met

les plus récentes parues dans ce domaine dans les sources ouvertes de diverses origines, mais de demander à des experts d'en faire une analyse critique permettant entre autres de faire la distinction entre information et désinformation, et de préciser sur des bases objectives la probabilité d'une menace globale dont le système « Échelon » ne serait qu'une manifestation exemplative.

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

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

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

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

LE RÉSEAU ÉCHELON

Existe-t-il ?

Que peut-il faire ?

Peut-on et doit-on s'en protéger ?

Rapport d'expertise rédigé à l'attention du Comité permanent de contrôle des services de renseignements le 7 mars 2000

Par Yves Poullet (yves.poullet@ofundp.ac.be), docteur en droit, professeur et directeur du Centre de recherche informatique et droit (FUNDP) et Jean-Marc Dinant (jmdinant@ofundp.ac.be), maître et doctorant en informatique chargé de recherche au Centre de recherche informatique et droit de l'université de Namur

een synthese van informaties die hierover recent verschenen in open bronnen van diverse origines, maar aan deskundigen te vragen om er een kritische analyse van te maken die toelaat onder andere een onderscheid te maken tussen informatie en desinformatie en de waarschijnlijkheid te preciseren op objectieve basis van de globale bedreiging, waarvan het Echelon-systeem slechts een voorbeeld zou zijn.

Getroffen door de problemen waarmee onze inlichtingendiensten geconfronteerd worden en om te pogen alternatieve oplossingen voor te stellen voor het gebrek aan middelen waarmee ze te maken hebben, wenste het Comité I eveneens in praktijk de mogelijkheid om beroep te doen op deskundigen uit de universitaire wereld, duidelijk te maken.

Zoals hierboven aangehaald heeft het Comité I zijn initiatief gebaseerd op enerzijds de mogelijkheden die het gegeven worden door de wet houdende het toezicht op de politie- en inlichtingendiensten van 18 juli 1991, artikel 48, § 3, om beroep te doen op deskundigen en anderzijds op zijn dubbele controle-opdracht van de coördinatie en de doelmatigheid van de veiligheids- en inlichtingendiensten enerzijds en anderzijds de bescherming van de rechten die de Grondwet en de wet aan personen verlenen.

Het Comité I vroeg eveneens aan de deskundigen om aanbevelingen op te stellen die toelaten om middelen en te nemen maatregelen aan te duiden om aan dit type bedreiging een antwoord te bieden.

De opdrachten die het Comité I aan de deskundigen verleenden worden hernomen in het corpus van het verslag dat op 7 maart 2000 werd neergelegd en waarvan de inhoud hierna integraal wordt weergegeven.

HET ECHELON-NETWERK

Bestaat het ?

Waartoe is het in staat ?

Kan men en moet men zich ertegen beschermen ?

Expertiseverslag ter attentie van het Vast Comité van toezicht op de Inlichtingendiensten 7 maart 2000

Door Yves Poullet (yves.poullet@fundp.ac.be), doctor in de rechten professor en directeur van het Centre de recherche informatique et droit (FUNDP) Jean-Marc Dinant (jmdinant@ofundp.ac.be), meester en doctorandus in de informatica belast met een onderzoeksopdracht in het Centre de recherche informatique et droit van de universiteit van Namen

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

INTRODUCTION

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

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

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

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

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

5. décrire l'environnement juridique en la matière;

6. formuler, le cas échéant, des recommandations.

Le présent rapport reprend ces différents points, en tire les conclusions et formule certaines recommandations. Les auteurs tiennent à souligner que ce document a dû être rédigé dans des délais extrêmement brefs.

Les éléments décrits dans ce rapport l'ont néanmoins été avec toute la rigueur scientifique possible mais certaines analyses n'ont pu être menées de manière aussi approfondie qu'il eût fallu. C'est en particulier le cas pour l'analyse de l'importance et de la nature des télécommunications potentiellement vulnérables à l'interception par le réseau Échelon.

1. ANALYSE DES DOCUMENTS ISSUS DE SOURCES OUVERTES

1.1. Les rapports du STOA

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

— les travaux de Duncan Campbell menés dans les années 70;

— le livre « the Puzzle Palace » de James Bamford;

De opstellers geven in dit verslag hun persoonlijke mening en verbinden geen enkele instelling.

INLEIDING

Op 23 februari 2000 belastte het Vast Comité van toezicht op de Inlichtingendiensten de ondertekenende experten met de volgende opdrachten :

1. onderzoeken, analyseren en becommentariëren van alle beschikbare documenten, afkomstig van open bronnen, die handelen over het bestaan van het Echelon-netwerk dat tot doel heeft communicatie te intercepteren, onder andere met economische bedoelingen;

2. evalueren van de betrouwbaarheid van deze documenten en van de aannemelijkheid van deze hypotheses, door ze te confronteren met de mening van telecommunicatie-operatoren;

3. het mogelijk bestaan van het Echelon-netwerk situeren in een ruimere context van internationaal gebruik van bewakingstechnologieën;

4. in de mate van het mogelijke, de gebruikte technologieën beschrijven en de aard van de geïntercepteerde berichten preciseren;

5. de juridische omgeving terzake beschrijven;

6. eventueel aanbevelingen formuleren.

In hun verslag behandelen de auteurs deze punten, ze trekken de nodige conclusies en formuleren een aantal aanbevelingen. Ze benadrukken echter dat ze over heel weinig tijd beschikten om hun rapport op te stellen.

Niettemin hebben ze alle elementen met een zo groot mogelijke wetenschappelijke nauwkeurigheid beschreven, al konden ze bepaalde zaken niet grondig genoeg analyseren. Dit geldt in het bijzonder met betrekking tot het belang en de aard van telecommunicatie die eventueel kwetsbaar kan zijn in geval van interceptie door Echelon.

1. ANALYSE VAN DE DOCUMENTEN AFKOMSTIG VAN OPEN BRONNEN

1.1. De STOA-rapporten

Het eerste STOA-rapport verscheen in 1998 en bracht toen al heel wat reactie teweeg, waaronder een aanbeveling van het Europees Parlement. Slechts twee pagina's van dit eerste rapport besteden aandacht aan Echelon, op grond van drie afzonderlijke bronnen :

— de werkzaamheden van Duncan Campbell in de jaren zeventig;

— het boek « The Puzzle Palace » van James Bamford;

— le livre «the Secret Power» de Nicky Hager.

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

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

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

Cette recommandation confirme l'existence de ce document classifié.

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

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

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

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

(3) JO C329 du 14 novembre 1996.

— het boek «The Secret Power» van Nicky Hager.

Dit laatste boek bevat de beste beschrijving van Echelon. Het somt de basissen van het netwerk overal ter wereld op en legt uit dat Echelon de Intelsat-satellieten bespioneert die worden gebruikt bij het versturen van de meerderheid van het mondiale telefoon-, fax-, telex- en internetverkeer (inclusief e-mail) dat per satelliet verloopt.

Hoewel dit vaak in de pers wordt beweerd, is het niet juist dat dit netwerk al het Europese telefoonverkeer kan afluisteren. Echelon zou vooral de berichten kunnen onderscheppen die via de Intelsat-satellieten worden verstuurd.

Dit eerste rapport maakt gewag van een document d.d. 25 oktober 1995 dat nog steeds geheim zou zijn. Op 8 mei 1999 formuleerde de werkgroep-29(1) een aanbeveling over de eerbied voor de persoonlijke levenssfeer bij het intercepteren van telecommunicatie(2).

Deze aanbeveling bevestigt het bestaan van dit geclassificeerd document.

«De werkgroep maakt zich ook zorgen over het toepassingsgebied van de maatregelen beschreven in de resolutie van de Raad d.d. 17 januari 1995(3). Een niet-gepubliceerde versie van het bovengenoemde document, die recenter is dan deze versie van het document (d.d. 25 oktober 1995), bepaalt dat de ondertekenaars van de tekst met betrekking tot de specificaties inzake het intercepteren van telecommunicatie contact kunnen opnemen met de directeur van het Federal Bureau of Investigation in de Verenigde Staten. Voorts staat in deze tekst dat andere staten, op voorwaarde dat de «deelnemers» daarmee akkoord gaan, kunnen deelnemen aan het uitwisselen van informatie, aan het herzien en bijwerken van de specificaties. De groep is verontrust over het feit dat technische maatregelen voor het intercepteren van telecommunicatie worden ontwikkeld in overleg met staten die niet onderworpen zijn aan de voorwaarden van het Europees Verdrag voor de rechten van de mens en van de richtlijnen 95/46 en 97/66.»

Het tweede STOA-rapport verscheen begin 2000. Het bevat meer details en is in twee stukken ingedeeld.

(1) Hierna Groep-29 genoemd. Deze groep is opgericht krachtens artikel 29 van de Richtlijn 95/46 en groepeert alle nationale commissies ter bescherming van gegevens in de Europese Unie.

(2) Beschikbaar op de server van de Europese Unie: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp18fr.pdf

(3) *Publicatieblad* C329 d.d. 14 novembre 1996.

La première partie, assez technique, présente quatre études :

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

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

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

— La perception des risques économiques dérivés de la vulnérabilité potentielle des médias commerciaux par rapport aux interceptions (cabinet d'études Zeus, entouré de l'avis de 49 experts en technologies de la télécommunication).

La deuxième partie, plus juridique, analyse la protection des données et les droits de l'homme dans l'Union européenne et le rôle du parlement européen. Au niveau technique, les éléments décrits dans la première partie sont exposés avec soin et précision et l'ensemble du travail a été réalisé de manière professionnelle.

Suite à l'audition par le Parlement européen de l'auteur Duncan Campbell, aucune critique sérieuse de ce rapport n'a d'ailleurs été formulée, même si l'auteur est en défaut d'apporter des preuves formelles de tous les éléments de son rapport. Certains éléments de son rapport sont d'ailleurs basés sur des coupures de presse.

En dehors de ce rapport, d'autres éléments apportent des preuves de l'existence du réseau Échelon.

1.2. Les questions parlementaires au Royaume-Uni

L'existence de la base anglaise de Menwith Hill, considérée comme le nœd du réseau Échelon au cœur de l'Europe, peut être établie par plusieurs questions parlementaires à la Chambre des Lords du Royaume-Uni, telles que publiées sur le site officiel du Parlement britannique (1).

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

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

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

Het eerste deel is vrij technisch en stelt vier studies voor :

— *Electronic surveillance* (Duncan Campbell).

— *Encoding, encryption systems and electronic surveillance* (F. Leprévost, hoogleraar aan de Technische Universiteit van Berlijn).

— *Legality of the interception of communications* (Chris Elliott, jurist en ingenieur gespecialiseerd in telecommunicatie).

— *Economic risks linked to the vulnerability of communications* (Studiebureau « Zeus », met het advies van 49 experten op het gebied van telecommunicatietechnologieën).

Deel twee van het rapport is eerder juridisch en analyseert de bescherming van de gegevens en de rechten van de mens binnen de Europese Unie en de rol van het Europees Parlement. Technisch gezien worden de elementen in het eerste deel zorgvuldig en nauwkeurig beschreven en is het hele onderzoek met grote deskundigheid gevoerd.

Het Europees Parlement heeft de auteur van de studie, Duncan Campbell, gehoord en formuleerde daarna geen enkele ernstige kritiek op zijn rapport, ook al kon de auteur geen formele bewijzen aanbrengen voor al de elementen in zijn rapport. Sommige van die elementen waren trouwens gebaseerd op krantenknipsels.

Buiten dit rapport leveren nog andere elementen bewijzen van het bestaan van Echelon.

1.2. Parlementaire vragen in het Verenigd Koninkrijk

Het bestaan van de Engelse basis in Menwith Hill, die wordt beschouwd als het Europese knooppunt van het netwerk Echelon, kan worden aangetoond op grond van diverse parlementaire vragen die werden gesteld in het Hogerhuis van het Verenigd Koninkrijk en die zijn gepubliceerd op de officiële website van het Britse parlement (1).

U vindt hieronder de vertaling van een aantal vragen en het antwoord daarop :

29 maart 1994, Brian Sedgemore : « Mijn geachte collega had het over de basis van Menwith Hill. Ik geloof dat het gaat om een GCHQ-station. Kan mijn geachte collega verklaren waarom de Britse spoorwegen het willen belasten op grond van zijn belastbare waarde? »

(1) De originele vragen en antwoorden in het Engels zijn het voorwerp van de bijlage (afgedrukt zoals gevonden op Internet).

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

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

Réponse: « ...Comme la Chambre le sait, j'ai visité la station le 27 janvier. J'ai reçu des briefings concernant son rôle actuel de la part du personnel senior américain et anglais travaillant là-bas, celui-ci incluant le chef de la base...

Le travail effectué là-bas est très sensible et classifié secret. Je crois très fermement que si je commentais en détail les activités que j'ai vu menées là-bas, cela ne serait pas dans l'intérêt national et nuirait en tout cas à l'objectif véritable de ce travail...

Il y a actuellement 600 employés britanniques servant à chaque niveau de la base et 1 200 employés américains. L'honorable membre pour Bradford Sud a mentionné des visites de Menwith Hill par des membres du Parlement et des membres du Parlement européen.

Des demandes antérieures pour de telles visites ou conférences n'ont pas été approuvées sur base des dérangements [que cela causerait] dans le fonctionnement opérationnel de la base et pour des raisons de sécurité. J'ai déclaré qu'il en serait de même tant pour les membres du parti conservateur que pour les membres du parti travailliste.

Il n'entre pas dans la pratique du ministère de la Défense d'organiser des visites guidées des installations de travail de Menwith Hill. Dans ma réponse à la Chambre le 8 mars, j'ai dit que ces restrictions s'appliqueraient à tous [les parlementaires].»

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

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

Le 6 avril 1998, Norman Baker: «Quel mécanisme est en place pour garantir que l'information glanée

Antwoord: «(...) Menwith Hill is een afluister- en spionagebasis... op een terrein van 125 ha met 21 radarkoepels».

25 maart 1994, de heer Cryer: «Welke rechten hebben personen en ondernemingen die menen dat ze door Menwith Hill worden bespioneerd? Kan de minister ons bijvoorbeeld formeel verzekeren dat Menwith Hill geen communicatie inzake handelsverkeer onderschept? ... En indien de minister zoveel vertrouwen heeft in de democratie, zal hij dan toelaten dat ikzelf en andere leden van Labour een bezoek brengen aan de basis?»

Antwoord: «Dit Huis weet dat ik op 27 januari een bezoek heb gebracht aan de basis. Amerikaanse en Engelse officieren, waaronder het hoofd van de basis, hebben me uitgelegd wat de huidige rol van deze basis is...

Het werk dat er wordt verricht is bijzonder gevoelig en kreeg de classificatie «geheim». Ik geloof stellig dat ik het nationaal belang niet dien door een gedetailleerde beschrijving te geven van de activiteiten die ik er heb gezien. In elk geval zou ik daarmee schade berokkenen aan de nationale belangen en aan het werkelijke doel van deze werkzaamheden...

Momenteel werken er 600 Britten en 1 200 Amerikanen, alle niveaus bijeengenomen. De geachte collega voor Zuid-Bradford verklaarde dat leden van het parlement en van het Europees Parlement Menwith Hill hebben bezocht.

Vroegere aanvragen voor dergelijke bezoeken of conferenties werden niet goedgekeurd omdat dit de operationele werking van de basis zou verstoren, alsook uit veiligheidsoverwegingen. Ik heb verklaard dat dit zou gelden voor de leden van de conservatieve partij en van Labour.

Het ministerie van Landsverdediging heeft niet de gewoonte rondleidingen van de installaties in Menwith Hill te organiseren. In mijn antwoord aan het Huis op 8 maart heb ik gezegd dat deze beperkingen golden voor alle parlementsleden.»

3 juni 1996, Lord Jenkins uit Putney: «Intercepteert het Amerikaanse National Security Agency (NSA) telecommunicatie in Menwith Hill? Zo ja, welk soort berichten intercepteert het en met welke bedoeling?»

Antwoord: «Het beleid van de regering voorziet niet dat ze gedetailleerde uitleg verstrekt over de operaties die in Menwith Hill plaatsvinden. In elk geval wordt (of zou) op deze basis geen enkele activiteit (worden) toegelaten die als nadelig wordt beschouwd voor de Britse belangen.»

6 april 1998, Norman Baker: «Hoe garandeert men dat de informatie verkregen door het intercepteren

des interceptions des télécommunications par les forces américaines à Menwith Hill n'est pas utilisée de manière préjudiciable aux intérêts du Royaume-Uni ? »

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

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

Réponse de John Reid, ministre des Forces armées : « L'honorable gentleman ne devrait pas s'attendre à ce que ce que je commente un rapport que je n'ai jamais vu et dont je n'ai entendu que très peu de garanties eu égard à sa véracité. Menwith Hill est une installation de communications et il y a là-bas une intégration totale entre le personnel américain et anglais.

En cette matière, il y a un droit de regard par le parlement mais aussi par le biais du comité « Intelligence and Security » et notamment par l'honorable gentleman. Parmi les milliers de questions qu'il a déposées depuis qu'il est entré au Parlement — à 600 livres par question —, plus d'une vingtaine sur ce sujet ont déjà reçu mon attention personnelle. »

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

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

Question : « S'ils [les ministres concernés] surveillent les activités qu'ils permettent aux États-Unis de mener à Menwith Hill, y compris les activités de maintien de l'ordre menées par le personnel américain afin de s'assurer qu'elles ne compromettent pas les

van telecommunicatie door de Amerikaanse troepen in Menwith Hill niet wordt gebruikt op een manier die de belangen van het Verenigd Koninkrijk schaadt? »

Antwoord van de minister van Landsverdediging : « Op elk niveau in Menwith Hill maken Engelsen deel uit van het personeel. Bijgevolg kunnen we er vertrouwen in hebben dat op deze basis geen activiteiten plaatsvinden die nadelig zijn voor de belangen van het Verenigd Koninkrijk. »

De heer Baker : « Kan de minister [van Landsverdediging] de waarheid of andere aspecten bevestigen van de elementen in het rapport « Assessing the Technologies of Policitical Control » dat voor het Europees Parlement wordt voorbereid en dat suggereert dat alle communicatie per telefoon, fax en e-mail in heel Europa wordt bewaakt door de Amerikaanse troepen in Menwith Hill ? Mogen we redelijkerwijze aannemen, rekening houdend met het feit dat een dergelijke activiteit tegen grote snelheid verloopt en de Koude Oorlog voorbij is, dat het doel van deze intercepties niet militair is ? Kan de minister bevestigen dat de Engelse regering toegang heeft tot alle intercepties in Menwith Hill ? Indien hij dat niet kan, hoe kan hij dan de bovenstaande verzekering geven? »

Antwoord van John Reid, minister van Landsverdediging : « Mijn geachte collega kan niet verwachten dat ik commentaar geef op een rapport dat ik nooit heb gezien en waarvan ik slechts weinig waarborgen heb gekregen met betrekking tot de waarheid van zijn inhoud. Menwith Hill is een communicatiebasis met volledige integratie van het Amerikaanse en Engelse personeel.

In verband hiermee heeft het parlement recht van controle, ook via het comité « Intelligence and Security » en in het bijzonder door mijn geachte collega. Van de duizenden vragen die hij heeft neergelegd sinds hij lid is geworden van het Parlement — voor een bedrag van 600 per vraag — heb ik persoonlijk aandacht besteed aan een twintigtal ».

9 maart 1999, Lord Kennet : « Wanneer heeft een minister voor het laatst een bezoek gebracht aan Menwith Hill, de Amerikaanse basis in het Verenigd Koninkrijk ? Hoelang is hij er gebleven ? Kon hij alle activiteiten observeren die het Amerikaanse personeel er verricht en heeft hij deze activiteiten begrepen? »

Antwoord : « Sinds 1 mei 1997 heeft geen enkele minister van deze regering nog een bezoek gebracht aan Menwith Hill. De betrokken ministers worden echter op de hoogte gehouden van alle activiteiten die er plaatsvinden. »

Vraag : « Indien ze [de betrokken ministers] toezicht houden op de activiteiten waarvoor ze aan de Verenigde Staten de toelating geven ze in Menwith Hill te verrichten, met inbegrip van activiteiten inzake het bewaren van de orde door het Amerikaanse perso-

droits et intérêts, commerciaux, sociaux ou autres, des citoyens et entreprises du Royaume-Uni et de l'Union européenne.»

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

1.3. Les documents déclassifiés par la NSA

Le rapport STOA fait état de documents déclassifiés sur base du «Freedom of Information Act»(1). La lecture de ces documents (dont certaines parties sont illisibles ou censurées) reste sibylline mais le nom «Échelon» y apparaît et ces documents confirment donc l'existence de ce réseau même s'ils n'apportent que peu de renseignements relatifs à son fonctionnement.

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

2.1. Quelques éléments concernant la National Security Agency

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

— «la menace par rapport à nos systèmes d'information grandira dans les années futures au fur et à mesure que les technologies permettant l'attaque de ces systèmes prolifèreront et que de plus en plus de pays et de groupes développeront des stratégies incluant de telles attaques»(2);

— «Ces pages décrivent le plan stratégique de la NSA/(CSS) pour le XXI^{e} siècle et comment nous comptons atteindre notre but: la supériorité américaine en matière d'information»(3).

Selon plusieurs sources convergentes, la NSA posséderait un personnel d'environ quarante mille personnes et un budget de l'équivalent de 160 milliards de francs belges en 1997. À titre de comparaison, un géant industriel comme Belgacom a dépensé

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

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

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

neel, teneinde zich ervan te vergewissen dat ze de rechten en de commerciële, maatschappelijke of andere belangen van de burgers en ondernemingen in het Verenigd Koninkrijk en de Europese Unie niet in het gedrang brengen.»

Antwoord: «De regering van Hare Majesteit heeft kennis van de activiteiten van het Amerikaanse personeel in Menwith Hill. De politie van het ministerie van Landsverdediging staat in voor de ordehandhaving op de RAF-basis in Menwith Hill.»

1.3. Door het NSA gedeclassificeerde documenten

Het STOA-rapport heeft het over documenten die zijn gedeclassificeerd op grond van de wet inzake «Freedom of Information»(1). Ook na lezing van deze documenten (waarvan sommige stukken onleesbaar of gecensureerd zijn) blijven heel wat zaken onduidelijk, al komt de naam «Echelon» erin voor en bevestigen deze documenten dus het bestaan van dit netwerk. Ze geven echter heel weinig informatie over de werking van Echelon.

2. ANALYSE VAN DE AANNEMELIJKHEID VAN DE HYPOTHESEN VOLGENS STOA

2.1. Enkele gegevens met betrekking tot het «National Security Agency»

Op de website van het NSA vinden we een beschrijving van de ideologie van deze dienst:

— «tijdens de komende jaren zal de dreiging voor onze informatiesystemen steeds groter worden naarmate de technologieën waarmee deze systemen kunnen worden aangevallen zich vermenigvuldigen en steeds meer landen en groepen strategieën ontwikkelen waarvan dergelijke aanvallen deel uitmaken»(2);

— «Deze pagina's beschrijven het strategisch plan van het NSA/CSS voor de 21e eeuw en de manier waarop we ons doel willen bereiken: Amerikaanse suprematie op het gebied van informatie»(3).

Volgens diverse gelijkluidende bronnen zou het NSA ongeveer 40 000 personeelsleden tellen en beschikken over een budget ter waarde van 160 miljard frank in 1997. Ter vergelijking: in 1997 bedroegen de uitgaven van een industriereus als Belgacom 131

(1) De Amerikaanse *Freedom of Information Act* van 1966 (5 USC, section 552) verplicht de overheden tot openbaarheid van bestuur en creëert voor de burgers een recht van toegang tot documenten die de overheid bewaart.

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

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

la même année 131 milliards de francs belges et son personnel comptait environ vingt six mille personnes (1).

Les capacités de décryptage de la NSA sont importantes quoique non connues avec certitude et donc sujettes à spéculation.

À titre d'illustration, le système DES 56 bits recommandé par le gouvernement américain pour chiffrer les documents gouvernementaux non classifiés a été présenté en 1998 par les services américains comme impossible à casser sans utiliser 14 000 PC Pentium pendant 4 mois.

Quelques mois après cette déclaration, l'Electronic Frontier Fundation a réalisé une machine effectuant ce cassage de la clé 56 bits en moins de deux jours (2).

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

Par ailleurs, il est intéressant de noter (3) que cet algorithme, conçu à l'origine par IBM était doté d'une clé de 128 bits.

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

2.2. Que fait le réseau Échelon ?

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

James Bamford, auteur du livre « The Puzzle Palace » a pour sa part déclaré (4) :

« En tant que l'une des rares personnes extérieures à avoir suivi l'agence (la NSA) pendant des années, je

(1) *Source :* rapport annuel de Belgacom 1998.

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

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

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

miljard frank en telde deze maatschappij ongeveer 26 000 werknemers (1).

Het NSA beschikt over belangrijke capaciteiten inzake decodering, ook al zijn ze niet precies bekend en bijgevolg vatbaar voor speculaties.

In 1998 verklaarden de Amerikaanse diensten dat het systeem DES 56 bits, aanbevolen door de Amerikaanse regering om niet-geclassificeerde regeringsdocumenten te coderen, onmogelijk kon worden gekraakt zonder gedurende vier maanden gebruik te maken van 14 000 pc's van het type Pentium.

Een paar maanden later produceerde Electronic Frontier Fundation een machine die minder dan twee dagen nodig had om de 56 bits-sleutel te kraken (2).

Een dergelijke machine kost 8 miljoen frank. We kunnen moeilijk geloven dat een organisatie die inzake personeel en budget al jaren beschikt over middelen die groter zijn dan de middelen van onze nationale telecommunicatie-operator er nooit in is geslaagd een dergelijke machine te bouwen, laat staan een machine die tot veel meer in staat is dan deze machine van amateurs die over slechts heel weinig middelen beschikken.

We merken trouwens op dat dit algoritme, oorspronkelijk ontworpen door IBM, was uitgerust met een 128 bits-sleutel (3).

Het is duidelijk dat het NSA over enorme decoderingscapaciteiten beschikt en dat de Amerikanen de neiging hebben deze capaciteit in hun openbare verklaringen opzettelijk veel kleiner voor te stellen dan ze in werkelijkheid is.

2.2. Wat doet Echelon ?

We kunnen deze vraag niet met absolute zekerheid beantwoorden.

James Bamford, auteur van « The Puzzle Palace » verklaarde (4) :

« Als een van de weinige externe personen die het bureau (het NSA) jarenlang hebben gevolgd, is de

(1) *Bron :* Belgacom-jaarverslag 1998.

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

(3) Elke bit die aan een sleutel wordt toegevoegd verdubbelt het aantal mogelijke sleutels en bijgevolg ook de tijd nodig om de goede sleutel te vinden. Een 128 bits-sleutel is bijgevolg vierduizend miljard miljard keer veiliger dan een 56 bits-sleutel. Op verzoek van het NSA werd de lengte van de sleutel van het algoritme DES verminderd tot 56 bits in plaats van 128 bits zoals aanvankelijk voorzien. (Zie in verband hiermee Bruce Schneier, *Cryptographie appliquée*, International Thomson Publishing France, Parijs, 1997, blz. 283.)

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

pense que les craintes sont fort exagérées. Me basant sur tout ce que je sais de l'agence, et sur d'innombrables conversations que j'ai eues avec des membres actuels ou anciens de la NSA, je suis certain que la NSA n'outrepasse pas son mandat.

Mais cela ne signifie pas qu'elle ne le fera jamais. Mon véritable souci est que les technologies qu'elle développe à huis clos, ainsi que les méthodes qui ont éveillé de telles craintes, ont donné à l'agence la capacité d'étendre son réseau d'écoutes de manière presque illimitée. Alors que la NSA fonce dans le développement de satellites et d'ordinateurs assez puissants pour passer au crible des montagnes de données interceptées, les lois fédérales (à présent vieilles d'un quart de siècle) qui régissent l'agence n'en sont encore qu'à leurs prémices».

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

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

Les faisceaux satellitaires descendant des réseaux Intelsat (téléphonie et fax principalement) et Eutelsat (connexions internet point à point ou multipoint fournies par Belgacom) montrent que Menwith Hill est judicieusement positionnée pour capter le maximum de satellites.

À titre d'exemple nous montrons le faisceau descendant d'un satellite utilisé par Belgacom pour le trafic internet.

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

vrees volgens mij sterk overdreven. Voortgaand op al wat ik over het bureau weet en op ontelbare gesprekken die ik met de huidige of met gewezen leden van het NSA heb gevoerd, ben ik zeker dat het NSA zijn opdracht niet te buiten gaat.

Dat betekent echter niet dat het dit nooit zou doen. Ik maak me vooral zorgen over het feit dat de technologieën die het achter gesloten deuren ontwikkelt en de methoden die aanleiding hebben gegeven tot de huidige vrees, het bureau in staat hebben gesteld zijn afluisternetwerk bijna onbeperkt uit te breiden. Terwijl het NSA heel actief is in het ontwikkelen van satellieten en computers die sterk genoeg zijn om enorme hoeveelheden geïntercepteerde gegevens grondig te ziften, staan de federale wetten (die nu een kwarteeuw oud zijn) die het bureau beheersen pas aan het begin.»

Niettemin is het zeker dat dit netwerk — in het bijzonder de basis Menwith Hill bij Harrogate in Yorkshire, Engeland — wel degelijk bestaat en in aanzienlijke mate is uitgerust om alle satellietverkeer af te luisteren dat op het grondgebied van de Europese Unie wordt ontvangen.

Technisch gezien is een satelliet niets meer dan een geheel van transponders die een radiogolf vanop aarde ontvangen en ze in een bundel doorsturen. In het algemeen zijn de bundels golven die naar de aarde lopen niet op een bepaalde plaats (een stad of zelfs een land) gericht, maar omvatten ze verschillende landen.

De satellietbundels die neerdalen van de netwerken Intelsat (voornamelijk telefoon- en faxverkeer) en Eutelsat (door Belgacom geleverde punt-tot-punt- of multipuntverbindingen voor internet) tonen duidelijk aan dat Menwith Hill op een strategische plaats is gevestigd om zoveel mogelijk bundels van satellieten op te vangen.

Als voorbeeld tonen we de bundel die neerkomt van een satelliet die Belgacom gebruikt in het kader van het internetverkeer.

Het lijkt vast te staan dat bijna alle informatie die via Intelsat of Eurosat loopt, wordt opgevangen door een van de 23 antennes (volgens Duncan Campbell zijn het er 26) op de basis van Menwith Hill. Radarkoepels (ondoorzichtige koepels die elektromagnetische golven doorlaten) verbergen de exacte positie van de antennes, waardoor het niet mogelijk is na te gaan hoe ze gericht staan.

2.3. Les avis des experts européens en la matière

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

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

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

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

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

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

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

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

En d'autres termes, l'individu communiquant a conscience de laisser de plus en plus de traces mais sans pouvoir les identifier avec précision et sans connaître leurs destinataires réels. Ceci se manifeste par la réponse à la question 18 de l'étude précitée.

Face à l'assertion « Il est largement évident que les grands gouvernements utilisent la surveillance des communications pour procurer des avantages commerciaux aux entreprises et organisations », 40 % des experts interrogés en sont persuadés, 30 % sont persuadés du contraire et les 30 % restants ne peuvent pas se prononcer.

2.3. De mening van Europese experten ter zake

De opstellers van dit rapport sluiten zich aan bij de besluiten van dertig Europese experten uit alle landen, van elke leeftijd en uit alle sectoren die werden ondervraagd in het kader van het vierde STOA-rapport. In het bijzonder nemen ze de drie volgende beweringen over waarmee bijna alle ondervraagde personen akkoord gingen, te weten :

1. Tot op heden wordt alle economische informatie uitgewisseld met behulp van elektronische middelen (telefoon, fax, e-mail). Alle informatica-apparaten en schakelaars bieden steeds meer mogelijkheden om communicatie af te luisteren. Bijgevolg moeten we de bescherming van de persoonlijke levenssfeer in een context van internationale netwerken plaatsen.

2. Het belang van informatie- en communicatiesystemen voor de maatschappij en de wereldeconomie neemt evenredig toe met de kwantiteit en de steeds grotere waarde van de gegevens die met deze systemen worden opgeslagen of verstuurd. Tegelijk worden deze systemen en gegevens steeds kwetsbaarder voor diverse bedreigingen zoals toegang of gebruik zonder toelating, verduistering, vervalsing en vernietiging.

3. Encryptie is een wezenlijk bestanddeel in het beveiligen van informatie en communicatiesystemen. Er zijn toepassingen ontwikkeld waarin coderingsmethodes zijn geïntegreerd met het oog op het beveiligen van de gegevens.

Samengevat kunnen we stellen dat de steeds grotere informatisering in alle sectoren meebrengt dat

1. elke menselijke activiteit steeds meer sporen achterlaat;

2. de bewaarder, de aard en de plaats van opslag van deze sporen steeds minder zichtbaar worden voor de persoon die deze sporen meestal achterlaat zonder dat hij dat zelf wil of weet;

3. er tegelijk steeds minder zichtbare sporen zijn van het opvangen van voornoemde onzichtbare sporen.

Met andere woorden, een persoon die communiceert beseft dat hij steeds meer sporen achterlaat, maar hij kan deze sporen niet precies identificeren en weet niet wie de werkelijke bestemmelingen zijn. Dit blijkt uit het antwoord op vraag 18 van de bovengenoemde studie.

Geconfronteerd met de stelling « Het is overduidelijk dat regeringen van grote landen van de controle op de communicatie gebruik maken om aan ondernemingen en organisaties commerciële voordelen te bezorgen », antwoordt 40 % van de ondervraagde experten dat ze daarvan overtuigd zijn, terwijl 30 % van het tegendeel is overtuigd en 30 % zich niet durft uitspreken.

Il est probable que cette répartition d'opinion en trois tiers se retrouvera parmi le grand public et parmi ... les lecteurs de ce rapport.

2.4. L'avis de Belgacom

Selon l'avis de plusieurs ingénieurs de Belgacom, le trafic Intelsat (principalement fax et téléphonie) ne serait pas crypté par l'opérateur. Toutefois, seulement un pourcent du trafic téléphonique international transiterait par satellite, principalement pour assurer la connexion vis-à-vis de pays ne possédant pas une bonne infrastructure filaire terrestre (les exemples de certains pays d'Afrique et de l'Inde ont été cités). Les liaisons fournies dans le cadre des services V-STAR (1), utilisant le réseau Eurosat ne sont pas systématiquement cryptées par l'opérateur mais elles peuvent l'être lorsque Belgacom fournit l'applicatif au client.

Par ailleurs le trafic V-link se déroule suivant un protocole propriétaire, propre à Belgacom, ce qui compliquerait le décodage des informations transmises.

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

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

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

Ce point a déjà été esquissé (supra nº 2). Une caractéristique majeure des nouvelles technologies de l'information et de la communication se situe dans les traces que chaque télécommunication laisse, généralement à l'insu de la personne qui communique.

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

Wellicht vinden we deze verdeling van de meningen in drie min of meer gelijke stukken terug onder het grote publiek en ... bij de lezers van dit rapport.

2.4. De mening van Belgacom

Diverse Belgacom-ingenieurs zijn van mening dat het Intelsat-verkeer (vooral fax en telefoon) niet wordt gecodeerd door de operator. Anderzijds zou slechts één procent van het internationaal telefoonverkeer via satelliet verlopen, in hoofdzaak om de verbinding te verzekeren met landen die op het aardoppervlak niet over een degelijke draadinfrastructuur beschikken (als voorbeeld werd verwezen naar een aantal Afrikaanse landen en naar India). De verbindingen in het kader van de V-STAR-diensten (1), waarbij gebruik wordt gemaakt van het Eurosatnetwerk, worden door de operator niet systematisch gecodeerd, maar dit kan wel gebeuren indien Belgacom de nodige applicaties daarvoor aan de klant bezorgt.

Overigens verloopt het V-STAR-verkeer volgens een protocol dat eigendom is van Belgacom en dat het ontcijferen van de verstuurde informatie zou bemoeilijken.

In elk geval is het helemaal niet moeilijk om telecommunicatie feitelijk te intercepteren. Meer dan een antenne en een decoder heeft men niet nodig. Met betrekking tot Intelsat vindt al wie communicatie wil intercepteren op het internet de nodige programma's die hem toelaten zijn antenne voortdurend op de gewenste satelliet te richten.

In de heel korte periode (12 dagen) waarover ze beschikten, konden de experten geen diepgaander analyse maken van de internationale en/of satelliettelecommunicatie die de nationale operators verrichten. Een dergelijk uitgebreid onderzoek lijkt ons echter absoluut noodzakelijk wil men alle telecommunicatieverkeer in België beter beveiligen.

3. ECHELON IN DE BREDERE CONTEXT VAN HET TOEZICHT OP TELECOMMUNICATIE

We hebben dit punt al even aangehaald (*cfr. supra* nr. 2). Een van de belangrijkste kenmerken van de nieuwe informatie- en communicatietechnologieën heeft te maken met het feit dat alle telecommunicatieverkeer sporen achterlaat, gewoonlijk zonder dat de persoon die communiceert dat beseft.

(1) De diensten voor het versturen van gegevens via satelliet, worden V-STAR genoemd (http://www.belgacom.be/satellite). Ze omvatten de diensten V-STAR voor multipuntverbindingen en V-Link voor punt-tot-puntverbindingen.

C'est un phénomène global et le réseau Échelon n'est qu 'une manifestation de ce qui est possible à partir de la surveillance des satellites.

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

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

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

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

3.1. Les vulnérabilités du hardware et du software

Tant le hardware que le software peuvent offrir ce que l'on appelle en sécurité informatique des judas (peep hole), des portes dérobées (backdoors) ou des fonctions cachées (non signalées dans la documentation).

Dans tous ces cas de figure, l'utilisateur d'un routeur ou d'un processeur ignore certaines fonctionnalités qui peuvent être utilisées, de manière invisible et de plus en plus souvent à distance par un tiers les connaissant.

Le premier rapport du STOA cite ainsi une fonctionnalité des centraux RNIS permettant d'écouter ce qui se dit dans une pièce via un téléphone raccroché.

En juillet 1999, Richard Smith, un consultant en sécurité, a mis en évidence que RealJukebox, un logiciel gratuit d'écoute de CD musicaux diffusé en Europe à des millions d'exemplaires transmettait à la maison mère américaine, de manière cryptée et à intervalles réguliers les index des CDROM qui étaient insérés dans le lecteur du PC (1).

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

Dans les versions de Microsoft Office 1997, chaque document Word, Excel ou Powerpoint était marqué d'un numéro de série unique composé en partie du numéro de série de la carte Ethernet de l'ordinateur.

Ceci permettait à Microsoft de retrouver l'auteur de n'importe quel document Word, Excel ou Powerpoint 97, pour peu que celui-ci se soit enregistré en ligne.

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

Dit is een algemeen fenomeen en Echelon is niet meer dan een voorbeeld van wat mogelijk is als men satellieten bewaakt.

Afgezien van de problemen inzake vertrouwelijkheid die opduiken telkens wanneer men met mensen te maken heeft, berust de moderne telecommunicatietechnologie op een keten van drie afzonderlijke elementen die elkaar aanvullen en elk hun eigen zwakke punten hebben.

1. Communicatiehardware (routers, geïntegreerde schakelingen, processors, antennes enz.).

2. Communicatiesoftware (het programma dat de hardware stuurt).

3. Communicatie-dragers (kabels, glasvezels, radiogolven enz.).

3.1. Zwakke punten van hardware en software

Zowel hardware als software kunnen vertonen wat men op het gebied van informaticabeveiliging kijkgaatjes (peepholes), geheime deurtjes (backdoors) of verborgen functies (niet vermeld in de documentatie) noemt.

In al deze gevallen is de gebruiker van een router of processor niet op de hoogte van bepaalde functionaliteiten die onzichtbaar en steeds vaker vanop afstand kunnen worden gebruikt door een derde die ze wel kent.

In het eerste STOA-rapport wordt gewezen op een functionaliteit van ISDN-centrales die het mogelijk maakt af te luisteren wat in een bepaald lokaal wordt gezegd via een opgehangen telefoon.

In juli 1999 bewees Richard Smith, een beveiligingsconsulent, dat RealJukebox, een softwareprogramma voor het gratis beluisteren van CD's en waarvan in Europa miljoenen exemplaren verdeeld zijn, de indexen van de cd-roms in de PC-lezer regelmatig gecodeerd doorstuurde naar de Amerikaanse moedermaatschappij (1).

Een paar maanden eerder had diezelfde Richard Smith ontdekt dat de software voor de on line-registratie van Windows 98 gedetailleerde gegevens betreffende de uitrusting van de internaut naar Microsoft stuurde, met inbegrip van bepaalde serienummers.

In de versies van Microsoft Office 1997 werd elk Word-, Excel- of PowerPoint-document gemerkt met een uniek serienummer dat onder meer het serienummer bevatte van de Ethernet-kaart van de computer.

Zo kon Microsoft de auteur van eender welk document in Word, Excel of PowerPoint 97 opsporen op voorwaarde dat de betrokkene zich on line had geregistreerd.

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

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

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

La liste de ce qui se passe sur le réseau Internet à l'insu de l'utilisateur est longue et les quelques cas relevés ci-dessus n'ont valeur que d'exemples non sujets à caution (1).

3.2. La vulnérabilité des supports de communication

En ce qui concerne le support de communication, chaque support rayonne une part de l'information qu'il transporte. Cela est clair pour le satellite qui transmet à l'Europe entière l'information destinée à une antenne particulière dans un pays déterminé.

Le courant circulant dans les câbles de télécommunication produit une onde électromagnétique dont une partie se déploie à l'extérieur du câble et peut donc être capturée sans rupture de celui-ci.

La fibre optique elle-même laisse passer une quantité infime de lumière. Il est possible de la polir légèrement ou de la courber afin de capturer une partie significative de lumière de façon à pouvoir reconstituer le message. Néanmoins, à ce jour, la fibre optique reste de loin le support le plus difficile à espionner.

Par ailleurs, grâce à la cryptographie quantique (2) associée à ce média, il semble qu'il serait possible de détecter automatiquement et systématiquement toute écoute du signal transitant sur une fibre optique, ce qui ferait de la fibre un support non sujet à des écoutes invisibles.

4. DESCRIPTION DES TECHNOLOGIES UTILISÉES ET NATURE DES MESSAGES INTERCEPTÉS

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

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

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

Dankzij het gebruik van cookies in onzichtbare hyperlinks en de onzichtbare communicatie van navigatieprogramma's (bv.: Internet Explorer of Netscape Communicator), geïmplementeerd in strijd met mondiale voorschriften, slagen onbekende cybermarketingbedrijven er in op individuele basis alle sleutelwoorden te verzamelen en op te slaan die elke Europese internaut ingeeft op een aantal grote zoekmachines.

DoubleClick alleen al, een Amerikaans cybermarketingbedrijf, gebruikt dit procédé meer dan een half miljard keer per dag.

De lijst van al wat op het internet gebeurt zonder dat de gebruiker het beseft is heel lang. We hebben hierboven slechts een paar vaststaande voorbeelden gegeven (1).

3.2. De kwetsbaarheid van communicatie-dragers

Elk communicatie-drager straalt een deel uit van de informatie die het vervoert. Dit is duidelijk in het geval van een satelliet die de informatie bestemd voor een specifieke antenne in een welbepaald land aan heel Europa bezorgt.

De stroom die door telecommunicatiekabels loopt, produceert een elektromagnetische golf waarvan een deel zich buiten de kabel ontplooit en bijgevolg kan worden opgevangen zonder dat men de kabel moet breken.

Glasvezels laten een heel minieme hoeveelheid licht door. Het is mogelijk dit licht ietwat te bewerken of om te buigen teneinde een grotere hoeveelheid licht te verkrijgen en het bericht zo opnieuw samen te stellen. Toch blijven glasvezels het moeilijkst te bespioneren middel.

Trouwens, dankzij de kwantumencryptie (2) die met deze communicatie-drager is verbonden zou het blijkbaar mogelijk zijn elk geval van afluistering van het signaal dat per glasvezel wordt vervoerd automatisch en systematisch op te sporen. Als gevolg daarvan zouden glasvezels niet kunnen worden afgeluisterd zonder dat men het merkt.

4. BESCHRIJVINGVANDEGEBRUIKTETECHNOLOGIEËN EN AARD VAN DE GEÏNTERCEPTEERDE BERICHTEN

In de eerste plaats verwijzen we naar de bovengenoemde studies van Leprévost en Campbell die volgens ons van een uitstekend wetenschappelijk niveau zijn.

(1) De hierboven beschreven gevallen waren het voorwerp van een studie in het kader van het Europees project Eclip. Het rapport waarin sommige «privacide» technologieën worden beschreven staat op het internet: http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf

(2) Zie het STOA-rapport van F. Leprévost, punt 6.2. en Bruce Schneier, op. cit., pp. 584-586.

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

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

Pour ce faire, il faudrait tout d'abord que la communication internationale passe par satellite, ce qui semble être le cas d'un pourcent seulement des communications internationales (*cfr. supra*).

Même dans ce cas de figure, la technologie actuelle de reconnaissance vocale universelle n'est pas suffisamment au point pour permettre la reconnaissance vocale en temps réel. Par contre, il est possible actuellement de réaliser un dispositif capable de reconnaître l'empreinte vocale d'une personne particulière et d'initier un processus d'enregistrement et de traitement à ce moment.

La recherche de mots-clés sensibles contenus dans un dictionnaire reste néanmoins possible lors de la surveillance des courriers électroniques ou du trafic Internet en général (si celui-ci circule par satellite)(1) ainsi que lors de la surveillance des téléfax, dans la limite des performances des logiciels de reconnaissance de caractère (les caractères envoyés doivent être clairs et non manuscrits).

En d'autres termes, la surveillance exploratoire et généralisée sur base de renifleurs (snifer) de mots-clés sensibles n'est possible que sur une partie du trafic satellitaire.

Il semble aussi ou ainsi possible de détecter l'auteur d'une communication téléphonique sur base de son empreinte vocale.

4.2. La NSA-KEY de Microsoft

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

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

(1) Le présent rapport concerne Échelon. D'autres techniques d'écoute des réseaux terrestres existent ...

Voorts willen we de nadruk leggen op een bepaald punt in het onderhavige rapport, een element in de mondelinge presentatie van Campbell voor het Europees Parlement in februari 2000 ontkrachten en een nieuw element naar voren brengen dat we in de bovengenoemde rapporten niet terugvinden.

4.1. Het woord «bom» gebruiken in een telefoongesprek leidt niet tot een afluisteroperatie

Hiervoor zou alle internationale communicatie per satelliet moeten verlopen, maar dit lijkt slechts het geval te zijn in één procent van de internationale communicaties (*cfr. supra*).

Zelfs in dit geval is de universele spraakherkenningstechnologie vandaag nog niet voldoende ontwikkeld om de spraakherkenning in reële tijd toe te laten. Het is momenteel wel al mogelijk een systeem te produceren dat de stemafdruk van een privépersoon kan herkennen en op dat ogenblik een registratie- en verwerkingsproces in gang kan zetten.

Het zoeken naar gevoelige sleutelwoorden opgeslagen in een woordenboek blijft echter wel mogelijk bij het bewaken van e-mail of van internetverkeer in het algemeen (indien het per satelliet plaatsvindt(1), alsmede bij het bewaken van faxverkeer, binnen de beperkingen van de prestaties die de letterherkenningssoftware kan leveren (de verstuurde letters moeten duidelijk en niet handgeschreven zijn).

Met andere woorden, het verkennend en veralgemeend bewaken met behulp van «snuffelaars» die gevoelige sleutelwoorden zoeken is alleen mogelijk bij een deel van het satellietverkeer.

Voorts lijkt het mogelijk te zijn de persoon die een telefoongesprek voert te herkennen aan de hand van zijn stemafdruk.

4.2. De NSA-KEY van Microsoft

Het internet stond in rep en roer toen in het register van het Windows-besturingssysteem een variabele voorkwam die NSA-KEY werd genoemd. Heel veel mensen beweerden toen dat deze geheime sleutel het NSA toeliet alle gecodeerde berichten te lezen met behulp van coderingsfuncties die Microsoft leverde.

1. Microsoft heeft deze hypothese weerlegd, hoewel ze de «zwakke punten» waarnaar hierboven (punt 3.1.) wordt verwezen heeft toegegeven.

(1) Dit rapport heeft betrekking op Echelon. Er bestaan nog andere technieken om netwerken op aarde af te luisteren ...

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

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

Cette fausse alerte ne doit cependant pas faire croire que les fonctions de chiffrement fournies par Microsoft soient sûres. Les signataires de ce rapport partagent avec de nombreux experts l'opinion selon laquelle toute exportation d'outils de chiffrement hors des USA n'est autorisée que lorsque les services américains possèdent la capacité technique de casser le chiffrement.

De toutes façons, il est actuellement généralement admis dans le monde de la cryptographie qu'un logiciel de chiffrement n'est fiable que lorsque l'on dispose de son code source.

4.3. Des clés faussement 128 bits

Il existe au moins deux manières de faire croire à un utilisateur même averti qu'il utilise un mode chiffrement à 128 bits (1) alors que son chiffrement effectif se limite à quarante bits.

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

La deuxième technique est plus subtile et consiste à conditionner le générateur de clés secrètes inclus dans le logiciel de chiffrement (2) de telle manière que celui-ci ne puisse générer que des clés incluses dans un espace de chiffrement limité à quarante bits.

Sans accès au code source du logiciel de chiffrement, cette dernière technique est difficilement détectable car il faudrait générer plusieurs centaines de milliards de clés pour s'apercevoir de la supercherie.

Selon un expert de Belgacom, cette dernière technique serait largement répandue dans les logiciels de chiffrement américains autorisés à l'exportation.

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

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

2. We kunnen ons moeilijk voorstellen dat een geheime decoderingssleutel wordt opgeslagen op een zo zichtbare plaats als het register.

3. Het lijkt nog veel onvoorstelbaarder dat deze sleutel de naam NSA-KEY zou hebben gekregen.

Dit vals alarm mag ons echter niet doen geloven dat de door Microsoft geleverde coderingsfuncties veilig zijn. De ondergetekende opstellers zijn van mening, net als vele andere deskundigen, dat coderingsinstrumenten pas buiten de USA mogen worden uitgevoerd wanneer de Amerikaanse diensten over de technische mogelijkheden beschikken om de code te breken.

In elk geval neemt men in de encryptiewereld vandaag algemeen aan dat coderingssoftware alleen betrouwbaar is wanneer men over de broncode ervan beschikt.

4.3. Valse 128 bits-sleutels

Er bestaan ten minste twee manieren om zelfs een gewaarschuwd gebruiker te doen geloven dat hij een coderingsmodus met 128 bits (1) gebruikt terwijl zijn reële codering beperkt is tot 40 bits.

De eerste techniek, die Lotus Notes zou hebben ontworpen, wordt door Campbell beschreven. Bij deze techniek worden de laatste 88 bits van de sleutel zichtbaar verstuurd in het eigenlijke bericht. Het is mogelijk deze techniek op te sporen.

De tweede techniek is heel wat subtieler en bestaat erin de generator van geheime sleutels in de coderingssoftware (2) zodanig te conditioneren dat hij slechts sleutels kan genereren die vervat zijn in een coderingsruimte van maximum 40 bits.

Wie geen toegang heeft tot de broncode van de coderingssoftware kan deze techniek heel moeilijk op het spoor komen, aangezien men honderden miljarden sleutels zou moeten genereren om het bedrog te ontdekken.

Volgens een Belgacom-expert zou deze laatste techniek vaak voorkomen in Amerikaanse coderingssoftware die mag worden uitgevoerd.

(1) We herinneren eraan dat een 128 bits-sleutel duizenden miljard keer veiliger is dan een 56 bits-sleutel.

(2) We merken op dat dit risico niet bestaat indien de geheime sleutel is ontworpen door een betrouwbare derde die zijn eigen generator van geheime sleutels heeft bedacht met naleving van de regels van de kunst.

5. LA LÉGALITÉ DISCUTABLE DES PRATIQUES DU RÉSEAU ÉCHELON — COUP D'ŒIL SUR L'ENVIRONNEMENT JURIDIQUE DES « INTERCEPTIONS DE TÉLÉCOMMUNICATIONS » (1)

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

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

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

5.1. Premier temps : les principes de la Convention européenne des droits de l'homme s'opposent aux pratiques dénoncées propres au système Échelon

L'interception de messages transmis par télécommunications représente un danger tant pour la vie privée des personnes mises sur écoutes que pour leur liberté d'expression.

Ces deux libertés représentent des libertés essentielles dont la protection est assurée par nombre de textes internationaux dont la Convention européenne des droits de l'homme (2).

Certes, des impératifs légitimes de sécurité de l'État justifient que les États disposent de moyens techniques efficaces permettant l'interception légale des

(1) Le lecteur se référera également à l'étude du professeur Elliot, *The legality of the interception of electronic communications. A concise survey of the principal legal issues and instruments under international, European and national law, working document for the STOA Panel*, Luxembourg, octobre 1999, PE 168 184, Vol. 4 et 5. L'auteur y décrit d'autres sources nationales et internationales.

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

5. DE BETWISTBARE LEGALITEIT VAN DE ECHELON-PRAKTIJKEN — EEN BLIK OP DE JURIDISCHE CONTEXT INZAKE HET « INTERCEPTEREN VAN TELECOMMUNICATIE » (1)

De bovenstaande beschrijving van het systeem Echelon roept vele vragen op met betrekking tot de wettelijkheid van het intercepteren van telecommunicatie waartoe dit systeem overgaat.

Om te beginnen wijzen we in verband hiermee op de beginselen van het Europees Verdrag voor de rechten van de mens. Ten tweede beschrijven we de positie van Europa, dat geleidelijk de beginselen van het Europees Verdrag heeft overgenomen. Ten derde onderstrepen we hoe België deze beginselen in de nationale wetgeving heeft omgezet, in het bijzonder bij het goedkeuren van de organieke wet over de inlichtingen- en veiligheidsdiensten, ook al zegt de wet helaas niets over hetgeen ons vandaag bezighoudt.

Tot slot tonen we aan dat het helemaal niet vanzelfsprekend is dat de Verenigde Staten, de voornaamste protagonist op het vlak van afluisteren van communicatie, de Europese beginselen naleven.

5.1. Ten eerste : de beginselen van het Europees Verdrag voor de rechten van de mens verzetten zich tegen de aangeklaagde praktijken die eigen zijn aan Echelon

De interceptie van telecommunicatieberichten bedreigt de persoonlijke levenssfeer en de vrije meningsuiting van personen die worden afgeluisterd.

Deze twee vrijheden zijn fundamentele vrijheden waarvan de bescherming wordt verzekerd door een groot aantal internationale teksten, waaronder het Europees Verdrag voor de rechten van de mens (2).

Toegegeven, wettelijke imperatieven m.b.t. de veiligheid van de Staat rechtvaardigen dat staten over doeltreffende technische middelen beschikken die de

(1) De lezer kan ook de studie van Professor Elliot raadplegen, *The legality of the interception of electronic communications. A concise survey of the principal legal issues and instruments under international, European and national law, working document for the STOA Panel*, Luxemburg, oktober 1999, PE 168 184, Vol. 4 en 5. In zijn studie beschrijft de auteur andere nationale en internationale bronnen.

(2) Zie ook artikel 17 van het Internationaal Pact d.d. 19 december 1966 over burgerlijke en politieke rechten : « Niemand wordt onderworpen aan willekeurige en onwettelijke inmenging die zijn persoonlijke levenssfeer in het gedrang brengt. » « Eenieder heeft recht op wettelijke bescherming tegen dergelijke inmenging. »

télécommunications peu importe, le réseau ou le medium utilisé et peu importe qu'il s'agisse de la prise de connaissance du contenu des messages ou simplement de certains éléments de ceux-ci (ex : origine ou destination de l'appel, localisation de celui-ci).

Cependant comme le notent l'arrêt Klass (1) et l'arrêt Leander, il est nécessaire de disposer « de garanties suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre ».

Quatre conditions dès lors limitent l'immixtion possible de l'État. Ces quatre conditions applicables en matière d'interception des télécommunications ont été maintes fois rappelées par la jurisprudence de la Cour européenne des droits de l'homme.

Ainsi, il importe :

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

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

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

4º enfin selon l'arrêt Leander rendu à propos de la contestation d'un citoyen convaincu d'être fiché par la sûreté de l'État et se voyant opposer lors de sa demande d'accès à son dossier, le dogme du secret indispensable à la sécurité de l'État, il importe qu'une balance soit opérée entre d'une part la protection de la vie privée et d'autre part les impératifs de sécurité et d'ordre public qui fondent la mission des services de renseignements et de sûreté; importe plus encore, ajoute l'arrêt, que cette balance soit opérée par une autorité indépendante (2).

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

(2) Comme peut l'être en Belgique, le Comité R, Comité permanent de contrôle des services de renseignements dépendant du Parlement.

legale interceptie van telecommunicatie mogelijk maken, ongeacht het gebruikte netwerk of medium en ongeacht of het gaat om het kennis nemen van de inhoud van berichten of van bepaalde elementen daarvan (vb. : oorsprong of bestemming en lokalisatie van de oproep).

Toch is het noodzakelijk, zoals bepaald in het arrest-Klass (1) en het arrest-Leander, te beschikken « over voldoende waarborgen tegen misbruiken, aangezien een systeem van geheim toezicht met het oog op het beschermen van de nationale veiligheid het risico inhoudt dat de democratie wordt ondermijnd, zelfs vernietigd ».

Vier voorwaarden beperken de mogelijke inmenging van de Staat. In de rechtspraak van het Europees Hof voor de rechten van de mens wordt vele keren verwezen naar deze vier voorwaarden, toepasbaar inzake het intercepteren van telecommunicatie.

Het is van belang :

1º dat de interceptie alleen plaatsvindt in het kader van de doelstellingen van vitaal belang voor de Staat, opgesomd in de artikelen 8 en 10 van het Verdrag zelf;

2º dat deze doelstellingen wettelijk worden bepaald, d.w.z. in een reglementaire tekst waartoe het publiek toegang heeft en die is opgesteld met zodanige precisie dat de burger er passend op kan reageren (arrest-Kruslin d.d. 24 april 1990);

3º vervolgens, dat de genomen maatregel strikt in verhouding staat tot het doel dat men nastreeft. In dit opzicht is een verkennend of algemeen toezicht op grote schaal verboden, zoals met name wordt bepaald in het arrest-Klass (d.d. 6 september 1978) en het arrest-Leander (d.d. 25 februari 1987);

4º tot slot, overeenkomstig het arrest-Leander — dat werd verleend naar aanleiding van de betwisting door een burger die ervan overtuigd was dat hij geregistreerd was bij de staatsveiligheid en vaststelde, toen hij een aanvraag neerlegde om inzage te krijgen van zijn dossier, dat het dogma van het noodzakelijk geheim voor de veiligheid van de Staat tegen hem werd ingeroepen — is het van belang dat er een evenwicht tot stand wordt gebracht tussen enerzijds de bescherming van de persoonlijke levenssfeer en anderzijds de imperatieven inzake veiligheid en openbare orde die de basis vormen van de opdrachten van de inlichtingen- en veiligheidsdiensten; het is van nog groter belang, voegt het arrest eraan toe, dat een onafhankelijke overheid dit evenwicht tot stand brengt (2).

(1) Klass v. Germany (1978), 2HRR, p. 214; cf. ook Malone v. UK (1984), 7EHRR, p. 14.

(2) In België kan het Comité I - het Vast Comité van Toezicht op de inlichtingendiensten bij het parlement - deze taak waarnemen.

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

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

— que la (ou les) finalité(s) d'Échelon soi(en)t définie(s) par des textes réglementaires, clairs et accessibles au public (1);

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

— qu'un tel système limite strictement la collecte de données à ce qui est nécessaire aux finalités de sûreté de l'État;

— qu'il soit analysé si un contrôle des écoutes par une autorité indépendante est prévu (2) conformément à l'exigence de l'arrêt Léander de la Cour européenne des droits de l'homme.

(1) À tel point qu'il est évoqué l'utilisation du réseau Échelon à des fins d'espionnage industriel, ce qui est difficilement compatible avec les impératifs de la sûreté de l'État.

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

Precies in verband met het intercepteren van telecommunicatie raadt de aanbeveling R(95)14 van het ministercomité van de Raad van Europa, goedgekeurd op 11 september 1995 «met betrekking tot de strafrechtelijke procedure in verband met informatietechnologieën» onder meer aan de strafwetten te wijzigen om de interceptie toe te laten in geval van onderzoek bij ernstige aanvallen tegen informatie- en telecommunicatiesystemen en maatregelen te nemen om de negatieve weerslag van de encryptie te beperken zonder het gebruik ervan, voorbijgaand aan wat noodzakelijk is, in twijfel te trekken.

Onder voorbehoud van wat we hierna stellen met betrekking tot de Verenigde Staten en hun reglementaire situatie (*cf. infra* punt 5.4.), opdat er conformiteit zou zijn met de vereisten van de beginselen van de Raad van Europa, is het nodig:

— dat de doelstelling(en) van Echelon wordt (worden) gedefinieerd in duidelijke reglementaire teksten waarvan het publiek kennis kan nemen (1);

— dat de intercepties in het kader van Echelon niet plaatsvinden op grond van het systematisch zoeken naar sleutelwoorden of van andere algemene criteria, maar, zoals bepaald in de rechtspraak van het Europees Hof voor de rechten van de mens, in functie van specifieke criteria die verband houden met precieze inbreuken of met de vermoedelijke daders van die inbreuken;

— dat een dergelijk systeem het verzamelen van gegevens strikt beperkt tot wat nodig is voor de doelstellingen van de staatsveiligheid;

— dat wordt onderzocht of een controle op het afluisteren door een onafhankelijke overheid is ingesteld (2) overeenkomstig de voorwaarde van het arrest-Leander van het Europees Hof voor de rechten van de mens.

(1) Men heeft het over het gebruik van Echelon met het oog op industriële spionage, wat moeilijk verzoenbaar is met de imperatieven van de veiligheid van de Staat.

(2) Zie in verband hiermee het onderzoeksrapport «over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het intercepteren van telefoon- en faxverkeer in België», voorgesteld door het Comité I aan de Belgische senaat op 14 februari 2000, p. 8, alsmede de opmerkingen over het amendement van de Intelligence Authorization Act, ingediend door Bob Barr, lid van het Amerikaanse Congres, waarin hij eiste dat er een wettelijke grondslag kwam voor de interventie van het Amerikaanse NSA op het gebied van elektronisch toezicht en het intercepteren van telecommunicatie.

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

L'article 6 du Traité sur l'Union européenne affirme :

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

Le Traité d'Amsterdam (1) complète cette disposition de principe étendant par son article 46 la compétence juridictionnelle de la Cour de Justice des Communautés européennes à l'action des institutions : il s'agit de vérifier le respect des droits fondamentaux garantis à travers la référence que l'article 6 fait à la CEDH.

Émerge dans l'ordre juridique communautaire un système commun de protection des droits fondamentaux.

C'est sur base de cet élargissement des compétences techniques que deux directives, l'une dite générale relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci, l'autre, spécifique (2); concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, ont été prises et doivent être transposées dans les divers États membres.

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

Cet ajout impose ce respect à la fois pour l'agréation des équipements terminaux (3), pour la

(1) Signé le 2 octobre 1997 (J.O.C.E. C. 103, 24 avril 1977).

(2) Directive 95/40/CE du 24 octobre 1995, J.O., L 281 du 23 novembre 1995, p. 31.

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

5.2. Ten tweede : de positie van Europa : van dubbelzinnigheid tot concrete voorstellen

Artikel 6 van het Verdrag over de Europese Unie bepaalt :

« De Unie is gebaseerd op de beginselen van vrijheid, van democratie, van eerbied voor de rechten van de mens en de fundamentele vrijheden, alsmede de rechtsstaat, beginselen die alle lidstaten gemeen hebben. De Unie heeft eerbied voor de fundamentele rechten zoals ze worden gewaarborgd door het EVRM, getekend op 4 november 1950 in Rome, en zoals ze voortvloeien uit de grondwettelijke tradities die de lidstaten gemeen hebben, als algemene beginselen van het communautair recht ».

Het Verdrag van Amsterdam (1) vult deze principiële bepaling aan door in artikel 46 de rechtsprekende bevoegdheid van het Hof van Justitie van de Europese Gemeenschappen uit te breiden tot de werking van de instellingen : het gaat erom toe te zien op de eerbied voor de gewaarborgde fundamentele rechten door de verwijzing in artikel 6 naar het EVRM.

In de juridische orde van de Europese Gemeenschap verschijnt een gemeenschappelijk systeem tot bescherming van de fundamentele rechten.

Op grond van deze uitbreiding van de technische bevoegdheden zijn twee richtlijnen uitgevaardigd die in de nationale wetgeving van de verschillende lidstaten moeten worden omgezet. De eerste richtlijn is van algemene aard en betreft de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en het vrij verkeer daarvan. De tweede richtlijn is van specifieke aard (2) en betreft de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector.

Deze uitbreiding van de basisakten houdende de vaststelling van de Europese bevoegdheid rechtvaardigt ook de toevoeging, in de zogenaamde richtlijnen-Telecommunicatie, van de eerbied voor de bescherming van gegevens onder de « essentiële voorwaarden ».

Deze toevoeging legt deze eerbied op voor de erkenning van eindapparatuur (3), voor de levering

(1) Getekend op 2 oktober 1997 (Publicatieblad, C. 103, 24 april 1997).

(2) Richtlijn 95/40/EG d.d. 24 oktober 1995, Publicatieblad, L. 281 d.d. 23 november 1995, p. 31.

(3) Richtlijn 99/5/EG d.d. 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit, L. 91/10, 7.4.99 artikel 3.3., dat bepaalt dat de Commissie inzake radioapparatuur maatregelen kan nemen.

fourniture des réseaux ouverts (1) et de manière générale pour les autorisations générales et les licences individuelles dans les États membres (2). Surtout, il autorise la prise de mesures nationales et européennes pour assurer cette protection (3).

En ce sens, le rapport STOA (4) préconisait l'adoption par les pays européens d'un encryptage généralisé comme mesure de protection contre des écoutes ou des mesures de surveillance contraires aux principes déjà décrits (5).

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

Ainsi, c'est dans une totale méconnaissance de ces préoccupations que le Conseil de la Communauté européenne a adopté, sous la pression américaine, le 17 janvier 1995, une résolution (6) visant à faciliter les écoutes téléphoniques.

La résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications détaille les conditions techniques nécessaires à l'inter-

van open netwerken (1) en in het algemeen voor de algemene machtigingen en individuele vergunningen in de lidstaten (2). De toevoeging laat vooral toe dat op nationaal en Europees vlak maatregelen worden genomen om deze bescherming te verzekeren (3).

In deze zin beval het STOA-rapport (4) aan dat de Europese landen een algemeen coderingssysteem zouden aannemen als bescherming tegen afluisteroperaties of maatregelen van toezicht die strijdig zijn met de hierboven beschreven beginselen (5).

Wie het Europese standpunt inzake de legitimiteit van de « intercepties » van telecommunicatie goed wil begrijpen, moet er rekening mee houden dat de Europese bezorgdheid betreffende de rechten van de mens en de aanvaarding van de reeds aangehaalde beginselen van de rechtspraak van het Europees Hof voor de rechten van de mens, recent is.

Zonder de minste kennis van deze preoccupaties keurde de Raad van de Europese Gemeenschap op 17 januari 1995, onder druk van de Amerikanen, een resolutie (6) goed om het afluisteren van telefoonverkeer te vergemakkelijken.

De resolutie van de Raad d.d. 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer geeft een gedetailleerde beschrijving van de tech-

---

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

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

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

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

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

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

---

(1) Richtlijn van de Raad 90/387/EEG d.d. 28 juni 1990 gewijzigd door richtlijn 97/51/EG van het Europees Parlement en de Raad d.d. 6 oktober 1997 met het oog op de aanpassing aan een door concurrentie gekenmerkte context in de telecommunicatie, Publicatieblad nr. L 295/ 23, 29.10 1997 genoemd « richtlijn ONP Amendment ».

(2) Het gaat om de richtlijn 97/13/EG van het Europees Parlement en de Raad d.d. 10 april 1997 (Publicatieblad, L. 117, mei 1997).

(3) Artikel 3.3. van de richtlijn 99/15/EG bepaalt : « Overeenkomstig de procedure bepaald in artikel 15 kan de Commissie besluiten dat apparatuur van bepaalde apparatuurcategorieën of apparatuur van een bepaalde soort zo geconstrueerd moet zijn : *b)* dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen; ... »

(4) Het gaat om deel 4/4 van de STOA-rapporten die in april en mei 1999 in het Europees Parlement zijn voorgesteld en op verzoek van dit Parlement zijn opgesteld. De titel van dit deel luidt als volgt : *« The State of the Art in communication Intelligence (COMINT) for intelligence purpose of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT Targeting and Selection, including speech recognition »* en vooral om het STOA-rapport dat in oktober 1999 aan het Europees Parlement is voorgesteld (PE 168 184/ Vol; 1 tot 5), getiteld *Development of Surveillance Technology and Risk of Abuse of economic Information.*

(5) Het rapport pleit ook voor een liberalisering van de encryptie in het Europees beleid inzake encryptie in de akkoorden van Wassenaar en de reglementeringen van de lidstaten, cfr. de website van B.J. Koops : *Crypto Law Survey*, http ://CWIS.Kab.nl/ friv/people/cls2.htm

(6) Resolutie van de Raad 17/1/1995, Publicatieblad C. 329 d.d. 4 november 1996 p. 1 tot 6 (we merken op dat de publicatie van deze resolutie lang op zich liet wachten en dat de resolutie werd goedgekeurd zonder dat het advies van het Parlement werd gevraagd). Deze resolutie wordt gevolgd door een gemeenschappelijke interventieverklaring, getekend door de Amerikaanse en Europese overheden, betreffende het wettelijk toezicht op telecommunicatie die bepaalt dat inlichtingen en aanbevelingen kunnen worden uitgewisseld m.b.t. de specificaties inzake intercepties bestemd voor het bestuur van het Amerikaanse FBI en voor het algemeen secretariaat van de Raad van de Europese Unie (Doc. ENFOPOL 112 - Brussel 25 oktober 1995).

ception des télécommunications, sans aborder la question des conditions dans lesquelles de telles interceptions devraient avoir lieu.

Le texte de la résolution prévoit une obligation dans le chef des opérateurs de réseaux ou des fournisseurs de services de fournir en clair aux « services autorisés » les données interceptées.

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

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

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

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

Ses recommandations sont plus nettes encore.

Le Parlement européen :

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

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

nische voorwaarden vereist voor het intercepteren van telecommunicatie.

Ze bevat echter geen bepalingen over de voorwaarden waarin dergelijke intercepties zouden moeten plaatsvinden. De tekst van de resolutie bevat voor de netwerkexploitanten of de dienstenverstrekkers de verplichting om de geïntercepteerde communicaties « ongecodeerd » aan de « erkende diensten » te leveren.

Deze gegevens omvatten (mobiel) telefoonverkeer, e-mail, faxverkeer en telexberichten, de gegevensstroom op het internet, zowel met betrekking tot het kennis nemen van de inhoud van de telecommunicatie als met betrekking tot gegevens inzake het verkeer, maar ook van elk signaal dat uitgaat van de persoon die in de gaten wordt gehouden.

De gegevens hebben betrekking zowel op de persoon die onder toezicht staat als op de personen die de betrokkene oproepen of door hem worden opgeroepen.

Voorts bepaalt deze resolutie dat de geografische lokalisatie van de mobiele gebruiker een gegeven is waartoe de bevoegde diensten toegang moeten hebben.

Onlangs heeft het Parlement, dat ter zake de gevolgen trekt uit de goedkeuring van het Verdrag van Amsterdam door de Europese Unie, vragen gesteld bij deze resolutie die in alle haast en zonder parlementaire controle is aangenomen. Het is interessant dat de resolutie d.d. 16 september 1998 van het Europees Parlement precies betrekking had op de transatlantische verhoudingen en in het bijzonder op Echelon. Deze resolutie besluit dat, niettegenstaande het bestaan van dergelijke relaties en de veronderstelde doelstellingen van Echelon, « het essentieel is dat men kan steunen op democratische controlesystemen met betrekking tot het gebruiken van deze technologieën en de verkregen informatie ».

De aanbevelingen van deze resolutie zijn nog duidelijker.

Het Europees Parlement :

« 12 ... vraagt dat dergelijke bewakingstechnologieën van het voorwerp zijn van een echt open debat op nationaal vlak en op het niveau van de Europese Unie, en onderworpen worden aan procedures die een aansprakelijkheid garanderen op democratisch vlak;

13 ... eist dat een gedragscode wordt goedgekeurd die garandeert dat fouten of misbruiken worden goedgemaakt;

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

15 ... charge son président de transmettre la présente résolution, à la Commission, au Conseil et au Congrès américain. »

Le 3 mai 1999, le Groupe de protection des personnes à l'égard du traitement des données personnelles (1) émettait une recommandation concernant le respect de la vie privée dans le contexte de l'interception des télécommunications (2).

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

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

Au-delà, la recommandation insiste sur les obligations des opérateurs et fournisseurs de télécommunications de prévoir toutes les mesures de sécurité (3) ainsi que le cryptage systématique des messages afin

14 ... meent dat het toenemend belang van internet en, meer in het algemeen, van telecommunicatie op wereldschaal en in het bijzonder het systeem Echelon, alsmede de risico's van hun bedrieglijk gebruik, het noodzakelijk maken dat er maatregelen worden genomen met het oog op het beschermen van economische informatie en dat er een doeltreffend coderingssysteem in gebruik wordt genomen;

15 ... belast de voorzitter ermee deze resolutie ter kennis te brengen van de Commissie, de Raad en het Amerikaanse Congres. »

Op 3 mei 1999 formuleerde de Groep voor de bescherming van personen i.v.m. de verwerking van persoonsgegevens (1) een aanbeveling betreffende de eerbied voor de persoonlijke levenssfeer in de context van het intercepteren van telecommunicatie (2).

Deze aanbeveling grijpt terug naar het beginsel van het geheim van de communicatie en wijst er op dat dit geheim wordt verzekerd door de richtlijn 97/66/EG die voor de lidstaten een verplichting creëert tot het waarborgen van het geheim van de communicatie die verloopt via een openbaar telecommunicatienetwerk of via telecommunicatiediensten die toegankelijk zijn voor het publiek.

Artikel 14 § 1 van de richtlijn 97/66/EG bepaalt dat de lidstaten deze verplichting tot vertrouwelijkheid van de communicatie op openbare netwerken slechts mogen beperken indien dit noodzakelijk is voor het vrijwaren van de veiligheid van de staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Indien er dus al een uitzondering is, wordt ze strikt geïnterpreteerd en veronderstelt ze dat afluisteren het absoluut noodzakelijke middel is om de beoogde doelstelling te verwezenlijken.

Voorts legt deze aanbeveling de nadruk op de verplichtingen van de exploitanten en leveranciers van telecommunicatie om alle beveiligingsmaatregelen te voorzien (3), waaronder het systematisch coderen

---

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

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

(3) Il s'agit du principe général de sécurité des données, affirmé par l'article 7 de la Convention du Conseil de l'Europe nº 108, par l'article 17 § 1 et § 2 de la directive 95/46 et par les articles 4,5 et 6 de la directive 97/66/CE.

(1) Deze groep is opgericht krachtens artikel 29 van de richtlijn 95/46. Zijn bevoegdheid is louter raadgevend.

(2) Aanbeveling 2/99 document 5005/99/final W.P. 18. De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer lag aan de oorsprong van deze aanbeveling. Ze werd gevat in 1998 door een brief van de toenmalige Belgische minister van Justitie.

(3) Het gaat om het algemeen beginsel van de beveiliging van gegevens, bekrachtigd door artikel 7 van het Verdrag van de Raad van Europa nr. 108, door artikel 17 §1 en 2 van de richtlijn 95/46 en door de artikelen 4, 5 en 6 van de richtlijn 97/66/EG.

de rendre techniquement difficile ou impossible, selon l'état actuel de la technique, l'interception des télécommunications par des instances non autorisées par la loi.

Le groupe souligne à cet égard que la mise en œuvre de moyens efficaces d'interception des communications à des fins légitimes, utilisant précisément les techniques les plus avancées, ne doit pas avoir pour conséquence d'abaisser le niveau général de confidentialité des communications et la protection de la vie privée des individus.

Ces obligations prennent un sens particulier dans le cas où les télécommunications entre des personnes situées sur le territoire des États membres transitent ou peuvent transiter hors du territoire européen notamment lors de l'utilisation de satellites ou d'Internet(1).

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

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

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

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

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

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

— le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités

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

van de berichten, teneinde het intercepteren van telecommunicatie door bij wet niet-gemachtigde instanties technisch moeilijk of onmogelijk te maken, rekening houdend met de huidige staat van de techniek.

In verband hiermee benadrukt de groep dat de aanwending van doeltreffende middelen voor het intercepteren van communicatie met wettelijke doeleinden, waarbij precies gebruik wordt gemaakt van de meest gesofistikeerde technieken, er niet toe mag leiden dat het algemeen niveau van vertrouwelijkheid van de communicatie en de bescherming van de persoonlijke levenssfeer van individuen wordt beperkt.

Deze verplichtingen krijgen bijzondere betekenis in het geval waarin de telecommunicatie tussen personen die zich op het grondgebied van de lidstaten bevinden, dit Europese grondgebied (kan) verlaten, met name wanneer gebruik wordt gemaakt van satellieten of van het internet(1).

De aanbeveling besluit met het opsommen van een reeks voorwaarden betreffende eender welke vorm van intercepteren van telecommunicatie. We nemen de tekst hierna over.

«Het is van belang dat het nationaal recht nauwkeurig en met naleving van alle bovenstaande bepalingen de volgende elementen beschrijft:

— De overheden bevoegd om de wettelijke interceptie van telecommunicatie toe te laten, de diensten bevoegd om intercepties te verrichten en de wettelijke grond van hun interventie,

— De doelstellingen waarvoor dergelijke intercepties mogen plaatsvinden, die het mogelijk maken te beoordelen of ze in verhouding staan tot de nationale belangen die op het spel staan,

— Het verbod op eender welke verkennende of algemene controle van telecommunicatie op grote schaal;

— De precieze omstandigheden en voorwaarden (bv.: feitelijke elementen die de maatregel wettigen, duur van de maatregel) waaraan de intercepties onderworpen zijn, met eerbied voor het beginsel van specificiteit waaraan elke inmenging in andermans privéleven is onderworpen,

— De eerbied voor dit beginsel van specificiteit, gevolg van het verbod op eender welke verkennende of algemene controle, impliceert meer in het bijzonder met betrekking tot de gegevens inzake verkeer dat de

(1) Op dit punt verwijst de aanbeveling naar artikel 25 van de richtlijn dat verbiedt dat eender welke communicatiestroom loopt naar landen die geen passende bescherming bieden.

publiques ne peuvent avoir accès à ces données qu'au cas par cas, et non de façon générale et proactive;

— les mesures de sécurité en ce qui concerne le traitement et le stockage des données, et leur durée de conservation;

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

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

— les types de recours que peut exercer la personne surveillée;

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

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

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

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

Sans vouloir revenir sur les péripéties de la naissance et du vote de la loi organique des services de renseignement et de sécurité (Sénat n^{os} 1-758/10, 11 et 15, *Moniteur belge* du 18 décembre 1998)(1), on peut considérer que finalement le législateur belge a entendu faire siennes les demandes réitérées du Conseil d'État et de la jurisprudence belge qui depuis 1990 rappelaient avec énergie la jurisprudence constante de la Cour européenne des droits de l'homme pour dénier tout droit de la Sûreté de l'État et des services de renseignement à la collecte et aux traite-

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

publieke overheden slechts van geval tot geval toegang hebben tot deze gegevens, en dus niet op algemene en proactieve wijze.

— De beveiligingsmaatregelen m.b.t. het verwerken en opslaan van de gegevens, en de duur tijdens dewelke ze worden bewaard.

— Met betrekking tot de personen die op indirecte of wisselvallige wijze bij het afluisteren zijn betrokken, de bijzondere waarborgen betreffende de verwerking van persoonsgegevens : met name, de criteria die de bewaring van de gegevens wettigen en de voorwaarden voor de communicatie van deze gegevens aan derden;

— De bewaakte persoon op de hoogte brengen, zodra dit mogelijk is;

— De vormen van verhaal die de bewaakte persoon mag uitoefenen.

— De controlemodaliteiten op deze diensten door een onafhankelijke controlerende overheid;

— De openbaarheid — bijvoorbeeld in de vorm van periodieke statistische verslagen — van het effectief gevoerde beleid inzake de interceptie van telecommunicatie;

— De precieze voorwaarden waarin de gegevens aan derden mogen worden meegedeeld in het kader van bilaterale of multilaterale akkoorden. »

5.3. Ten derde : met betrekking tot het intercepteren van telecommunicatie neemt de Belgische wetgeving de beginselen van de Raad van Europa over, zonder ze echter voldoende om te zetten

Zonder dat we willen terugkomen op alle verwikkelingen rond het ontstaan en de goedkeuring van de organieke wet over de inlichtingen- en veiligheidsdiensten (Senaat nrs. 1-758/10, 11 en 15, *Belgisch Staatsblad* van 18 december 1998)(1), kunnen we stellen dat de Belgische wetgever zich eindelijk heeft voorgenomen om de herhaalde vragen van de Raad van State en van de Belgische rechtspraak over te nemen, die al sinds 1990 krachtig wezen op de vaststaande rechtspraak van het Europees Hof voor de rechten van de mens teneinde elk recht van de Staats-

(1) Zie in verband hiermee : Yves Poullet, B. Havelange, « Secrets d'État et Vie Privée ou Comment concilier l'inconciliable? », Internationaal colloquium « Staatsgeheim of transparantie? » d.d. 20 januari 1999 georganiseerd door het Comité I, Brussel, gepubliceerd in *« Droit des technologies de l'Information et de la Communication »*, Regards Prospectifs, E. Montero (uitg.), Cahier du CRID nr. 16, Bruylant, Brussel, 1999, blz. 233.

ments d'informations vis-à-vis de citoyens ou de manière plus large d'individus (1):

« Considérant que l'article 8, § 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales permet l'ingérence de l'autorité publique dans l'exercice du droit de toute personne au respect de sa vie privée, pour autant que cette ingérence est conforme à la loi, qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, notamment à la sécurité nationale et à la sûreté publique, et que les textes qui la prévoient soient accessibles à l'intéressé et rédigés en termes assez clairs pour lui indiquer de manière adéquate quelles circonstances et sous quelles conditions, ils habilitent la puissance publique à s'y livrer, spécialement si l'ingérence présente un caractère secret » (arrêt Wicart du Conseil d'État (30 juin 1995, arrêt nº 54-139).

Ainsi, la loi organique, par touches successives depuis le projet initial, a défini avec précision tant les activités qui menacent ou peuvent menacer la sécurité de l'État, que les intérêts qui doivent être protégés contre ces menaces (2).

Comme le notait d'emblée l'exposé des motifs du projet de loi organique: « Les respect et la protection des droits et libertés individuels ainsi que le développement démocratique de la Société doivent toujours guider l'action des services de renseignements et de sécurité. Ce principe fonde la légitimité de leur action et est rappelé aux articles 6 et 8 du projet » (3).

(1) *Cf.* également l'avis de la Commission de Protection de la Vie Privée relative au projet de loi organique des services de renseignements et de sécurité, avis nº 12/98 du 23 mars 1998.

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

(3) Exposé des motifs. Projet de loi organique des services de renseignements et de sécurité, Chambre des représentants, session ordinaire, 2 juillet 1996, Doc. Parl., nº 638/1, 95/96, p. 3.

veiligheid en van de inlichtingendiensten te betwisten op het inzamelen en verwerken van gegevens ten overstaan van burgers of meer in het algemeen van individuen (1):

« Overwegende dat artikel 8, § 2, van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden de inmenging toelaat van de publieke overheid in de uitoefening van het recht van elk individu op de eerbied voor zijn persoonlijke levenssfeer, voor zover deze inmenging conform de wet is, dat ze een maatregel vormt die in een democratische samenleving noodzakelijk is, met name voor de nationale en de openbare veiligheid, en dat de teksten die deze inmenging voorzien toegankelijk zijn voor de betrokkene en voldoende duidelijk zijn opgesteld om hem op passende wijze aan te geven in welke omstandigheden en onder welke voorwaarden ze de openbare macht de toelating geven daartoe over te gaan, in het bijzonder indien de inmenging van geheime aard is » (arrest-Wicart van de Raad van State, 30 juni 1995, arrest nr. 54-139).

Zo geeft deze organieke wet, in opeenvolgende fasen vanaf het oorspronkelijk ontwerp, een precieze beschrijving niet alleen van de activiteiten die de veiligheid van de Staat bedreigen of kunnen bedreigen, maar ook van de belangen die tegen deze bedreigingen moeten worden beschermd (2).

In de memorie van toelichting van het ontwerp van organieke wet stond al: « De eerbied voor en de bescherming van de individuele rechten en vrijheden alsmede de democratische ontwikkeling van de samenleving moeten te allen tijde de werking van de inlichtingen- en veiligheidsdiensten leiden. Dit beginsel vestigt de wettelijkheid van hun actie en wordt opnieuw aangehaald in de artikelen 6 en 8 van het ontwerp » (3).

(1) Zie ook het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer met betrekking tot het ontwerp van organieke wet over de inlichtingen- en veiligheidsdiensten, Advies nr. 12/98 d.d. 23 maart 1998.

(2) Zie in verband hiermee de opmerkingen van de heer van Lysebeth, administrateur-generaal van de Veiligheid van de Staat, tijdens zijn verhoor in de Senaat, Doc. Senaat, 1997-1998, Doc. I/758/10, blz. 62 en volgende.

(3) Memorie van toelichting. Ontwerp van organieke wet over de inlichtingen- en veiligheidsdiensten, Kamer van volksvertegenwoordigers, gewone zitting 2 juli 1996, Doc. Parl. nr. 638/1, 95/96, blz. 3.

Certes en ce qui concerne le sujet qui nous occupe, on regrettera avec le Comité R(1) que la loi organique, même si elle rappelle à suffisance les principes de la jurisprudence du Conseil de l'Europe, ne prenne soin d'appliquer ces principes de manière précise aux écoutes téléphoniques(2) par les services de renseignements et de sécurité voire établisse des principes communs à toutes les formes d'interception qu'elles soient opérées dans le cadre d'une instruction criminelle par les autorités de police, de gendarmerie ou judiciaires ou par les Services de renseignement et de sécurité(3).

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

Le gouvernement américain(4) répond aux interrogations européennes du Parlement européen en faisant valoir sa soumission à l'amendement nº 4 de la Constitution américaine compris dans le fameux Bill of Rights(5).

---

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

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

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

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

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

Toegegeven, met betrekking tot het onderwerp van het onderhavige rapport betreuren we samen met het Comité I(1) dat de organieke wet de beginselen van de rechtspraak van de Raad van Europa, waarnaar ze nochtans voldoende verwijst, niet duidelijk toepast op het afluisteren van telefoonverkeer(2) door de inlichtingen- en veiligheidsdiensten, of zelfs geen gemeenschappelijke principes vastlegt voor elke vorm van interceptie, ongeacht of deze plaatsvindt in het kader van een strafrechtelijk onderzoek door de politie, de rijkswacht, de gerechtelijke overheden of door de inlichtingen- en veiligheidsdiensten(3).

5.4. Ten vierde : De Verenigde Staten lijken de hierboven beschreven beginselen niet na te leven

In haar antwoord op de vragen van het Europees Parlement beroept de Amerikaanse regering(4) zich op haar onderwerping aan het 4e amendement van de Amerikaanse Grondwet, dat deel uitmaakt van de beroemde « Bill of Rights »(5).

---

(1) Zie in verband hiermee de aanbevelingen van het Comité I in zijn jaarverslag van 1996, Titel II, Hoofdstuk 2, blz. 47, in het jaarverslag van 1997, 2e deel, hoofdstuk 1, Afdeling 3, blz. 99 en tot slot in het jaarverslag van 1998, deel II, B, hoofdstuk 1, blz. 102. We verwijzen in het bijzonder naar de besluiten in het jaarverslag van 1996 : « Met het oog op de doeltreffendheid van de inlichtingendiensten kan het Comité niet anders dan goedkeuren dat het voornemen bestaat om aan deze diensten wettelijke mogelijkheden inzake het afluisteren en intercepteren van telecommunicatie te verlenen. Met het oog op de bescherming van de rechten van personen kan het Comité niet goedkeuren dat dit middel om inlichtingen in te winnen wordt verleend zonder het gepaard te laten gaan met strikte waarborgen en voorwaarden inzake toezicht. »

(2) We wijzen hier toch op de uitzondering gevormd door artikel 44 van de organieke wet. Dit artikel laat de Algemene Dienst inlichting en veiligheid van de Krijgsmacht toe militaire radioverbindingen uitgezonden in het buitenland te onderscheppen, af te luisteren, er kennis van te nemen of op te nemen, maar uitsluitend om redenen van militaire aard. Met betrekking tot deze uitzondering en de argumentatie *a contrario* waartoe deze enige wettelijke uitzondering uitnodigt naar aanleiding van andere gevallen van afluisteren door de inlichtingen- of veiligheidsdiensten, lees Y. Poullet en B. Havelange, voornoemd artikel.

(3) We vestigen de aandacht op de aanbeveling van het Comité I in zijn jaarverslag van 1997. Wij (Y. Poullet, B. Havelange, voornoemd artikel) pleitten in dezelfde zin.

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

(5) De tekst van de « Bill of Rights » is te vinden op de website http://lcweb2.loc.gov/const/bor.html.

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

Il n'est pas certain que l'interprétation du texte de l'amendement nº 4 soumette la NSA aux mêmes exigences que celles imposées par la jurisprudence européenne.

De l'analyse des documents présentant la NSA (1), il ressort certes que les activités de la NSA sont soumises à la fois à la Constitution, la loi fédérale (2), les réglementations de l'exécutif et du département de la défense et qu'une procédure « effective » de surveillance menée à la fois par le President's Intelligence Oversight Board (IOB) et les Comités de contrôle des congrès (composés à la fois de représentants du Sénat et de la Chambre des représentants) permet à ces organes d'être informés des activités de la NSA et veille en particulier au respect du droit à la vie privée des citoyens américains.

(1) *Cf.* en particulier, le site du NSA et en particulier les pages relatives aux FAQ http://www.NAS.gov/about nsa/faq8.internet.html. Nous reprenons ci-après le texte de la réponse à deux questions essentielles dans le contexte qui nous occupe :

« How are the activities of NSA/CSS regulated ?

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

How is compliance with the regulations monitored ?

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

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

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

Het is niet zeker dat de interpretatie van de tekst van het 4e amendement het NSA onderwerpt aan dezelfde vereisten als de vereisten die de Europese rechtspraak oplegt.

Uit de analyse van de documenten waarin het NSA wordt voorgesteld (1), blijkt wel dat de activiteiten van het NSA zijn onderworpen aan de Grondwet, de federale wet (2), de reglementeringen van de uitvoerende macht en van het ministerie van Defensie. Voorts laat een « effectieve » procedure van toezicht, die tegelijk wordt gevoerd door de President's Intelligence Oversight Board (IOB) en door de controlecomités van het Congres (waartoe leden van de Senaat en van de Kamer van volksvertegenwoordigers behoren), deze organismen toe op de hoogte te blijven van de activiteiten van het NSA en in het bijzonder toe te zien op de eerbied voor het recht op de persoonlijke levenssfeer van de Amerikaanse burgers.

(1) Zie in het bijzonder de website van het NSA en vooral de FAQ-bladzijden : http://www.Nas.gov/about nsa/faq8.internet.html. We nemen hierna de tekst over van het antwoord op twee vragen die essentieel zijn in de context die ons bezighoudt :

« How are the activities of NSA/CSS regulated ?

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

How is compliance with the regulations monitored ?

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

(2) Het gaat om de Foreign Intelligence Surveillance Act (FISA) van 1978, die betrekking heeft op activiteiten inzake spionage en contraspionage (Intelligence and Counterintelligence). Elliott (bovengenoemd rapport, blz. 12) : afluisteroperaties kunnen worden toegelaten krachtens een « Presidential Order » en indien het gaat om het afluisteren van vreemde mogendheden; de communicatie die wordt afgeluisterd moet niet noodzakelijk in verband staan met een « crime » (misdaad) : aanvallen, sabotage, terrorisme, spionageactiviteiten ...

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

En conclusion, la protection des citoyens, à supposer qu'elle soit comparable, équivalente ou adéquate vis-à-vis des exigences européennes, n'existe que pour les citoyens américains. Cette limite est d'autant plus significative que les législations américaines protectrices des citoyens, ainsi le Privacy Act de 1974 et le Freedom of Information Act de 1966, ne concernent également que les seuls citoyens américains (1).

6. CONCLUSIONS

6.1. De l'existence du réseau Échelon

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

6.2. De la capacité technique du réseau Échelon

Échelon peut capter la totalité du trafic satellitaire à destination de l'Europe. La NSA, un des services secrets américains qui serait présent sur la base anglaise possède un budget et un personnel plus important que Belgacom.

(1) À cet égard, la réponse d-à la FAQ: « Does NSA/CSS unconstitutionally « spy on » or garget ? » The NSA/CSS performs SIGINT operations against foreign powers or agents of foreign powers. We strictly follow laws and regulations designed to preserve every American's privacy rights under the Fourth Amendment to the United States Constitution. The Fourth Amendment protects US persons from unreasonable searches and seizures by the US Government or any person or agency acting on behalf of the US Government ». A noter, dans le même sens, la réponse du ministre britannique interrogé à propos des interceptions et de la protection des citoyens, le ministre se montre rassurant vis-à-vis de la protection des seuls citoyens anglais (*supra*, nº 1, 2).

We kunnen ons afvragen of deze organismen zonder uitstel kennis krijgen van en toezicht uitoefenen op de activiteiten van het NSA. Dat staat lang niet vast, aangezien uit de bronnen die we konden raadplegen, blijkt dat dit toezicht verloopt via het Office of the Inspector General (OIG). Dit bureau verricht de inspecties, onderzoeken en audits die nodig zijn om na te gaan of de uitvoering van de NSA-activiteiten wettelijk verloopt. Het OIG stelt verslagen van zijn opdrachten op ten behoeve van de bovengenoemde overheden.

Tot besluit kunnen we stellen dat de bescherming van de burgers, aangenomen dat ze vergelijkbaar, gelijkwaardig of passend is in vergelijking met de Europese vereisten, alleen geldt voor Amerikaanse burgers. Deze beperking is van des te meer betekenis omdat ook de Amerikaanse wetten tot bescherming van de burgers — de Privacy Act van 1974 en de Freedom of Information Act van 1966 — alleen betrekking hebben op Amerikaanse burgers (1).

6. BESLUITEN

6.1. Over het bestaan van Echelon

Volgens ons is het duidelijk dat het netwerk Echelon bestaat en dat de Engelse basis Menwith Hill in Yorkshire (Engeland) daarvan een belangrijke schakel is. Op de basis werken meer dan duizend Amerikanen en iets meer dan vijfhonderd Engelsen. Er werken Engelsen op alle niveaus van de basis, hetgeen door de Britse regering wordt voorgesteld als een garantie van het feit dat er op deze basis geen activiteiten plaatsvinden die nadelig zijn voor het Verenigd Koninkrijk of voor Britse burgers. De basis ontsnapt aan de parlementaire controle op het terrein, ook al hebben Britse ministers in het verleden nu en dan antwoord gegeven op bepaalde parlementaire vragen.

6.2. Over de technische capaciteiten van Echelon

Echelon kan alle satellietverkeer bestemd voor Europa opvangen. Het NSA, een Amerikaanse geheime dienst die op de Engelse basis aanwezig zou zijn, beschikt over een groter budget en telt meer werknemers dan Belgacom.

(1) Zie in verband hiermee het antwoord op de FAQ: « Does NSA/CSS unconstitutionally « spy on » or target Americans ? The NSA/CSS performs SIGINT operations against foreign powers or agents of foreign powers. We strictly follow laws and regulations designed to preserve every American's privacy rights under the Fourth Amendment to the United States Constitution. The Fourth Amendment protects US persons from unreasonable searches and seizures by the US Government or any person or agency acting on behalf of the US Government. » Het antwoord van de Britse minister, ondervraagd over de intercepties en de bescherming van de burgers, gaat in dezelfde zin. Hij toont zich alleen geruststellend met betrekking tot de bescherming van Engelse burgers (*cf. supra*, nr. 1.2).

Ses capacités de déchiffrement sont gigantesques et l'histoire récente tend à prouver qu'elles sont minimalisées d'au moins un facteur mille à dix mille dans les déclarations publiques des services américains. Par ailleurs, toute technologie américaine (software et hardware) licitement exportée vers l'Europe est considérée par de nombreux experts, — et nous partageons cet avis —, comme intrinsèquement et volontairement sujette à une surveillance aisée, à distance et discrète par les services américains.

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

6.3. Des activités du réseau Échelon

Que font les 1 800 personnes travaillant à Menwith Hill ? Les signataires du présent rapport sont incapables de répondre à cette question. Les cas d'espionnage industriel dévoilés principalement par la France vis-à-vis d'entreprises françaises n'ont pas à ce jour été démontrés. Ils ne le seront probablement jamais tant les technologies d'écoute actuelles laissent peu de traces.

Tant les Américains que les Anglais ont démenti que ce réseau soit utilisé à des fins d'espionnage économique (ce qui revient à admettre son existence et ses capacités à le faire).

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

Nous tenons ici à souligner avec vigueur qu'il est impossible de connaître avec certitude ce que fait ou ce que ne fait pas le réseau Échelon.

Selon Bamford(1), « Il est hautement improbable qu'Échelon surveille tout le monde partout comme les critiques le proclament. Il serait impossible à la NSA d'intercepter toutes les communications. L'agence a connu d'importantes réductions de personnel au

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

Het beschikt over enorme decoderingscapaciteiten. De recente geschiedenis toont aan dat de Amerikaanse diensten deze capaciteiten in publieke verklaringen met een factor van ten minste duizend tot tienduizend verminderen. Overigens zijn vele experten — met wie wij het eens zijn — van mening dat alle Amerikaanse technologie (software en hardware) die op wettige wijze naar Europa wordt uitgevoerd intrinsiek en doelbewust is onderworpen aan een gemakkelijke en discrete controle vanop afstand door de Amerikaanse diensten.

De huidige technologie maakt het verkennend en veralgemeend toezicht mogelijk, op basis van een woordenboek van sleutelwoorden, van ongecodeerde e-mail en in bepaalde mate van het faxverkeer, op de uitdrukkelijke voorwaarde dat deze telecommunicatie via satellieten verloopt. Dit verkennend en veralgemeend toezicht op telefoonverkeer per satelliet (ongeveer één procent van alle internationaal telefoonverkeer) is niet mogelijk met de huidige stand van de technologie. Het is wel mogelijk een particulier spreker te herkennen aan de hand van zijn stemafdruk.

6.3. Over de activiteiten van het Echelon-netwerk

Wat doen de 1 800 werknemers op Menwith Hill ? De opstellers van dit rapport blijven het antwoord op deze vraag schuldig. Tot op heden zijn geen bewijzen geleverd van gevallen van industriële spionage ten nadele van Franse ondernemingen, die in hoofdzaak door Frankrijk werden aangevoerd. Wellicht zullen er nooit bewijzen worden gevonden, aangezien de huidige afluistertechnologieën zo goed als geen sporen nalaten.

Zowel de Amerikanen als de Engelsen ontkenden dat Echelon wordt gebruikt voor industriële spionage (al gaven ze met die verklaring toe dat het netwerk bestaat en tot industriële spionage in staat is).

Toch blijven er grote twijfels bestaan, niet alleen bij parlementsleden en burgers, maar ook bij Europese telecommunicatie-experten. Eén derde van hen gelooft dat grote mogendheden zich aan industriële spionage overgeven, terwijl twee derde dat niet gelooft of hierover zich niet kan uitspreken.

We leggen grote nadruk op het feit dat het onmogelijk is zekerheid te hebben over wat Echelon doet of niet doet.

Volgens Bamford(1) « is het uiterst onwaarschijnlijk dat Echelon de hele wereld bewaakt, zoals critici beweren. Het NSA zou onmogelijk alle communicatie kunnen intercepteren. De laatste vijf jaar is het personeelsbestand van het bureau sterk verminderd,

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

cours des cinq dernières années alors que ses cibles pour la sécurité nationale ont augmenté en nombre: le déploiement des missiles nord-coréens, les essais nucléaires en Inde et au Pakistan, la circulation de présumés terroristes, etc. Être à l'écoute du business européen en vue d'aider des sociétés américaines ne serait qu'une mission de faible priorité. Et transmettre le produit d'interceptions secrètes à des compagnies serait rapidement découvert».

Par contre, il est possible d'établir une évaluation raisonnable des possibilités minimales d'interception d'Échelon. Au nom des principes de précaution et de souveraineté, la description des capacités d'un tel réseau suffit ici amplement à justifier l'intervention de l'État.

6.4. De la légalité de l'interception des télécommunications

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

Ces principes généraux exigent que les interceptions

— aient lieu sur base d'un fondement légal, définissant avec précision les finalités de telles interceptions;

— ne puissent en aucune manière être opérées de manière générale et exploratoire;

— menées dans ce cadre fassent l'objet d'un contrôle par une instance indépendante.

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

6.5. Des enjeux de la sécurité des télécommunications

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

Le premier concerne l'écoute politique menée par des partis politiques au pouvoir ou des membres de ceux-ci afin d'espionner les adversaires politiques. On peut rappeler le scandale du Watergate ou les écoutes effectués par l'Élysée en France.

Il reste extrêmement tentant pour un parti au pouvoir de surveiller ses adversaires démocratiques

terwijl zijn doelwitten met betrekking tot de nationale veiligheid zijn toegenomen: plaatsing van raketten in Noord-Korea, nucleaire tests in India en Pakistan, het verkeer van vermeende terroristen enz. Het Europese bedrijfsleven afluisteren om Amerikaanse ondernemingen te helpen zou een opdracht met lage prioriteit zijn. Bovendien zou het bezorgen van de geïntercepteerde geheime informatie aan bedrijven snel worden ontdekt».

Het is daarentegen wel mogelijk een redelijke evaluatie te maken van de minimale interceptiecapaciteiten van Echelon. In naam van de beginselen van zorgvuldigheid en soevereiniteit volstaat de beschrijving van de capaciteiten van een dergelijk netwerk hier ruimschoots om de tussenkomst van de Staat te rechtvaardigen.

6.4. Over de wettelijkheid van het intercepteren van telecommunicatie

Blijkbaar hebben Europa en België de algemene beginselen van de rechtspraak van de Raad van Europa, die de interceptie van telecommunicatie in aanzienlijke mate beperken, grotendeels overgenomen.

Deze algemene beginselen vereisen dat de interceptie:

— plaatsvinden op grond van een wettelijke basis, die de finaliteiten van dergelijke intercepties precies beschrijft;

— nooit op algemene en verkennende wijze mogen plaatsvinden;

— die binnen dit kader plaatsvinden het voorwerp zijn van toezicht door een onafhankelijk organisme.

Het is helemaal niet zo evident dat de Amerikaanse wetgeving en reglementering dezelfde beginselen volgen en in het bijzonder de bescherming van niet-Amerikaanse burgers mogelijk maken.

6.5. Over de inzet van de beveiliging van telecommunicatie

Economische spionage en de bescherming van de persoonlijke levenssfeer zijn al vaak genoemd als een belangrijke inzet en we komen er niet meer op terug. Drie andere elementen verdienen het wel hier onder de aandacht te worden gebracht.

Het eerste element heeft betrekking op politieke afluisteroperaties door de regerende politieke partijen of van hun leden die politieke tegenstanders bespioneren. We verwijzen naar het Watergate-schandaal of naar de afluisteroperaties door het Élysée in Frankrijk.

Voor een regeringspartij is het heel verleidelijk haar democratische tegenstanders in de gaten te houden en

afin d'obtenir sur lui un avantage politique déterminant. Ce type d'écoute sape le jeu normal de la démocratie et tout État démocratique se doit de les empêcher.

Le deuxième enjeu est la confiance des citoyens dans leur réseau de télécommunication. Les pseudos capacités de ce réseau ont été amplifiées et déformées par la presse et il existe un risque croissant du développement d'une réticence à l'utilisation des réseaux, notamment dans le cadre du commerce électronique, mais aussi dans le cadre de l'utilisation d'internet à des fins non commerciales.

Nous pensons par exemple à l'utilisation d'internet pour la recherche d'informations politiques, médicales, religieuses, philosophiques, scientifiques ou culturelles et à la participation à des forums publics de discussion. Le sentiment d'être espionné, même en l'absence de tout fondement scientifique raisonnable, risque d'être un obstacle majeur au développement de l'utilisation des réseaux de télécommunication.

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

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

La sécurité des communications se situe donc bien au-delà du contrôle du trafic satellitaire ou des câbles des réseaux de télécommunication mais passe obligatoirement par le contrôle des logiciels et du matériel, notamment d'origine étrangère, utilisé lors des télécommunications.

Des instruments juridiques existent déjà à cet effet et même s'ils ont été sous-utilisés jusqu'à présent, il nous semble inutile de créer un nouveau dispositif légal contraignant. Des moyens techniques sont également disponibles. Les recommandations ci-après détaillent quelques-uns des raisons et des moyens d'agir.

Toutefois il ne faudrait pas, en tentant d'éviter la peste, attraper le choléra. Le réseau de télécommunication d'un état démocratique moderne doit pouvoir faire l'objet d'écoutes par des services autorisés, à certaines conditions et moyennant un certain contrôle.

Il nous semble exclu qu'existe un contrôle *a priori*, général et exploratoire de toutes les écoutes et il nous apparaît important que le comité de surveillance *ad hoc* puisse être informé de manière certaine du volume, des services responsables et de la finalité

zo een beslissend politiek voordeel te behalen. Dit soort afluisteroperaties ondermijnt echter het gewone spel van de democratie en elke democratische Staat is het aan zichzelf verplicht ze niet toe te laten.

Het tweede element betreft het vertrouwen van de burgers in hun telecommunicatienetwerk. De pers heeft de vermeende capaciteiten van dit netwerk opgeblazen en vervormd. Het risico dat de mensen steeds terughoudender worden om deze netwerken te gebruiken wordt groter, vooral in het kader van e-commerce maar ook met betrekking tot het gebruik van internet met niet-commerciële doeleinden.

We denken bijvoorbeeld aan het gebruik van internet bij het zoeken naar politieke, medische, religieuze, filosofische, wetenschappelijke of culturele informatie en aan de deelname aan publieke discussieplatformen. Het gevoel dat men bespioneerd wordt, zelfs wanneer daarvoor geen enkele redelijke wetenschappelijke grond bestaat, kan een belangrijke hinderpaal worden voor de ontwikkeling van het gebruik van telecommunicatienetwerken.

Het derde element houdt verband met het risico van de ordeloze verschijning van steeds betere technische coderingsoplossingen die de wettelijke interceptie van de inhoud van telecommunicatie moeilijk of zelfs onmogelijk maken.

6.6. Over de middelen om de veiligheid van telecommunicatie te verhogen in een democratische context

De veiligheid van de communicatie overstijgt dus de controle van het satellietverkeer of van de kabels van telecommunicatienetwerken, maar verloopt verplicht via de controle van software en hardware, vooral wanneer ze uit het buitenland komen, die worden gebruikt bij telecommunicatie.

Daartoe bestaan al juridische instrumenten en ook al zijn ze tot op heden niet ten volle aangewend, lijkt het ons niet nodig een nieuw dwingend geheel van wettelijke regels op te stellen. Er zijn ook technische middelen beschikbaar. In de onderstaande aanbevelingen gaan we nader in op een aantal redenen tot en middelen van handelen.

Toch moeten we er ons voor hoeden dat we in onze pogingen aan de pest te ontkomen door cholera te worden getroffen. Het telecommunicatienet van een moderne democratische staat moet door de bevoegde diensten kunnen worden afgeluisterd, onder bepaalde voorwaarden en met een bepaalde vorm van controle.

Het lijkt ons uitgesloten dat er een a-priorische, algemene en verkennende controle zou zijn op alle communicatie. Volgens ons is het belangrijk dat het comité van toezicht *ad hoc* op zekere wijze op de hoogte kan worden gehouden van de omvang, de ver-

générale (par exemple terrorisme, blanchiment, ...) des interceptions légales des télécommunications. Un droit ponctuel de regard, par rapport à certaines interceptions particulières, devrait également lui être accordé. En bref, nous plaidons pour que les conditions légales qui président à l'interception légale des télécommunications s'appliquent, *mutatis mutandis*, à la surveillance légale de ces interceptions. Faut-il rappeler qu'il s'agissait, dès 1996, d'une recommandation du Comité R (*cf. supra*, point 5.3)?

7. DE QUELQUES RECOMMANDATIONS

7.1. ... et de leur double fondement

Nos recommandations (*cf.* le point 6.2.) s'appuient sur un double fondement: le principe de précaution récemment mis en exergue par l'Union Européenne et considéré par elle comme une règle coutumière de droit international (1) est le premier.

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

Le principe de souveraineté «fonctionnelle» est le second fondement. Il représente «la manifestation de liberté et d'indépendance par laquelle l'État impose sa règle à ses nationaux et en impose le respect de la part des autres États» (2).

7.1.1. Le principe de précaution (3)

«Le principe de précaution devrait aussi consolider l'approche préventive en forçant les pouvoirs publics à agir alors même qu'ils ne disposent pas de toutes les

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

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

(3) *Erratum:* .....

antwoordelijke diensten en de algemene doelstellingen (bijvoorbeeld terrorisme, witwassen ...) van de legale intercepties van telecommunicatie. Met betrekking tot bepaalde bijzondere intercepties zou dit comité ook een specifiek controlerecht moeten genieten. Kortom, we zijn er voorstander van dat de wettelijke voorwaarden die de legale interceptie van telecommunicatie regelen, worden toegepast, *mutatis mutandis*, op het wettelijk toezicht op deze intercepties. Moeten we er nog op wijzen dat het Comité I deze aanbeveling al in 1996 heeft geformuleerd (*cf. supra*, punt 5.3.)?

7. ENKELE AANBEVELINGEN

7.1. ... en hun dubbele grondslag

Onze aanbevelingen (zie punt 6.2) steunen op een dubbele grondslag: de eerste is het zorgvuldigheidsbeginsel waarop de Europese Unie onlangs de nadruk heeft gelegd en dat door de Unie wordt beschouwd als een gewone internationale rechtsregel (1).

Dit beginsel bekrachtigt de plicht van de Staat om te handelen wanneer een risico, zelfs wanneer het onzeker is en de exacte omvang ervan onbekend is, zijn burgers bedreigt.

Het beginsel van «functionele» soevereiniteit is de tweede grondslag van onze aanbevelingen. Het gaat om «de uiting van vrijheid en onafhankelijkheid waarmee de Staat zijn regels aan zijn onderdanen oplegt alsook de eerbied ervoor vanwege de andere staten» (2).

7.1.1. Het zorgvuldigheidsbeginsel (3)

«Het zorgvuldigheidsbeginsel zou ook de preventieve benadering moeten consolideren door de overheid tot handelen te dwingen, zelfs als ze niet beschikt

(1) In verband hiermee verwijzen we de lezer naar de ontwikkelingen inzake de Europese argumentatie voor het OMC door Kowilsky en Viney in hun rapport aan de (Franse) eerste minister op 15 oktober 1999, La documentation française, blz. 115 en volgende: «Het voornaamste argument van de Europese Gemeenschappen is dat het zorgvuldigheidsbeginsel een gewone algemene internationale rechtsregel is (geworden), of ten minste een algemeen rechtsbeginsel ... De Europese instanties zijn van mening dat de toepassing van het zorgvuldigheidsbeginsel betekent dat het niet nodig is dat alle wetenschappers in de hele wereld het eens zijn over de mogelijkheid en de omvang van het risico ... De Verenigde Staten beschouwen het zorgvuldigheidsbeginsel niet als een gewone internationale rechtsregel. Volgens hen gaat het meer om een «benadering» dan om een «beginsel» ...»

(2) R. Wilkin, *«Dictionnaire du droit public»*, Brussel, Bruylant, 1963.

(3) *Erratum*: in bovenstaande tekst, zoals bezorgd aan de overheden, worden de termen«précaution» en «principe de précaution» ten onrechte vertaald als «zorgvuldigheid(-sbeginsel)». Gelieve deze te lezen als «voorzorg(-sbeginsel)» n.v.d.r.

preuves justifiant le bien-fondé de leur action» écrit N. de Saedeleer(1).

L'auteur, à la suite d'une doctrine et d'une jurisprudence nombreuse, distingue ainsi la prévention de la précaution. «Alors que la certitude appelle une attitude de prévention, son incertitude requiert la précaution».

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

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

Sans doute, le principe de précaution est-il habituellement évoqué à propos des soucis de protéger la santé, la sécurité humaine et l'environnement(2) mais l'extension aux exigences de protection de l'information personnelle et économique véhiculées par les correspondances privées ne devraient pas poser de difficultés tant il est déjà reconnu par l'organisation mondiale du commerce que les exigences de la protection de la vie privée pouvaient, à l'instar des préoccupations sanitaires, sécuritaires et environnementales, justifier une restriction légitime à la liberté des échanges.

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

«Le principe de précaution définit l'attitude que doit observer toute personne qui prend une décision concernant une activité dont on peut raisonnablement supposer qu'elle comporte un danger grave pour la santé ou la sécurité des générations actuelles ou futures, ou pour l'environnement. Il s'impose spécialement aux pouvoirs publics qui doivent faire prévaloir les impératifs de santé et de sécurité sur la liberté des échanges entre particuliers et entre États.

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

(2) Ainsi, le récent débat sur les OGM (sur ce point, le rapport de Kowilsky et Viney, p. 74 et suivantes).

over alle bewijzen die de gegrondheid van haar actie rechtvaardigt», schrijft N. de Saedeleer(1).

Na het bestuderen van de doctrine en een uitgebreide rechtspraak maakt de auteur een onderscheid tussen preventie en zorgvuldigheid. «Terwijl zekerheid aanleiding geeft tot een houding van preventie, vereist onzekerheid zorgvuldigheid.»

De auteur wordt nog preciezer: «Preventie houdt in dat men de nodige maatregelen neemt om ervoor te zorgen dat een voorzienbare of in elk geval waarschijnlijke gebeurtenis niet plaatsvindt. Ze vormt het middelpunt van een hele reeks juridische bepalingen inzake milieu, veiligheid, ihb veiligheid op het gebied van werk. Voorzorg betekent dat men nog meer doet en ofwel de veiligheidsmaatregelen vermenigvuldigt door verder te gaan dan wat de waarschijnlijkheid noodzakelijk maakt, ofwel veiligheidsmaatregelen neemt tegen risico's die zelfs niet waarschijnlijk zijn.»

De risico's die bewakingssystemen zoals Echelon vandaag en morgen vormen laten zich moeilijk meten. Ze zijn afhankelijk van een groot aantal onbekende parameters, de kracht van de codering, de omvang van de aangewende menselijke en technische middelen enzovoort.

Wellicht wordt gewoonlijk verwezen naar het zorgvuldigheidsbeginsel wanneer het gaat om de bescherming van de gezondheid, de menselijke veiligheid en het milieu(2). De uitbreiding van dit beginsel tot de vereisten inzake de bescherming van persoonlijke en economische gegevens die via particuliere correspondentie reizen zou geen moeilijkheden mogen veroorzaken. De wereldhandelsorganisatie erkent immers dat de vereisten inzake de bescherming van de persoonlijke levenssfeer, naar het voorbeeld van de bekommernis met betrekking tot gezondheid, veiligheid en milieu, een wettelijke beperking van de vrijheid van communicatie kunnen rechtvaardigen.

In hun rapport aan de Franse eerste minister beschrijven Kowilsky en Viney de gevolgen van het aannemen van het zorgvuldigheidsbeginsel:

«Het zorgvuldigheidsbeginsel beschrijft de houding die eenieder moet aannemen die een beslissing neemt over een activiteit waarvan men redelijkerwijze mag veronderstellen dat ze een ernstig gevaar vormt voor de gezondheid of de veiligheid van de huidige of toekomstige generaties, of voor het milieu. Het geldt in het bijzonder voor de overheid die aan de imperatieven inzake gezondheid en veiligheid voorrang moet geven boven de vrijheid van uitwisselingen tussen privépersonen en tussen Staten.

(1) N. de Sadeleer, *«Les principes du pollueur-payeur, de prévention et de précaution»,* Bruylant, 1999, blz. 395.

(2) Zie het recente debat over de «Genetisch gemodifieerde organismen»(GGO) (*cf.* het rapport van Kowilsky en Viney, blz. 74 en volgende).

Il commande de prendre toutes les dispositions permettant, pour un coût économiquement et socialement supportable, de détecter et d'évaluer le risque, de le réduire à un niveau acceptable et, si possible, de l'éliminer, d'en informer les personnes concernées et de recueillir leurs suggestions sur les mesures envisagées pour le traiter.

Ce dispositif de précaution doit être proportionné à l'ampleur du risque et peut être à tout moment révisé.» (1)

7.1.2. La souveraineté

La captation de messages transitant par satellites suscite des questions délicates. On sait que l'espace aérien (au-delà de 100 km) appartient au domaine public international et est affecté à l'usage commun de l'ensemble des États.

Le droit international autorise chaque État à effectuer des actes d'utilisation sans distinction et sur une base d'égalité (2).

La captation des transmissions se fait cependant au sol. Il s'exerce dans le cadre des actes de «souveraineté territoriale» (3) même s'il suppose une utilisation de l'espace atmosphérique et peut concerner des messages n'ayant aucun lien avec le territoire où s'effectue la captation.

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

(1) Kowilsky-Viney, *op. cit.*, p. 117.

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

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

Dit beginsel schrijft voor dat men alle schikkingen treft die het mogelijk maken, voor een economisch en maatschappelijk redelijk bedrag, het risico te ontdekken en te evalueren, het tot een aanvaardbaar niveau te verminderen en, indien mogelijk, het uit te schakelen, het ter kennis te brengen van de betrokken personen en hun suggesties te verzamelen met betrekking tot de maatregelen die men overweegt te nemen om het risico te verwerken.

Dit geheel van zorgvuldigheidsmaatregelen moet in evenredige verhouding staan met de omvang van het risico en kan te allen tijde worden herzien.» (1)

7.1.2. Soevereiniteit

Het opvangen van berichten die via satellieten worden verstuurd, roept heel wat delicate vragen op. We weten dat het luchtruim (hoger dan 100 km) tot het internationaal publiek domein behoort en is bestemd voor het gemeenschappelijk gebruik door alle Staten.

Krachtens het internationaal recht mag elke Staat het luchtruim zonder onderscheid en op voet van gelijkheid gebruiken (2).

Niettemin vindt het opvangen van transmissies op de grond plaats. Dit gebeurt in het kader van handelingen van «territoriale soevereiniteit» (3), zelfs al veronderstelt het een gebruik van de atmosfeer en kan het betrekking hebben op berichten die geen enkel verband houden met het grondgebied waar ze worden opgevangen.

Precies dit ontbreken van een mogelijk verband tussen de afluisterlijn en het afgeluisterd bericht, in combinatie met de macht die voortvloeit uit de kracht van informatie- en communicatietechnologieën, waardoor duizenden berichten kunnen worden opgevangen en verwerkt, zorgt voor problemen. Bij het aannemen van de organieke wet wees de minister van Landsverdediging op de gevaren die deze nieuwe technologieën creëerden: «de informatie- en communicatietechnologieën kunnen echte wapens worden, vernietigings- en afschrikkingsmiddelen.

(1) Kowilsky-Viney, *op. cit.*, blz. 117.

(2) *Cf.* het verdrag dat op 27 januari 1967 in werking trad en door de algemene vergadering van de Verenigde Naties is goedgekeurd. Het verdrag heeft betrekking op de beginselen tot regeling van de activiteiten van staten inzake de verkenning en het gebruik van de ruimte buiten de dampkring, met inbegrip van de maan en andere hemellichamen.

(3) Het gaat om de eerste omschrijving van het begrip «soevereiniteit», zoals het wordt verdedigd in de beroemde zaak-Lotus (beslissing d.d. 7 september 1927, Internationaal Gerechtshof in Den Haag, met name gepubliceerd in het *«Journal de droit international privé»*, 1927, blz. 1002 en volgende).

Voir les propos récents du Président Chirac à propos d'Helios: «la possibilité de voir au-delà de l'horizon est une nouvelle source de puissance géopolitique, comme l'arme atomique.» (1)

Bref, la captation abusive de messages par une personne étrangère risque de remettre en cause la souveraineté des États en tant cette fois qu'expression du principe d'indépendance de chaque État dans l'ordre international (2).

Que devient l'indépendance d'un État, si les secrets de ses administrations, de son gouvernement, de ses entreprises, de ses citoyens peuvent être décryptés en des lieux inconnus au profit de puissances étrangères du seul fait qu'ils pénètrent l'espace extra atmosphérique? L'absolue limitation des écoutes est fondamentale pour que survivent l'égalité et l'indépendance des États.

Enfin, la souveraineté des états n'est-elle pas remise en cause dans un autre sens encore? L'appartenance d'un individu à un État lui donne le droit de bénéficier d'une protection par son État des garanties et libertés constitutionnelles qui lui sont octroyées (3).

Ik verwijs naar de recente verklaring van president Chirac over Helios: «De mogelijkheid om verder dan de horizon te kijken is een nieuwe bron van geopolitieke macht, net als het atoomwapen.» (1)

Kortom, het bedrieglijk opvangen van berichten door een vreemdeling houdt het risico in dat er opnieuw vragen worden gesteld betreffende de soevereiniteit van staten, deze keer als uitdrukking van het beginsel van autonomie van elke Staat in de internationale orde (2).

Wat gebeurt er met de autonomie van een Staat wanneer de geheimen van zijn besturen, zijn regering, zijn ondernemingen en zijn burgers op onbekende plaatsen kunnen worden ontcijferd ten behoeve van vreemde mogendheden, enkel en alleen omdat deze geheimen buiten de dampkring en in de ruimte komen? De absolute beperking van afluisteroperaties is van wezenlijk belang opdat de gelijkheid en autonomie van Staten zouden overleven.

Tot slot kunnen we ons afvragen of de soevereiniteit van staten niet in nog een andere betekenis in twijfel wordt getrokken. Het feit dat een individu tot een Staat behoort, geeft hem het recht de bescherming vanwege zijn Staat te genieten van de waarborgen en vrijheden die hem krachtens de Grondwet worden verleend (3).

---

(1) Projet de loi organique, Exposé du ministre de la Défense nationale, in Rapport fait au nom des Commission réunies de la Justice et des Affaires étrangères; Séance 9 juillet 1999, Doc. Sénat nº 1 758/10, p. 7.

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

(3) «Il est vrai qu'il faut éviter toute pétition de principe et ne pas légitimer tout transfert, d'un point de vue constitutionnel, par le seul fait qu'il résulte d'un accord international en bonne et due forme. Il y a des limites objectives et des garanties nécessaires.

La première est qu'on ne peut transférer plus de pouvoir qu'on n'en a. La souveraineté nationale belge est limitée par les droits individuels. Il serait impossible de consentir par traité à des organes supranationaux, des pouvoirs qui limitent ces libertés» (P. Vigny, *Propos institutionnels*, Bruxelles, Bruylant, 1963, p. 117).

(1) Ontwerp van organieke wet, toelichting van de minister van Landsverdediging, in Verslag aan de verenigde commissies Justitie en Buitenlandse Zaken; zitting 9 juli 1998, Doc. Senaat, nr. 1 758/10, blz. 7.

(2) Zie in verband hiermee de opmerking van R. de Bottini, «*Souveraineté et conflits de lois*, in *La Souveraineté au 20e siècle*», Armand Colin (uitg.), 1971, blz. 145: «De reden van dit verzet heeft wellicht te maken met de dubbelzinnigheid van het begrip soevereiniteit, dat in het onderhavige geval twee duidelijk verschillende betekenissen kan hebben. Ten eerste kan men er het beginsel in zien van een soevereine afbakening van de wetgevende bevoegdheden van elke Staat; ze zou het mogelijk maken, in de ruimte, eenzijdig de grenzen te bepalen die elke wet kan hebben in tegenstelling tot alle andere nationale wetten. Het begrip soevereiniteit kan ook een trivialer betekenis hebben en niet meer zijn dan de uitdrukking van het beginsel van autonomie van elke Staat binnen de internationale orde.»

(3) Het is waar dat men elke *petitio principi* moet vermijden en, uit grondwettelijk oogpunt, niet elke transfer moet rechtvaardigen enkel en alleen omdat hij het gevolg is van een volgens de vorm opgemaakt internationaal akkoord. Er bestaan objectieve beperkingen en noodzakelijke waarborgen.

De eerste bepalen dat men niet meer macht kan overdragen dan men bezit. Individuele rechten beperken de Belgische nationale soevereiniteit. Het zou onmogelijk zijn bevoegdheden die deze vrijheden beperken krachtens een verdrag aan supranationale instellingen toe te staan» (P. Vigny, «*Propos institutionnels*», Brussel, Bruylant, 1963, blz. 117).

Ces garanties et libertés ne peuvent être remises en cause du seul fait que les technologies de l'information et de la communication abolissent les frontières physiques et que l'envoi d'un courrier électronique de Namur à Bruxelles peut transiter par les États-Unis, au seul gré des réseaux et sans que l'utilisateur n'en soit ni conscient, ni averti.

C'est sur base de telles considérations et au nom des valeurs essentielles que représente la défense des libertés des citoyens européens que la directive 95/46 relative à la protection des données interdit les flux vers les pays ne présentant pas un régime de protection adéquat (1).

En conclusion, la souveraineté étatique apparaît alors comme une obligation mise à charge de l'État de garantir dans le cyberespace le respect des libertés individuelles de ses citoyens.

Comme le note Wilkin (2):

« La souveraineté est une manifestation de liberté et d'indépendance par laquelle l'État impose la règle à ses nationaux et en exige le respect de la part des autres États. L'État dicte la volonté commune qu'il fait prévaloir contre les volontés particulières: il exprime à l'égard des nationaux et de l'étranger la souveraineté de la Belgique et veille à son respect. Vis-à-vis des autres États, la souveraineté est une manifestation d'indépendance; ...

(1) L'article 25 est commenté comme suit dans les considérants de la Directive:

Considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;

Considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

À propos de cet article, et en particulier de la notion de protection adéquate, lire Y. Poullet, B. Havelange « Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regards to the processing of personal data, European Commission, Annex to the annual report 1998 (XV D/5047/98) of the working party established by art 29 of the Directive 95/46/EC, DG XV, 1998.

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

Deze waarborgen en vrijheden mogen niet in het gedrang worden gebracht enkel en alleen omdat materiële grenzen door de informatie- en communicatietechnologieën worden afgebroken en de verzending van een e-mailbericht van Namen naar Brussel via de Verenigde Staten kan verlopen, afhankelijk van de netwerken en zonder dat de gebruiker zich daarvan bewust is of er kennis van krijgt.

Op grond van dergelijke overwegingen en in naam van de fundamentele waarden vertegenwoordigd door de bescherming van de vrijheden van de Europese burgers verbiedt de richtlijn 95/46 met betrekking tot de bescherming van gegevens de stromen naar landen die niet over een passend systeem van bescherming beschikken (1).

Tot besluit komt de soevereiniteit van een Staat naar voor als een verplichting voor deze Staat om de eerbied voor de individuele vrijheden van zijn burgers in de cyberspace te verzekeren.

Wilkin stelt vast (2):

« Soevereiniteit is een uiting van vrijheid en autonomie waarmee de Staat zijn regels aan zijn onderdanen oplegt alsook de eerbied ervoor vanwege de andere staten. De Staat dicteert de gemeenschappelijke wil waaraan hij voorrang geeft boven de wil van elk individu: ten overstaan van zijn onderdanen en van vreemdelingen drukt hij de soevereiniteit van België uit en ziet hij toe op de eerbied daarvoor. Ten overstaan van de andere staten is de soevereiniteit een uiting van onafhankelijkheid; ...

(1) In de consideransen van de richtlijn wordt artikel 25 als volgt becommentarieerd:

Overwegende dat grensoverschrijdend verkeer van persoonsgegevens voor de ontwikkeling van het inernationaal handelsverkeer noodzakelijk is; dat de door deze richtlijn in de Gemeenschap gewaarborgde bescherming van personen het doorgeven van persoonsgegevens naar derde landen die een passend beschermingsniveau waarborgen niet in de weg staat; dat bij de beoordeling van het door een derde land geboden beschermingsniveau rekening dient te worden gehouden met alle omstandigheden van doorgifte of een categorie doorgiften;

Overwegende dat daarentegen doorgifte van persoonsgegevens naar een derde land dient te worden verboden, indien daar geen passend beschermingsniveau wordt geboden;

In verband met dit artikel en in het bijzonder met betrekking tot het begrip « passende bescherming, » lees Y. Poullet, B. Havelange, « Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data, European Commission, Annex to the annual report 1998 (XV D/5047/98) of the working party established by art. 29 of the Directive 95/46/EC, DG XV, 1998.

(2) R. Wilkin, V° *« Souveraineté, Dictionnaire de droit public »*, Brussel, Bruylant, 1963.

La souveraineté de l'État n'est pas en soi un point d'aboutissement; elle est le moyen, pour les pouvoirs établis de pourvoir aux besoins des nationaux et d'assurer à ceux-ci et aux étrangers le libre exercice de leurs droits.»

7.2. Le chiffrement

Tout chiffrement induit des coûts liés au choix de l'algorithme de chiffrement, à sa distribution, à la génération de clés sécurisées et au chiffrement/déchiffrement lui-même qui implique du temps de calcul et donc une lenteur dans la circulation de l'information.

Même si un cryptage fort, combiné à l'utilisation de fibres optiques à chiffrement quantique, semble la voie royale menant à une sécurisation maximale des données, une telle solution ralentirait fortement le réseau et n'est pas envisageable partout dans le monde. Par ailleurs son coût risque d'être particulièrement élevé.

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

7.3. L'agréation des appareils terminaux

La directive 1999/5/CE du Parlement européen et du Conseil, du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité définit comme (article 2, *b)* «équipement terminal de télécommunications», un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications.

Un simple programme de navigation ou de courrier électronique ou encore un routeur peuvent donc être considérés comme équipements terminaux de télécommunication.

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

De soevereiniteit van de Staat is geen streefdoel op zich, maar is voor de gevestigde machten het middel te voldoen aan de behoeften van de onderdanen en jegens hen en vreemdelingen de vrije uitoefening van hun rechten te verzekeren».

7.2. Het coderen (vercijfering)

Elke codering veroorzaakt kosten die te maken hebben met de keuze van het coderingsalgoritme, de verspreiding ervan, het genereren van beveiligde sleutels en het coderen/decoderen zelf, waarvoor tijd nodig is, zodat de informatie trager circuleert.

Hoewel een sterke codering, gepaard gaand met het gebruik van glasvezels met kwantumcodering, het middel bij uitstek lijkt om gegevens zoveel mogelijk te beveiligen, zou een dergelijke oplossing grote vertragingen teweegbrengen op het netwerk. Bovendien kan ze niet overal ter wereld worden toegepast en bestaat de kans dat de kosten heel hoog oplopen.

Hoewel de telecomoperator de vertrouwelijkheid van de telecommunicatie moet verzekeren, moet deze algemene verplichting worden afgewogen met de staat van de techniek, de kosten van de mogelijke oplossingen en de aard van de te beschermen informatie. Overigens moet de telecomoperator onder bepaalde omstandigheden de bevoegde diensten in staat stellen de berichten te decoderen.

7.3. De erkenning van eindapparatuur

In de richtlijn 1999/5/EG van het Europees Parlement en van de Raad d.d. 9 maart 1999 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit wordt «telecommunicatie-eindapparatuur» beschreven (artikel 2, *b)* als een product dat communicatie mogelijk maakt, of een relevant onderdeel daarvan, dat bedoeld is voor directe of indirecte aansluiting op welke wijze ook op interfaces van openbare telecommunicatienetten.

Een eenvoudig navigatie- of e-mailprogramma of een router kunnen dus worden beschouwd als telecommunicatie-eindapparatuur.

In artikel 3, *c)* (essentiële voorwaarden), bepaalt dezelfde richtlijn dat de Commissie kan besluiten dat apparatuur van bepaalde apparatuurcategorieën of apparatuur van een bepaalde soort zo geconstrueerd moet zijn dat zij voorzieningen bevat om de persoonsgegevens en de persoonlijke levenssfeer van de gebruiker en de abonnee te beschermen. De Europese Commissie beschikt dus over een dwingend juridisch instrument dat onmiddellijk beschikbaar is.

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

Corollairement à ce qui se passe en Amérique (1), il conviendrait que la Sûreté de l'État et le SRG puissent conseiller et former en matière de sécurité des télécommunications les entreprises stratégiques qui le souhaitent.

7.5. Créer un organisme national de sécurité aux télécommunications

Pour rappel, le groupe Belinfosec (2) avait produit, le 11 avril 1995, un document intitulé *« La sécurité des systèmes d'information, une préoccupation gouvernementale ? »* qui a été communiqué au Parlement ainsi qu'aux ministres de la Justice et de la Défense Nationale le 25 juillet 1995.

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

— réaliser les audits et l'évaluation des procédés de sécurité des systèmes d'information dans le secteur public;

— déterminer les domaines d'application des procédés de cryptographie;

— former les experts en sécurité du secteur public;

— faire élaborer la réglementation et veiller à son respect;

— favoriser le développement de la recherche et des compétences nationales dans ce domaine;

— suivre les études de sécurité confiées par l'Administration à des entreprises privées. »

Il nous semble toutefois que cette recommandation, écrite il y a cinq ans, devrait être réactualisée au regard de l'évolution rapide des télécommunications et des techniques d'écoute et, notamment, que le

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

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

7.4. Nieuwe doelstellingen voor de Veiligheid van de Staat

In navolging van wat er in Amerika (1) gebeurt zou het passend zijn dat de Veiligheid van de Staat en de SRG een taak van advies en opleiding inzake de beveiliging van telecommunicatie kunnen vervullen voor strategische ondernemingen die op dergelijke diensten een beroep willen doen.

7.5. Oprichting van een nationaal organisme voor de beveiliging van telecommunicatie

We herinneren eraan dat de groep Belinfosec (2) op 11 april 1995 een document voorstelde met de titel « De veiligheid van informatiesystemen, een regeringsbekommernis? » Op 25 juli 1995 werd dit document bezorgd aan het Parlement en aan de ministers van Justitie en Landsverdediging.

Het document bevatte de volgende aanbeveling : « Naar het voorbeeld van zijn buurlanden zou België een centrale structuur moeten creëren met betrekking tot de beveiliging van informatiesystemen. In samenwerking met de bestaande bevoegdheden in het land zou deze centrale instantie met name de volgende opdrachten moeten vervullen :

— verrichten van audits en evalueren van de beveiligingsprocédés van informatiesystemen in de overheidssector;

— bepalen van de toepassingsgebieden van encryptieprocédés;

— opleiden van beveiligingsdeskundigen in de overheidssector;

— de reglementering doen uitwerken en toezien op de naleving ervan;

— bevorderen van de ontwikkeling van het onderzoek en de nationale bevoegdheden op dit gebied;

— opvolgen van veiligheidsonderzoeken die de overheid aan private ondernemingen toevertrouwt. »

We zijn echter van mening dat deze aanbeveling, die vijf jaar geleden is opgesteld, moet worden geactualiseerd in het licht van de snelle ontwikkeling van de telecommunicatie en van afluistertechnieken. In

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

(2) Informele groep samengesteld uit wetenschappers van hoog niveau en vertegenwoordigers van diverse activiteitensectoren. Deze groep heeft niet meer vergaderd sinds België het gebruik van encryptie heeft geliberaliseerd. Het jaarverslag 1995 van het Comité I bevat meer informatie over deze groep, zijn structuur en zijn werking.

bénéfice d'une telle structure ne devrait pas être limité au seul secteur public

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

7.6. Les licences individuelles dans le secteur des télécommunications

La directive 97/13/CE(1) inscrit la protection des données dans la liste des « exigences essentielles ». Elle précise dans son article 1, *d),* que « la protection des données peut comprendre la protection des données personnelles, la confidentialité des informations transmises ou stockées, ainsi que la protection de la vie privée ».

Il semble possible, sur base de cette directive, d'imposer la mise en place de certaines mesures de sécurité comme condition impérative à l'octroi d'une licence.

Ceci est particulièrement pertinent dans le cas des opérateurs de mobilophonie, qui, selon Duncan Campbell, n'utiliseraient que 40 bits sur les 56 initialement prévus pour encrypter les télécommunications mobiles.

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

Cet audit nous semble une condition préalable à l'établissement de règles impératives à respecter en matière de cryptage des communications.

Cet audit devrait être suffisamment technique pour pouvoir vérifier de manière certaine(2) et en présence d'experts la réalité ou l'absence de mesures de sécurité ainsi que leurs performances.

En particulier, il y a lieu de vérifier si :

— les centraux numérique RNIS (ISDN) diffusés en Belgique ou certains d'entre eux permettent (et si

(1) Directive 97/13/CE du Parlement Européen et du Conseil du 10 avril 1997 relative à un cadre commun pour les autorisations générales et les licences individuelles dans le secteur des services de télécommunications, *Journal officiel,* L. 117, mai 1997 (déjà cité *supra* point 5.2.).

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

het bijzonder vinden we dat de voordelen van een dergelijke structuur niet tot de overheidssector zouden mogen worden beperkt.

Voorts zou een dergelijke structuur de taak moeten krijgen encryptienormen vast te stellen en te publiceren die vervolgens in diverse activiteitensectoren (bijvoorbeeld : banken, ziekenhuizen, overheidsdiensten, telecomoperators ...) kunnen worden voorgesteld of zelfs opgelegd. Deze structuur zou ook technische normen kunnen bepalen voor de legale interceptie van telecommunicatie door de bevoegde diensten.

7.6. Individuele licenties in de telecommunicatiesector

De richtlijn 97/13/EG(1) neemt de bescherming van gegevens op in de lijst met « essentiële voorwaarden ». Artikel 2-1, *d),* van de richtlijn bepaalt dat 'de gegevensbescherming de bescherming van persoonsgegevens, het vertrouwelijk karakter van informatie die wordt doorgegeven of opgeslagen, alsook de bescherming van de persoonlijke levenssfeer kan behelzen. »

Op grond van deze richtlijn lijkt het mogelijk de invoering van bepaalde veiligheidsmaatregelen op te leggen als dwingende voorwaarde voor het toekennen van een licentie.

Dit is bijzonder relevant in het geval van mobilofonie-operators die volgens Duncan Campbell slechts 40 bits zouden gebruiken van de oorspronkelijk voorziene 56 bits om mobiele telecommunicatie te coderen.

7.7. Een audit betreffende de beveiliging van telecommunicatie bij de nationale operatoren.

Een dergelijke audit is volgens ons een voorafgaande voorwaarde voor het vaststellen van dwingende regels die moeten worden nageleefd met betrekking tot het coderen van communicatie.

Deze audit zou voldoende technisch moeten zijn om op zekere manier(2) en in het bijzijn van deskundigen na te gaan of er al dan niet veiligheidsmaatregelen zijn genomen en of ze doeltreffend zijn.

In het bijzonder moet worden gecontroleerd of :

— de in België verspreide digitale ISDN-centrales of sommige daarvan het afluisteren (en zo ja, onder

(1) Richtlijn 97/13/EG van het Europees Parlement en van de Raad d.d. 10 april 1997 met betrekking tot een gemeenschappelijk kader voor de algemene machtigingen en de individuele licenties in de sector van de telecommunicatiediensten, *Publicatieblad,* L. 117, mei 1997 (*cf. supra* punt 5.2.).

(2) Hiertoe moet men het fenomeen « afluisteren » kunnen observeren en reproduceren. De wet op het afluisteren verbiedt niet dat iemand die communiceert zijn eigen gesprekken opvangt.

oui, dans quels conditions) l'écoute des conversations dans une pièce, à l'aide d'un poste téléphonique raccroché.

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

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

CONCLUSIONS ET RECOMMANDATIONS DU COMITÉ R

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

— en ce qui concerne l'existence « d'Échelon » et ses activités :

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

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

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

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

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

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

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

— tant l'administrateur général *ad interim* de la Sûreté de l'État que le chef du SGR confirment que

welke voorwaarden) van gesprekken in een kamer mogelijk maken, met behulp van een opgehangen telefoon;

— het coderingsalgoritme dat mobilofonie-operators gebruiken een codering van 40 of van 56 bits gebruikt.

Deze inleidende fase is absoluut noodzakelijk voor het invoeren van « goede » en passende encryptiemaatregelen. Indien een dergelijk onderzoek niet plaatsvindt, is het risico groot dat men maatregelen neemt die in het algemeen niet de gewenste prestaties leveren, heel veel kosten of wettelijke afluisteroperaties verhinderen.

DE CONCLUSIES VAN HET COMITÉ I

Het Comité I baseert zich op de vaststellingen van de heren Poullet en Dinant om de volgende besluiten te trekken :

— wat het bestaan betreft van « Echelon » en zijn activiteiten :

— welke ook de benaming mag zijn die gegeven wordt aan hun systemen (de benaming « Echelon » verschijnt nooit in officiële recente documenten) is het evident dat de Verenigde Staten en Groot-Brittanië over officiële diensten beschikken (de NSA en de GCHQ) die belast zijn met het intercepteren van telecommunicaties om veiligheidsredenen, maar eveneens « in the interest of the national well-beeing » (in het belang van het nationaal welzijn) van de betrokken landen;

— de technische en personeelscapaciteiten van deze diensten zijn enorm;

— er bestaan ernstige aanwijzingen, maar geen enkel sluitend bewijs, dat de afluister-capaciteiten kunnen gebruikt worden met als doel de economische spionage gericht op de landen van de Europese Unie;

— de dubbelzinnige verklaringen van Amerikaanse en Britse overheden over dit onderwerp laten niet toe om de twijfel weg te nemen;

— zoals de Amerikaanse journalist James Bamford opmerkte dat de NSA zijn mandaat niet overschrijdt, « betekent dit niet dat de NSA het nooit zal doen »;

— de garanties voor het respect voor de persoonlijke levenssfeer en de beroepsmogelijkheden die door de Amerikaanse en Britse wetgevingen geboden worden, richten zich uitsluitend tot burgers van deze twee landen en niet tot onderdanen van andere Staten;

— wat de houding van de Belgische inlichtingendiensten aangaat :

— zowel de Administrateur-generaal *ad interim* van de Veiligheid van de Staat als de Chef van SGR

leurs services ne suivent pas le système « Échelon »; ils déclarent ne pas disposer des moyens humains et techniques nécessaires pour le faire;

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

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

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

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

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

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

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

RECOMMANDATIONS

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

— de considérer l'éventualité de systèmes d'interceptions de communications mis en ouvre par des pays étrangers à des fins contraires aux intérêts légitimes de la Belgique (notamment la protection du potentiel scientifique et économique) comme hautement vraisemblable, à défaut d'être prouvée;

— de donner par conséquent comme mission aux services de renseignement belges de collaborer en vue de recueillir toute information disponible (de sources ouvertes et autres) sur la question;

— de donner aux services de renseignement les moyens techniques et humains nécessaires pour

bevestigen dat hun diensten het Echelonsysteem niet volgen; zij verklaren niet over de noodzakelijke menselijke en technische middelen te beschikken om dit te doen;

— de Veiligheid van de Staat heeft nog geen instructies ontvangen van het Ministerieel Comité voor de inlichtingen en veiligheid inzake de bescherming van het economisch en wetenschappelijk potentieel; zij heeft nog geen belangrijke middelen ingezet voor deze nieuwe opdracht;

— noch de economische spionage, noch het Echelonsysteem staan op de agenda van de ontmoetingen tussen vertegenwoordigers van Europese inlichtingendiensten;

— SGR verklaart dat de eventueel militaire spionage uitgaande van de aan België geallieerde landen voor haar geen prioriteit in haar opdrachten betekent;

— zowel de Veiligheid van de Staat als SGR betreuren dat zij niet kunnen overgaan tot veiligheidsintercepties binnen een wettelijk kader;

— SGR werkt evenwel vanuit de hypothese dat de interceptie van communicaties werkelijk bestaat en ongeacht het land dat ze uitvoert, men er zich tegen moet beschermen; SGR beschouwt eveneens dat éénder welk informatica-coderingssysteem vatbaar is om verbroken te worden;

— zijnde gelast met de veiligheid van de communicaties van de Strijdkrachten, heeft SGR verschillende regels opgesteld met als doel de vertrouwelijkheid te vrijwaren van geclassificeerde gegevens die door telecommunicatie worden doorgezonden of door informaticasystemen behandeld worden;

— SGR volgt van nabij de ontwikkeling van de wetgeving inzake cryptografie; zij stelt voor dat een officieel organisme gelast zou worden met het veiligheidsbeleid inzake informatie in België.

AANBEVELINGEN

Zich aansluitend bij de aanbevelingen van de heren Poullet en Dinant, beveelt het Comité I bovendien aan :

— de eventualiteit van communicatie-interceptiesystemen, die opgezet zijn door vreemde landen met doeleinden tegengesteld aan de wettelijke belangen van België (in het bijzonder de bescherming van het wetenschappelijk en economisch potentieel) te beschouwen als hoogst waarschijnlijk, bij gebreke aan bewijzen;

— om bijgevolg als opdracht te geven aan de Belgische inlichtingendiensten om samen te werken teneinde elke beschikbare informatie (van open bronnen of andere) over deze vraag te kunnen inwinnen;

— om aan de inlichtingendiensten de technische en menselijke middelen te verlenen die noodzakelijk

accomplir cette mission (en leur permettant notamment de faire appel à des experts externes comme des informaticiens, des ingénieurs en télécommunications, des spécialistes en cryptographie, des analystes, etc.);

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

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

LES DOCUMENTS «SOURCES»

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

Documents du Parlement européen:

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

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

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

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

• part 4/4: *the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multilanguage leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (april 1999);*

• vol 1/5: 1) présentation des quatre études; 2) protection des données et droit de l'homme dans l'Union européenne et rôle du Parlement européen; (octobre 1999);

• vol 2/5: *the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multilanguage leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (october 1999) — Duncan Campbell;*

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

zijn om deze opdracht te vervullen (en hun toe te staan om in het bijzonder beroep te doen op externe deskundigen zoals informatici, ingenieurs in telecommunicatie, specialisten in cryptografie, analisten, enz.);

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

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

BRONDOCUMENTEN

Het huidig verslag werd opgesteld op basis van volgende documenten:

Documenten van het Europees Parlement:

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

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

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

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

• part 4/4: *the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multilanguage leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (april 1999);*

• vol 1/5: 1) *présentation des quatre études*; 2) *protection des données et droit de l'homme dans l'Union européenne et rôle du Parlement européen*; (october 1999);

• vol 2/5: *the state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multilanguage leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (october 1999) — Duncan Campbell;*

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

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

• vol 5/5 : *the perception of economic risks arising from the potential vulnerability of electronic.*

CHAPITRE 2

Enquête sur la manière dont les services de renseignement ont participé à la découverte des faits d'espionnage imputés au colonel Bunel

1. PROCÉDURE

Le 21 février 2000, le Comité R réceptionne un courrier du président du Sénat, M. De Decker, daté du 14 février 2000 et libellé de la sorte : « ... lors de la réunion du 31 janvier dernier, les commissions de suivi ont clairement exprimé le souhait que le Comité R poursuive l'enquête sur le système « Échelon », et qu'il s'informe, dans ce cadre, sur l'arrestation du colonel français « Bunel » afin de déterminer que les informations qui ont mené à son arrestation proviennent d'un système de surveillance électronique ... » (1).

Lors de sa réunion plénière du 22 février 2000 le Comité « R » décide à l'unanimité, pour raisons de faisabilité et de délai octroyé, de scinder la demande exprimée, soit de s'atteler personnellement à la rédaction d'un rapport complémentaire sur le système d'écoutes électroniques baptisé « Échelon » et, concomitamment, de confier à son Service d'enquêtes la mission de vérifier auprès de services de renseignement belges s'ils disposent d'informations susceptibles de démontrer que l'arrestation du colonel français Bunel aurait été rendue possible en raison de l'utilisation de moyens de surveillance électronique.

Il convient de rappeler ici que le colonel Bunel était, jusqu'à son arrestation au 31 octobre 1998 du chef d'avoir remis à un agent serbe des informations classifiées « Secret-OTAN » relatives aux cibles des frappes aériennes, membre de la délégation militaire française auprès de l'Alliance et exerçait au siège de l'OTAN, à Evere, ses fonctions de chef de cabinet du représentant militaire français. Il a été remis en liberté le 23 août 1999.

Dès le 2 mars 2000, notification est adressée au président du Sénat, M. De Decker, conformément aux articles 32 et 35, 2º, de la loi organique du

(1) Traduction libre.

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

• vol 5/5 : *the perception of economic risks arising from the potential vulnerability of electronic.*

HOOFDSTUK 2

Onderzoek over de wijze waarop de inlichtingendiensten hebben bijgedragen tot de ontdekking van feiten van spionage ten laste van kolonel Bunel

1. PROCEDURE

Op 21 februari 2000 ontving het Comité I van de voorzitter van de Senaat, de heer De Decker, een brief d.d. 14 februari 2000, als volgt opgesteld : « (...) op de vergadering van 31 januari 2000 hebben de begeleidingscommissies duidelijk te kennen gegeven dat ze wensen dat het Comité I het onderzoek naar het systeem « Echelon » voortzet, en dat het in verband hiermee inlichtingen inwint over de arrestatie van de Franse Kolonel « Bunel », teneinde vast te stellen of de informatie, die tot zijn aanhouding heeft geleid, afkomstig is van een elektronisch bewakingssysteem » (1).

Op zijn plenaire zitting van 22 februari 2000 besloot het Comité I eensgezind, — om redenen van haalbaarheid en gelet op de toegekende termijn —, het gekregen verzoek te splitsen : het Comité zou zelf het aanvullend rapport over het elektronisch afluistersysteem « Echelon » opstellen, en tegelijk zijn Dienst Enquêtes de opdracht geven bij de Belgische inlichtingendiensten na te gaan, of ze beschikten over informatie op grond waarvan kon worden aangetoond dat de arrestatie van de Franse kolonel Bunel mogelijk zou zijn gemaakt door het gebruik van elektronische bewakingsmiddelen.

Hierbij is het aangewezen er aan te herinneren dat kolonel Bunel, tot aan zijn arrestatie op 31 oktober 1998 op beschuldiging van gegevens geclassificeerd als « NATO-Secret » aan een Servisch agent te hebben doorgegeven, lid was van de Franse militaire delegatie bij de Atlantische verdragsorganisatie en op de zetel van de NAVO te Evere zijn functie als kabinetschef van de Franse militaire vertegenwoordiger uitoefende. Hij werd opnieuw in vrijheid gesteld op 23 augustus 1999.

Op 2 maart 2000 werd de voorzitter van de Senaat, de heer De Decker, overeenkomstig de artikelen 32 en 35, 2º, van de wet d.d. 18 juli 1991 en artikel 44, lid 2,

(1) Vrije vertaling.

18 juillet 1991 et à l'article 44, deuxième alinéa, du règlement d'ordre intérieur du Comité R, de la mise à exécution de la double mission.

Tandis qu'il s'attèle par ailleurs à la collecte d'informations crédibles nouvelles et à la rédaction du complément de rapport demandé par les commissions de suivi dans le cadre du système « Échelon » pour le 15 mars 2000 (dont il ne sera plus fait mention dans le cadre strict du présent rapport d'enquête), le Comité R adresse le 10 mars 2000 une apostille au chef du Service d'enquêtes, l'invitant à procéder à l'audition des responsables de la Sûreté de l'État et du SGR, de sorte à savoir si ces deux services disposent d'un dossier concernant le colonel français Bunel et, dans l'affirmative, s'il contient des éléments de conviction permettant de mettre en cause l'intervention d'un système de surveillance électronique, le cas échéant activé par des services étrangers agissant en tout ou partie sur territoire belge, dans le cadre de l'arrestation de ce dernier.

Le même jour, en application de l'article 43.1 de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le chef du Service d'enquêtes avise à son tour M. Verwilghen, ministre de la Justice, et M. Flahaut, ministre de la Défense nationale, de l'ouverture de l'enquête.

Le Service d'enquêtes a déposé son rapport en date du 14 mars 2000.

Le présent rapport a été approuvé par le Comité R en date du 3 avril 2000.

2. AUDITIONS

Le 13 mars 2000, le Service d'enquêtes procède à l'audition de deux responsables du Service général de renseignement et de sécurité.

Ceux-ci exposent en substance que leur service ne disposait d'aucune information au sujet du colonel Bunel avant son arrestation. Tous deux ignorent parfaitement de quelle manière le rôle du colonel Bunel a été révélé.

À l'issue de ce bref entretien le Service d'enquêtes consulte la farde de travail du SGR, qui contient surtout des documents issus de sources ouvertes (presse quotidienne pour leur plus grande part).

D'autres documents, tels un fax et une note évoquant l'arrestation du colonel Bunel, ne permettent pas plus de mettre celle-ci en relation avec un système de surveillance électronique.

van het huishoudelijk reglement van het Comité I, op de hoogte gebracht van de tenuitvoerlegging van de dubbele opdracht.

Terwijl het Comité I nieuwe en geloofwaardige informatie verzamelde, en op verzoek van de begeleidingscommissies tegen 15 maart 2000 het aanvullend verslag opstelde in het kader van het systeem « Echelon » (waarnaar niet meer wordt verwezen in het strikte kader van onderhavig onderzoeksverslag), stuurde het op 10 maart 2000 een kantschrift naar het hoofd van de Dienst Enquêtes. Daarin verzocht het Comité I hem over te gaan tot het verhoor van de verantwoordelijken van de Veiligheid van de Staat en van de ADIV (Algemene Dienst inlichting en veiligheid), teneinde te vernemen of deze beide diensten een dossier bezitten over de Franse kolonel Bunel, en, in bevestigend geval, of dat dossier overtuigende elementen bevat die toelaten te stellen dat een elektronisch bewakingssysteem, — eventueel bediend door buitenlandse diensten die volledig of gedeeltelijk op het Belgisch grondgebied handelen —, een rol had gespeeld bij de arrestatie van de bovengenoemde persoon.

Dezelfde dag bracht het hoofd van de Dienst enquêtes op zijn beurt, overeenkomstig artikel 43.1 van de wet d.d. 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, de heer Verwilghen, minister van Justitie, en de heer Flahaut, minister van Landsverdediging, op de hoogte van de opening van het onderzoek.

De Dienst enquêtes heeft zijn verslag neergelegd op 14 maart 2000.

Het Comité I heeft het onderhavig verslag goedgekeurd op 3 april 2000.

2. VERHOREN

Op 13 maart 2000 heeft de Dienst enquêtes twee verantwoordelijken van de Algemene Dienst inlichting en veiligheid verhoord.

In hoofdzaak verklaarden ze dat hun dienst geen inlichtingen had over kolonel Bunel vóór zijn arrestatie. Geen van beiden hadden er een idee van op welke wijze de rol van kolonel Bunel aan het licht was gekomen.

Na afloop van dit korte onderhoud heeft de Dienst enquêtes inzage genomen van de werkmap van de ADIV, die vooral documenten bevat afkomstig van open bronnen (voornamelijk de dagelijkse pers).

Andere documenten, zoals een facsimile en een nota waarin de arrestatie van kolonel Bunel wordt gemeld, laten evenmin toe een verband te leggen tussen deze aanhouding en een elektronisch bewakingssysteem.

Le même jour le Service d'enquêtes s'est également rendu au siège de la Sûreté de l'État et y a entendu deux agents.

La sensibilisation de la Sûreté de l'État a débuté avec la prise de connaissance de l'arrestation de l'intéressé. Des informateurs ont été sollicités mais n'ont rien pu apporter de concret.

À titre anecdotique, signalons qu'il ressort de la documentation de la Sûreté de l'État, que le colonel Bunel a ouvert un site «internet» à l'adresse: «http://site.voila.fr/pierre_bunel». Il s'y présente et y accueille de nombreux «cyber-visiteurs» auxquels il expose, notamment, sa version des faits et sa motivation.

Ici aussi rien ne permet de supposer que l'arrestation de l'intéressé aurait été rendue possible en raison de la mise en œuvre de moyens électroniques d'écoute.

3. CONSTATATIONS

À la demande du Comité R le Service d'enquêtes a entendu les responsables du SGR et de la Sûreté de l'État. Si ces deux services ont effectivement cherché à s'informer sur le colonel Bunel, c'est à la suite de son arrestation, l'intéressé n'étant pas connu d'eux auparavant.

Ni la Sûreté de l'État, ni le Service général de renseignement et de sécurité ne sont en mesure d'avancer le moindre élément susceptible d'accréditer la thèse que l'arrestation du colonel Bunel aurait été rendue possible grâce à la mise en œuvre d'un système électronique d'écoute, y compris de la part d'autorités et ou de services étrangers.

B. LES PLAINTES

CHAPITRE 1

Rapport concernant l'enquête de contrôle du fonctionnement interne d'un département de la Sûreté de l'État

1. PROCÉDURE

Le Comité permanent R s'est saisi le 17 février 1999, d'une dénonciation anonyme rédigée en langue française, adressée le 16 février à son Service d'enquêtes.

Le Comité R a décidé le 24 février 1999 d'ouvrir une enquête intitulée: «Contrôle du fonctionnement interne d'un département de la Sûreté de l'État». Deux membres furent désignés pour suivre ce dossier.

Dezelfde dag heeft de Dienst enquêtes zich naar de zetel van de Veiligheid van de Staat begeven, waar hij twee agenten heeft verhoord.

De Veiligheid van de Staat werd zich bewust van het probleem, toen ze kennis kreeg van de arrestatie van de betrokkene. Informanten konden geen concrete inlichtingen bezorgen.

Bij wijze van anekdote merken we op dat uit de documentatie van de Veiligheid van de Staat blijkt dat kolonel Bunel op het internet een site heeft geopend, waarvan het adres luidt: http://site.voila.fr/pierre_bunel. Hij stelt er zich voor en onthaalt er talrijke «cybernauten» aan wie hij zijn versie van de feiten geeft en uitlegt waarom hij zo heeft gehandeld.

Ook hier laat niets toe te veronderstellen dat de arrestatie van de betrokkene mogelijk zou zijn gemaakt door het aanwenden van elektronische afluistertechnieken.

3. VASTSTELLINGEN

Op verzoek van het Comité I heeft de Dienst enquêtes de verantwoordelijken van de ADIV en van de Veiligheid van de Staat verhoord. Beide diensten hebben inderdaad gepoogd inlichtingen in te winnen over kolonel Bunel, maar dat gebeurde pas na zijn arrestatie, aangezien de betrokkene bij hen voordien niet bekend was.

Noch de Veiligheid van de Staat, noch de Algemene Dienst inlichting en veiligheid kunnen enig element naar voren brengen, op grond waarvan geloof kan worden gehecht aan de stelling volgens dewelke de arrestatie van kolonel Bunel mogelijk zou zijn gemaakt door het aanwenden van een elektronisch afluistersysteem, inclusief vanwege vreemde overheden en/of diensten.

B. DE KLACHTEN

HOOFDSTUK 1

Toezichtsonderzoek over de controle van de interne werking van een sectie van de Veiligheid van de Staat

1. PROCEDURE

Op 17 februari 1999 werd het Vast Comité I gevat door een in het Frans opgestelde anonieme aangifte die op 16 februari aan de Dienst enquêtes van het Comité I was gezonden.

Op 24 februari 1999 besliste het Comité I een onderzoek te openen met als titel: «Controle over de interne werking van een sectie van de Veiligheid van de Staat». Twee leden werden aangesteld om dit dossier op te volgen.

Le 24 février 1999, une apostille du Comité R a été adressée au Service d'enquêtes afin de procéder à l'enquête de contrôle.

En application de l'article 46, alinéa 3, de son règlement d'ordre intérieur le Comité R a averti, par lettres du 26 février 1999, les présidents de la Chambre des représentants et du Sénat de l'ouverture de l'enquête.

Par courrier du 2 mars 1999 et conformément à l'article 43, § 1, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, M. le ministre de la Justice a été averti de l'ouverture de l'enquête.

Le ministre de la Justice a accusé réception de cette notification le 29 mars 1999.

En date du 21 octobre 1999, le Service d'enquêtes a transmis son rapport au Comité R.

Par courrier du 24 novembre 1999, le président du Comité R a invité l'administrateur général *ad interim* à un échange de vues relatif aux conclusions à tirer de l'enquête.

Cette réunion s'est déroulée au siège du Comité R le 3 décembre 1999.

Le compte rendu de cette réunion a été transmis le 16 décembre 1999 à l'administrateur général *ad interim* de la Sûreté de l'État pour qu'elle puisse faire part de ses éventuels commentaires au sujet du contenu de ce document, en lui signalant que l'ensemble serait joint au dossier de l'enquête.

Les commentaires demandés ont fait l'objet de la lettre du 18 janvier 2000 transmise par l'administrateur général *ad interim* au président du Comité R.

Le Comité R a approuvé le présent rapport lors de sa réunion plénière du 22 mars 2000.

2. CONSIDÉRATIONS PRÉLIMINAIRES

La dénonciation portant sur des faits identifiables et donc en principe vérifiables, l'enquête a eu pour but de contrôler les activités de la section concernée de la Sûreté de l'État chargée de la protection des personnalités, pour déterminer, à la lumière des éléments contenus dans le courrier anonyme, si des dysfonctionnements internes avérés n'étaient pas susceptibles de porter atteinte à l'efficacité de cette section ou, vu le contexte de la dénonciation tel qu'il résulte du passage cité ci-après, à celle d'autres services extérieurs de la Sûreté de l'État.

Toutefois, il convenait aussi dans un premier temps de vérifier si les assertions contenues dans la dénonciation précitée ne résultaient pas d'un acte de

Op 24 februari 1999 stuurde het Comité I een kantschrift naar de Dienst enquêtes teneinde over te gaan tot dit toezichtsonderzoek.

Overeenkomstig artikel 46, lid 3, van zijn huishoudelijk reglement, heeft het Comité I de voorzitters van de Kamer van volksvertegenwoordigers en van de Senaat per brief d.d. 26 februari 1999, op de hoogte gesteld van de opening van het onderzoek.

Krachtens artikel 43, § 1, van de wet d.d. 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten kreeg de minister van Justitie per brief van 2 maart 1999 kennis van de opening van het onderzoek.

De minister van Justitie heeft de ontvangst van deze kennisgeving bevestigd op 29 maart 1999.

Op 21 oktober 1999 heeft de Dienst enquêtes zijn rapport aan het Comité I bezorgd.

Per brief d.d. 24 november 1999 heeft de voorzitter van het Comité I de administrateur-generaal *ad interim* uitgenodigd om van gedachten te wisselen over de conclusies van het onderzoek.

Deze vergadering vond op 3 december 1999 plaats op de zetel van het Comité I.

Het verslag van deze vergadering werd op 16 december 1999 verzonden naar de administrateur-generaal *ad interim* van de Veiligheid van de Staat teneinde haar toe te laten commentaar te geven op de inhoud van dit document; waarbij haar werd gemeld dat deze bij het onderzoeksdossier zou worden gevoegd.

In haar brief d.d. 18 januari 2000 aan de voorzitter van het Comité I, bezorgde de administrateur-generaal *ad interim* de gevraagde commentaar.

Op de plenaire vergadering van 22 maart 2000 keurde het Comité I het onderhavige rapport goed.

2. INLEIDENDE BESCHOUWINGEN

Aangezien deze aangifte betrekking had op identificeerbare en dus, in principe, op controleerbare feiten, had het onderzoek tot doel de activiteiten van de betrokken sectie van de Veiligheid van de Staat die belast is met de bescherming van personaliteiten, na te gaan en vast te stellen, in het licht van de elementen vermeld in de anonieme aangifte, of gebeurlijk bewezen interne disfuncties, geen afbreuk konden doen aan de doeltreffende werking van deze sectie of, rekening houdend met de context van de aangifte zoals deze blijkt uit het navolgend citaat, aan de doeltreffende werking van andere buitendiensten van de Veiligheid van de Staat.

In een eerste fase was het echter ook aangewezen na te gaan of de beweringen in de bovengenoemde aangifte niet het resultaat waren van kwaadwillig opzet

mauvais gré d'une ou de plusieurs personnes souhaitant sous le couvert de l'anonymat « régler des comptes » par Comité R interposé.

À la lecture des faits précis qui constituent le contenu de la dénonciation anonyme du 17 février 1999, ainsi que de ses annexes, il apparaît que le(s) rédacteur(s) de cette dénonciation serai(en)t membre(s) de la Sûreté de l'État.

La problématique principalement mise en évidence par un des cas décrits par le(s) dénonciateur(s) est relative à la rémunération de prestations de week-end « fictives ».

D'autres exemples d'irrégularités sont également dénoncés par le(s) auteur(s) de la lettre du 16 février 1999 dans le but de montrer qu' aurait été mis en place un système permettant à certains membres de l'équipe de profiter en outre d'avantages indus.

Cette situation de fait est apparemment à l'origine (au minimum) d'un malaise concrétisé par la dénonciation anonyme adressée au Service d'enquêtes du Comité R. Il est éclairant à ce sujet de citer les dernières phrases de cette dénonciation anonyme : « Étant donné qu'une plainte ouverte amènerait des mesures de représailles envers nos personnes, nous avons choisi la voie anonyme. Nous portons ces pratiques à votre connaissance parce que nous pensons que les limites du tolérable ont été franchies depuis longtemps et que tout indique qu'elles ne sont pas prêtes d'être réintégrées, ni qu'aucun changement ne peut être envisagé dans un avenir proche ... » (1).

Le problème de la surveillance interne exercée par la hiérarchie de la Sûreté de l'État sur les activités de la section « protection » était également posé.

Les différents faits dénoncés et les documents transmis, ainsi que d'autres éléments mis à jour au cours du contrôle, ont été examinés par le Service d'enquêtes sur la base des propres documents de la section « protection », des directives et notes de service mis à la disposition des enquêteurs, ainsi que sur la base des auditions des personnes concernées et des responsables hiérarchiques.

Révélée notamment par l'étude approfondie de certaines missions de protection de personnalités, l'ampleur de la problématique des heures de prestations irrégulières qualifiées par la Sûreté de l'État de « stand-by » est directement apparue au Service d'enquêtes lors de l'examen de l'ensemble des prestations irrégulières et de celles de week-end, dont la rémunération a été demandée par certains membres de la section concernée sur la base de l'arrêté ministériel du 23 juin 1997.

(1) Traduction libre.

van een of meer personen die de bedoeling hadden via het Comité I een « rekening te vereffenen », waarbij ze zelf anoniem bleven.

Uit de lezing van de precieze feiten die de inhoud vormen van de anonieme aangifte van 17 februari 1999, alsmede van de bijlagen, blijkt dat de opsteller(s) van deze aangifte lid zou(den) zijn van de Veiligheid van de Staat.

Het probleem waarop in hoofdzaak de aandacht wordt gevestigd in een van de gevallen die de aanklager(s) aanhaalt (aanhalen), heeft betrekking op de vergoeding voor « fictieve » weekendprestaties.

De aanklagers geven nog andere voorbeelden van onregelmatigheden om aan te tonen dat de verantwoordelijken van de sectie « bescherming » een systeem zouden hebben ingevoerd dat hen en sommige andere leden van het team toelaat voordelen te genieten waarop ze geen recht hebben.

Deze feitelijke situatie ligt klaarblijkelijk aan de oorsprong van wat men op zijn minst een malaise kan noemen, die nu concrete vorm krijgt in de anonieme aangifte bij de Dienst Enquêtes van het Comité I. De laatste zinnen van de bewuste aangifte zijn in dit opzicht heel verhelderend : « Aangezien een open klacht tot gevolg zou hebben dat we het slachtoffer worden van represailles, hebben we verkozen anoniem te blijven. We brengen u op de hoogte van het bestaan van deze praktijken, omdat we vinden dat de grenzen van het duldbare sinds lange tijd zijn overschreden en niets er op wijst dat de toestand snel opnieuw regelmatig zal worden of dat in de nabije toekomst enige wijziging mag worden verwacht ... » (1).

Het probleem van het intern toezicht dat de hiërarchie van de Veiligheid van de Staat uitoefent op de activiteiten van de sectie « bescherming » werd eveneens aan de orde gebracht.

Gebruik makend van documenten van de sectie « bescherming », van de richtlijnen en dienstnota's die ter beschikking van de onderzoekers zijn gesteld en van de verhoren van de betrokkenen en hun hiërarchische oversten, heeft de Dienst enquêtes de verschillende aangeklaagde feiten en de toegezonden documenten bestudeerd, alsook andere elementen die tijdens de controle aan het licht zijn gekomen.

Bij het onderzoek van alle onregelmatige prestaties en weekendprestaties, waarvoor sommige leden van de sectie « bescherming » een vergoeding hebben gevraagd op grond van het ministerieel besluit van 23 juni 1997, duurde het niet lang voor de Dienst enquêtes een duidelijk beeld kreeg van de omvang van het probleem van de onregelmatige door de Veiligheid van de Staat genaamde stand-byprestaties.

(1) Vrije vertaling.

D'une comparaison effectuée avec les systèmes mis en place par d'autres services confrontés à des prestations irrégulières, de nuit ou de week-end, il est apparu qu'aussi bien la gendarmerie, la police judiciaire ou le SGR ne rétribuent que les heures effectivement prestées dans les locaux officiels au cours d'une période de garde à domicile. Seule la section «protection» de la Sûreté de l'État applique un système plus large rémunérant systématiquement 12 heures de garde à domicile (stand-by) de week-end, même si celles-ci ne sont précédées ou ne débouchent sur aucune mission effective. Il est à remarquer également que les autres services extérieurs de la Sûreté de l'État ne bénéficient pas de ce régime.

Au cours de l'enquête il a été fourni à ce sujet un renseignement important: «Des 12 000 heures supplémentaires mises à la disposition de l'ensemble de la Sûreté de l'État par l'Inspection des finances, la moitié est en principe à peu près destinée à la section «protection». Les heures de stand-by sont différentes des heures supplémentaires et sont payées, tout au moins en ce qui concerne les week-ends, comme des heures de samedi et dimanche. Le quota de ces heures n'est pas précisé mais est prévu d'office par le service du personnel dans un article spécial au budget du ministère de la Justice. Les heures de stand-by pendant la semaine ne sont pas rémunérées.» (1)

Les constatations du Service d'enquêtes tendent à démontrer que, pour le premier semestre de l'année 1998, cette problématique concerne quelques 2 099 heures (soit 43% des sommes payées aux agents de la section «protection» sur base de l'arrêté ministériel précité) qui ne furent ni précédées, ni entrecoupées ni suivies d'une mission particulière de protection et donc sujettes à caution.

L'impact financier n'est donc pas négligeable et le Service d'enquêtes s'est livré à une évaluation qui permet de retenir pour le total de ces heures contestables, un montant annuel brut d'environ 3 millions de francs.

Comme dit plus haut, la base légale à prendre en considération de manière générale pour l'octroi aux membres du personnel des services extérieurs de l'Administration de la Sûreté de l'État d'une rémunération pour des prestations irrégulières, et plus particulièrement de week-end, est l'Arrêté ministériel du 23 juin 1997.

Le but de cet arrêté est d'étendre l'attribution d'une rémunération pour service irrégulier, déjà accordée depuis le 1er mai 1997 aux agents et officiers de la police judiciaire, aux agents des services extérieurs de la Sûreté de l'État.

(1) Traduction libre.

Uit een vergelijking met de systemen bij andere diensten, die eveneens worden geconfronteerd met onregelmatige prestaties, 's nachts en tijdens het week-end is gebleken dat de rijkswacht, de gerechtelijke politie of SGR alleen de reëel gepresteerde uren in de officiële lokalen, vergoeden van de periode waarin de leden thuis stand-by zijn. Alleen de sectie «bescherming» van de Veiligheid van de Staat past een ruimer systeem toe waarbij de agenten systematisch worden vergoed voor 12 uur stand-by ten huize tijdens het weekend, ook al zijn ze niet voorafgegaan of leidt dit niet tot een effectieve opdracht. We merken nog op dat dit stelsel evenmin geldt voor de andere buitendiensten van de Veiligheid van de Staat.

Tijdens het onderzoek werd hierover een belangrijke inlichting vernomen: «Van de 12 000 door de Inspectie van financiën ter beschikking van de hele Veiligheid van de Staat gestelde overuren zijn in principe ongeveer de helft bestemd voor de dienst «bescherming». Stand-by-uren zijn verschillend van overuren en worden voor wat betreft weekends althans, enkel betaald als zaterdag- en zondaguren. Deze zijn niet bepaald maar worden door de personeelsdienst ambtshalve voorzien op een bepaald artikel in het budget van het ministerie van Justitie. Stand-by-uren tijdens de week worden hierdoor niet vergoed».

Uit de vaststellingen van de Dienst enquêtes van het Comité I blijkt dat voor het eerste semester van het jaar 1998 deze problematiek handelt over ongeveer 2 099 uren (d.i. 43% van de bedragen betaald aan de leden van de sectie «bescherming» op grond van voornoemd ministerieel besluit) die niet worden voorafgegaan, onderbroken of gevolgd door een bijzondere beschermingsopdracht en waarbij dus vraagtekens kunnen worden geplaatst.

De financiële impact hiervan is niet onbelangrijk. De Dienst enquêtes heeft een evaluatie gemaakt volgens dewelke met het totaal van deze betwistbare uren, een jaarlijks brutobedrag van ongeveer 3 miljoen frank zou zijn gemoeid.

Zoals hierboven al gezegd vormt het ministerieel besluit van 23 juni 1997 de wettelijke basis waarmee algemeen rekening moet worden gehouden bij het toekennen van een toelage voor onregelmatige prestaties, in het bijzonder voor weekendprestaties, aan de personeelsleden van de buitendiensten van het Bestuur van de Veiligheid van de Staat.

Dit besluit heeft tot doel de toekenning van een toelage voor onregelmatige diensten, die sinds 1 mei 1997 al was toegekend aan de agenten en officieren van de gerechtelijke politie, uit te breiden en ook toe te kennen aan de agenten van de buitendiensten van de Veiligheid van de Staat.

(1) Vrije vertaling.

L'article 3 de cet arrêté prévoit notamment que : « Le service de week-end est celui accompli les samedis, les dimanches, les jours fériés légaux et réglementaires entre 0 et 24 heures. Toutefois, ne peuvent donner lieu à l'allocation que les services effectifs accomplis dans les locaux de la Sûreté de l'État et ceux requis pour l'exécution d'une mission précise ordonnée par le commissaire en chef (aujourd'hui appelé « directeur des opérations »), l'administrateur général adjoint ou l'administrateur général ... »

L'application de cet arrêté aux prestations effectuées à partir du 1er juillet 1997 a fait l'objet d'une note interne de l'administrateur général adjoint intitulée : « Service irrégulier ».

La note interne du 16 juillet 1997 ne donne aucune explication au sujet du concept « les services effectifs accomplis pour l'exécution d'une mission précise ». Par ailleurs, une note de service antérieure en date du 30 juin 1993 concernant la régulation des prestations exceptionnelles, signée par le commissaire en chef de la Sûreté de l'État, n'a pas été supprimée ni modifiée explicitement par la note du 16 juillet 1997. Cette directive ne répond plus aux conditions de l'arrêté ministériel précité, vu que cet arrêté permet explicitement aux chefs de brigades et de sections de mandater des prestations exceptionnelles.

Les dispositions légales en cette matière étant les mêmes que celles appliquées aux membres de la police judiciaire, il est relevant de constater que dans des notes de services de la police judiciaire de Bruxelles — antérieures il est vrai à l'arrêté ministériel du 23 juin 1997, mais toujours d'application — l'attention du personnel est attirée notamment : « sur le fait que seules les heures effectivement prestées et justifiées peuvent être comptabilisées ... et que les officiers partagent la responsabilité de la légalité des documents établis sous leur contrôle. Toute déclaration volontairement inexacte relevant du faux et usage de faux ».

Dans sa lettre du 8 juin 1999, adressée au président du Comité R relativement à la présente enquête, le précédent administrateur général de la Sûreté de l'État, rencontre d'ailleurs cette interprétation rigoureuse puisqu'il précise en ce qui concerne l'article 3, deuxième alinéa, de l'arrêté ministériel du 23 juin 1997 que : « Cette disposition, initialement rédigée sous forme de projet par la Sûreté de l'État, vise notamment d'une part les permanences et d'autre part, les prestations en dehors des locaux, expressement ordonnées afin de prévenir des initiatives incontrôlées et incontrôlables.

Il est évident que les missions de protection ordonnées par le ministre de l'Intérieur sont avalisées par la

Artikel 3 van dit besluit bepaalt : « Weekenddienst is arbeid verricht tussen 0 en 24 uur op zaterdagen, zondagen, wettelijke en reglementaire feestdagen. Voor de toelage komen echter alleen in aanmerking de ambtswerkzaamheden verricht in de lokalen van de Veiligheid van de Staat en die welke vereist zijn voor de uitvoering van een bepaalde opdracht welke vooraf bevolen is door de hoofdcommissaris (vandaag « directeur operaties » genoemd), door de adjunct-administrateur-generaal of door de administrateur-generaal. »

De toepassing van dit besluit op de prestaties verricht vanaf 1 juli 1997 was het voorwerp van een interne nota van de adjunct-administrateur-generaal met als titel : « Onregelmatige dienst ».

De interne nota van 16 juli 1997 geeft geen verdere toelichting bij het begrip « ambtswerkzaamheden vereist voor de uitvoering van een bepaalde opdracht ». Anderzijds wordt een vroeger dienstorder van 30 juni 1993 tot regeling van de uitzonderlijke prestaties, getekend door de hoofdcommissaris van de Veiligheid van de Staat, door deze interne nota niet ingetrokken noch expliciet gewijzigd. Dit order beantwoordt echter niet langer aan de voorwaarden van voornoemd ministerieel besluit, aangezien het de brigade- en sectiehoofden toelaat uitdrukkelijk de opdracht te geven tot uitzonderlijke prestaties.

Aangezien de wettelijke bepalingen ter zake dezelfde zijn als de bepalingen die gelden, voor de leden van de gerechtelijke politie, is het relevant vast te stellen dat in de dienstnota's van de gerechtelijke politie van Brussel — die weliswaar ouder zijn dan het ministerieel besluit van 23 juni 1997, maar nog steeds van toepassing zijn — de aandacht van het personeel in het bijzonder wordt gevestigd : « op het feit dat alleen de reëel gewerkte en gerechtvaardigde uren mogen worden geteld ... en dat de officieren mee verantwoordelijk zijn voor de wettelijkheid van de documenten die onder hun toezicht worden opgesteld. Elke opzettelijk onjuiste verklaring komt in aanmerking als valsheid in geschrifte en gebruik van valse stukken ».

In zijn brief d.d. 8 juni 1999 aan de voorzitter van het Comité I over dit onderzoek verwijst de vorige Administrateur-generaal van de Veiligheid van de Staat, trouwens naar deze strikte interpretatie, aangezien hij met betrekking tot artikel 3, tweede lid, van het ministerieel besluit van 23 juni 1997 schrijft : « Deze bepaling, oorspronkelijk een ontwerp door de Veiligheid van de Staat opgesteld, viseert dus enerzijds onder andere de permanenties en anderzijds de werkzaamheden buiten de lokalen die uitdrukkelijk zijn bevolen, en dit om ongecontroleerde en oncontroleerbare initiatieven uit te schakelen.

Het moet duidelijk zijn dat beschermingsopdrachten bevolen door de minister van Binnenlandse

hiérarchie de la Sûreté de l'État et transmises au chef de section pour exécution.

Il est confirmé que les «stand-by» octroyés au personnel dans le cadre de missions particulières, doivent répondre à des exigences strictes (réponse endéans l'heure) et ne se justifient que dans les cas où les chances d'être rappelé sont réelles.» (1)

Si dans les termes utilisés par l'administrateur général de la Sûreté de l'État, l'intention est manifeste d'appliquer la norme légale, et donc d'éviter les abus, les constatations qui suivent montrent qu'en pratique on est loin du compte. On se trouve, au moins, devant un phénomène exemplatif d'estompement de la norme.

Aucun document, note de service ou circulaire internes à la Sûreté de l'État explicitant les principes qui président à la rémunération des heures comptabilisées sous le vocable «stand-by» n'a été soumis aux enquêteurs.

La hiérarchie de la Sûreté de l'État a cependant mis en avant un certain nombre d'arguments légaux pour justifier la reconnaissance du principe des heures dites de «stand-by». Il n'entre certes pas dans les intentions du Comité R de contester la valeur de ces arguments à caractère juridique, le problème ne se situant pas immédiatement à ce niveau, mais plutôt à celui de se demander si toutes les heures de «stand-by» ou si certaines prestations irrégulières de week-end sont toujours bien fondées.

3. SYNTHÈSE DES ANOMALIES CONSTATÉES AU COURS DE L'ENQUÊTE EN CE QUI CONCERNE LES HEURES DE PRESTATIONS DE WEEK-END ET LES HEURES DE «STAND-BY»

Le Service d'enquêtes du Comité R a examiné, pour l'année 1998, quatre cas de missions de protection comportant des prestations de week-end et des stand-by. Un de ces cas faisait l'objet de la dénonciation anonyme, les autres ont été mis en évidence par le Service d'enquêtes.

Tous ces cas ont révélé des anomalies flagrantes répétées en ce qui concerne le bien fondé des heures réellement prestées ayant donné lieu à rémunération.

À chaque fois ont été constatées:

— l'absence d'éléments précis permettant de justifier des heures de stand-by de week-end qui répon-

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

Zaken door de hiërarchie van de Veiligheid van de Staat worden geavaleerd en voor uitvoering aan de sectie worden overgemaakt.

Voor wat de «stand-by» betreft die in het kader van bepaalde opdrachten aan het personeel wordt opgelegd, wordt bevestigd dat dit onder strikte voorwaarden gebeurt (respons binnen het uur) en alleen in die gevallen waarin de kans op oproeping reëel is».

Hoewel uit de bewoordingen van de administrateur-generaal van de Veiligheid van de Staat duidelijk blijkt dat men de bedoeling heeft de wettelijke norm toe te passen en bijgevolg misbruiken te voorkomen, bewijzen de hierna beschreven vaststellingen dat men daar in praktijk niet in slaagt. Er is op zijn minst sprake van een fenomeen van normvervaging.

De onderzoekers hebben geen enkel intern document, dienstnota of circulaire van de Veiligheid van de Staat ontvangen waarin toelichting wordt gegeven over de beginselen die de vergoeding regelen van uren die worden geteld in de rubriek «stand-by».

Van haar kant heeft de hiërarchie van de Veiligheid van de Staat een aantal wettelijke argumenten naar voren gebracht ter rechtvaardiging van het feit dat zij het principe van de zogenaamde stand-by-uren erkende (zie *infra* pagina 8). Het Comité I heeft geenszins de bedoeling de waarde van deze juridische argumenten te betwisten, aangezien het probleem zich niet in eerste instantie op dat niveau situeert. Veeleer moet men zich de vraag stellen of al die stand-by-uren en bepaalde onregelmatige weekendprestaties werkelijk hebben plaatsgevonden.

3. HET ONDERZOEK EN DE VASTGESTELDE ANOMALIEËN MET BETREKKING TOT DE WEEKENDPRESTATIES EN DE STAND-BY-UREN

De Dienst enquêtes van het Comité I heeft voor het jaar 1998 vier gevallen van beschermingsopdrachten onderzocht die prestaties inhielden tijdens het weekend en «stand-by». Eén van deze gevallen maakte het voorwerp uit van de anomieme aangifte, de andere werden naar voren gebracht door de Dienst Enquêtes.

Bij elk van deze gevallen werden herhaald overduidelijke misbruiken aan het licht gebracht, wat betreft de gegrondheid van de reële gepresteerde uren die vergoed werden.

Telkens opnieuw konden de volgende zaken worden vastgesteld:

— het ontbreken van precieze elementen die toelaten het bestaan van stand-by-uren in het weekend te

(1) N. de Sadeleer, *«Les principes du pollueur-payeur, de prévention et de précaution»*, Bruylant, 1999, blz. 395.

dent aux conditions strictes rappelées par l'administrateur général (voir supra);

— la non application des dispositions de l'arrêté ministériel du 23 juin 1997;

— l'altération matérielle de données initialement reprises sur des feuilles de prestations personnelles, avec l'intention vraisemblable de se faire payer les heures indiquées.

4. AUTRES ÉLÉMENTS DE FAIT CONTENUS DANS LA DÉNONCIATION ANONYME DU 16 FÉVRIER 1999

4.1. La prise en compte abusive d'heures de sport comme heures de service irrégulier

La prise en compte abusive d'activités sportives pratiquées pendant la pose de midi comme prestations irrégulières rémunérées est un des éléments repris dans la dénonciation anonyme.

Après vérification, le Service d'enquêtes du Comité R a en effet constaté qu'en l'occurence n'étaient pas respectées les conditions prévues dans les instructions internes, à savoir notamment que ce type de prestations doivent être nécessitées par l'intérêt du service et doivent faire l'objet d'un ordre émanant soit du chef de section, soit du commissaire en chef.

Cette pratique ne concerne qu'une seule personne, ce qui tend à confirmer son caractère irrégulier et discriminatoire par rapport aux autres membres de la section concernée et d'une manière générale des membres des autres services extérieurs de la Sûreté de l'État.

4.2. L'usage abusif de véhicules à des fins privées

Il est apparu des investigations que dans les deux cas dénoncés, les carnets de bord des véhicules concernés n'étaient pas tenus de la manière prescrite par la réglementation interne (les carnets de route doivent être remplis, par déplacement, avec soin, de manière complète et lisible).

Ainsi, à titre d'exemple significatif, le carnet de bord d'un véhicule utilisé du 17 mars 1998 au 1er septembre 1998 par la même personne, ne contient aucune indication pour cette période de huit mois au cours de laquelle le véhicule a parcouru un total d'un peu plus de 15 000 km.

Cette manière de procéder, dérogatoire à la réglementation interne en vigueur à la Sûreté de l'État, ne permet évidemment aucun contrôle sur l'utilisation faite des véhicules de services attribués à certaines personnes. *A posteriori*, il est donc impossible de vérifier aux conditions strictes rappelées par l'administrateur-generaal (zie supra);

— het niet toepassen van de bepalingen van het ministerieel besluit d.d. 23 juni 1997;

— de materiële wijziging van gegevens die aanvankelijk op de individuele prestatiefiches stonden, vermoedelijk met de bedoeling zich de opgegeven uren te doen uitbetalen.

4. ANDERE FEITELIJKE ELEMENTEN IN DE ANONIEME AANGIFTE VAN 16 FEBRUARI 1999

4.1. Het onterecht opgeven van sporturen als onregelmatige diensturen

In de anonieme aangifte wordt onder meer aangeklaagd dat sportactiviteiten, uitgeoefend tijdens de middagpauze, ten onrechte als bezoldigde onregelmatige prestaties worden opgegeven.

Na controle heeft de Dienst enquêtes van het Comité I inderdaad vastgesteld dat de voorwaarden van de interne richtlijnen niet waren nageleefd, met name dat dit type prestaties door het belang van de dienst moeten zijn vereist en het voorwerp moeten zijn van een bevel van het hoofd van de sectie of van de hoofdcommissaris.

Deze praktijk heeft echter betrekking op één persoon, wat de onregelmatige en discriminerende aard jegens de andere leden van de bedoelde sectie en, in het algemeen, jegens de leden van de andere buitendiensten van de Veiligheid van de Staat lijkt te bevestigen.

4.2. Het onterecht gebruik van voertuigen voor persoonlijke doeleinden

Uit het onderzoek blijkt dat in beide gevallen de reisboeken van de gebruikte voertuigen niet ingevuld waren, overeenkomstig de bepalingen voorgeschreven in de interne reglementen (bij elke verplaatsing moeten de reisboeken nauwkeurig, volledig en leesbaar worden ingevuld).

Het is veelzeggend dat het reisboek van een voertuig gebruikt van 17 maart 1998 tot 1 september 1998 door eenzelfde persoon, geen enkele vermelding bevat voor deze periode van acht maanden waarin het voertuig in totaal iets meer dan 15 000 km heeft gereden.

Deze handelwijze, die afwijkt van de vigerende interne reglementering bij de Veiligheid van de Staat, laat natuurlijk geen enkele controle toe van het gebruik van de dienstvoertuigen, toegewezen aan bepaalde personen. *A posteriori* is het dus onmogelijk

fier de manière certaines si, comme le prétendent les dénonciateurs anonymes, ces véhicules ont été utilisés de manière abusive en dehors des heures de service, durant les week-ends et même pendant les congés annuels et de maladie.

Toutefois, certains éléments mis en évidence par les investigations du Service d'enquêtes du Comité R permettent de constater que l'utilisation des véhicules à des fins strictement privées n'est pas à exclure.

De même, d'autres constatations relevées dans le rapport d'enquêtes à l'occasion d'un accident survenu avec un nouveau véhicule de service durant le mois de décembre 1998, ne font que confirmer le caractère peu transparent, et difficilement contrôlable, de certaines pratiques.

5. EXTRAITS DU COMPTE RENDU DE LA RÉUNION DU 3 DÉCEMBRE 1999 AVEC L'ADMINISTRATEUR GÉNÉRAL AD INTERIM DE LA SÛRETÉ DE L'ETAT, À PROPOS DE L'ENQUÊTE RELATIVE À LA SECTION «PROTECTION».

L'administrateur général *ad interim* déclare d'emblée être au courant des grandes lignes de l'enquête et avoir aussi vérifié les directives concernées en la matière.

Le président du Comité R expose que l'enquête a mis à jour des éléments qui permettraient de suspecter l'instauration d'un système accordant à ceux qui y participent le bénéfice d'avantages indus sur la base de prestations fictives ou exagérées. Ce système aurait été mis en place pour conserver, après la suppression des missions de protection de certains ministres, les avantages financiers liés à celles-ci.

La base légale pour la rémunération des prestations incriminées impose des conditions précises qui en l'espèce ne sont pas rencontrées. L'Arrêté ministériel du 23 juin 1997 évoqué par la Sûreté de l'État édicte que seules des heures réellement prestées peuvent être payées, alors qu'en l'espèce il s'agit d'heures de «stand-by» à domicile dont les justifications semblent insuffisantes; de surcroît, la mesure et les limites dans lesquelles un consensus préalable existerait sur ces pratiques au niveau de la hiérarchie de la Sûreté n'apparaîssent pas clairement.

L'enquête indiquerait une absence de normes précises applicables en l'espèce entraînant une déficience du contrôle interne qui aurait d'autre part pu également être abusé.

L'initiative de la dénonciation anonyme ne serait-elle pas à situer dans un contexte plus général d'un

met zekerheid vast te stellen of deze voertuigen, zoals de anonieme aanklagers beweren, onterecht zijn gebruikt buiten de diensturen, tijdens het weekend en zelfs gedurende de jaarlijkse vakantie en ziekteverlof.

Bepaalde elementen die tijdens het onderzoek van de Dienst enquêtes van het Comité I aan het licht zijn gekomen, laten toe vast te stellen dat het gebruik van de dienstvoertuigen voor louter persoonlijke doeleinden niet uit te sluiten is.

Ook andere vaststellingen in het onderzoeksrapport naar aanleiding van een ongeval met een nieuw dienstvoertuig tijdens de maand december 1998, bevestigen het weinig transparante en moeilijk controleerbare karakter van bepaalde praktijken.

5. VERSLAG VAN DE VERGADERING VAN 3 DECEMBER 1999 MET DE ADMINISTRATEUR-GENERAAL AD INTERIM VAN DE VEILIGHEID VAN DE STAAT, OVER HET ONDERZOEK BETREFFENDE DE SECTIE A 10

De administrateur-generaal *ad interim* verklaart onmiddellijk dat ze op de hoogte is van de grote lijnen van het onderzoek en dat ze de ter zake geldende richtlijnen heeft geraadpleegd.

De voorzitter van het Comité I deelt haar mee dat het onderzoek elementen aan het licht heeft gebracht op grond waarvan men kan vermoeden dat een systeem is ingevoerd waarbij de betrokkenen onterechte voordelen genieten voor fictieve of overdreven prestaties. Dit systeem zou zijn uitgewerkt om, na het afschaffen van de beschermingsopdrachten van bepaalde ministers, de daaraan verbonden financiële voordelen te behouden.

De wettelijke basis voor het bezoldigen van de aangeklaagde prestaties zou precieze voorwaarden opleggen die in dit geval niet worden nageleefd. Het ministerieel besluit d.d. 23 juni 1997, waarnaar de Veiligheid van de Staat verwijst, bepaalt dat alleen reëel gepresteerde uren mogen worden betaald. In het onderhavige geval gaat het echter om stand-by-uren thuis die onvoldoende bewezen lijken te zijn. Bovendien is niet duidelijk in welke mate en binnen welke beperkingen er een voorafgaande consensus zou bestaan met betrekking tot deze praktijken op het niveau van de hiërarchie van de Veiligheid van de Staat.

Uit het onderzoek blijkt dat er een gebrek zou zijn aan ter zake toepasbare duidelijke normen, met als gevolg een ontoereikende interne controle die anderzijds ook misleid zou kunnen zijn.

De vraag moet gesteld worden of het initiatief voor de anonieme aangifte niet moet worden gezocht in

mécontentement du personnel que ce soit à l'intérieur ou à l'extérieur de la section «protection».

Un membre du Comité R ajoute qu'il peut en tout cas être question ici d'un problème d'estompement de la norme et qu'il y aurait aussi des observations à formuler quant à l'utilisation des véhicules de service.

Mme l'administrateur général *ad interim* déclare qu'elle ne veut faire aucun commentaire concernant les cas particuliers. Elle est toutefois d'avis qu'il existe bien une base légale pour la compensation financière des heures de «stand-by». C'est la règle applicable dans le secteur public dont on trouve également les fondements juridiques dans le droit du travail et dans la jurisprudence.

Rester à disposition à domicile est une obligation, la question est de savoir comment compenser cette obligation? Dans l'arrêté ministériel du 23 juin 1997 il est question de missions précises données par le commissaire en chef, l'administrateur général adjoint ou l'administrateur général.

Mme l'administrateur général *ad interim* est bien d'accord sur le fait qu'aucun ordre de service n'existe pour ces prestations particulières. Il devrait être établi des directives qui seraient également d'application aux autres sections de la Sûreté de l'État. À la police judiciaire une telle réglementation est en cours d'élaboration. On éviterait ainsi dans l'avenir des dysfonctionnements dans le contrôle par le chef de section et par le directeur des opérations.

Le système actuel résulte d'un accord verbal entre différents niveaux de la hiérarchie. Cela aurait dû faire l'objet d'une note de service. Mme l'administrateur général *ad interim* maintient sa position suivant laquelle les compensations peuvent être déterminées dans le système actuel. Toutefois, après avoir reçu le rapport du Comité, les notes de service feront l'objet des adaptations nécessaires et les contrôles seront renforcés.

Le président du Comité R fait remarquer qu'en principe seules les heures réellement prestées devraient être compensées financièrement.

Il constate que cela va plus loin qu'un contrôle banal sur des heures prestées. En effet, d'une part on peut diagnostiquer un malaise réel susceptible de porter atteinte à l'efficacité des services et d'autre part, il n'est pas sans signification et sans importance de constater qu'aurait été mis en place au sein d'une section, un système particulier de compensation qui apparemment n'est pas applicable aux autres services extérieurs de la Sûreté de l'État.

L'administrateur général *ad interim* rappelle à ce sujet la nécessité d'un contrôle plus strict. Elle indique

een algemener context van mistevredenheid bij het personeel, het zij binnen of buiten de sectie «bescherming».

Een lid van het Comité I voegt eraan toe dat er in elk geval sprake kan zijn van een probleem van normvervaging en dat men opmerkingen kan maken betreffende het gebruik van de dienstvoertuigen.

Mevrouw de administrateur-generaal *ad interim* verklaart geen commentaar te geven op de afzonderlijke gevallen. Toch is ze van mening dat er wel degelijk een wettelijke basis bestaat voor de geldelijke bezoldiging van stand-by-uren, namelijk de regel die in de overheidssector toepasbaar is en waarvan men de juridische grondslagen vindt in het arbeidsrecht en in de rechtspraak.

Thuis ter beschikking blijven is een verplichting, maar hoe moet men deze verplichting vergoeden? In het ministerieel besluit d.d. 23 juni 1997 is er sprake van welomschreven opdrachten uitgaande van de hoofdcommissaris, de adjunct-administrateur-generaal of de administrateur-generaal.

Mevrouw de administrateur-generaal *ad interim* gaat ermee akkoord dat er voor deze bijzondere prestaties geen dienstorders bestaan. Men zou richtlijnen moeten opstellen die ook voor de andere secties van de Veiligheid van de Staat van toepassing zouden moeten zijn. Bij de gerechtelijke politie wordt momenteel een dergelijke reglementering uitgewerkt. Zo kunnen in de toekomst disfuncties worden voorkomen met betrekking tot het toezicht door het hoofd van de sectie en door de directeur operaties.

Het huidige systeem is het resultaat van een mondelinge overeenkomst tussen de verschillende niveaus van de hiërarchie. Deze overeenkomst had het voorwerp moeten zijn van een dienstnota. Mevrouw de administrateur-generaal *ad interim* houdt vol dat de compensaties binnen het huidige systeem kunnen worden vastgesteld, evenwel zullen de dienstnota's na ontvangst van het rapport van het Comité I, waar nodig worden aangepast en zullen de controles worden versterkt.

De voorzitter van het Comité I merkt op dat in principe alleen de reëel gewerkte uren geldelijk mogen worden gecompenseerd.

Hij stelt vast dat er meer aan de hand is dan een probleem met betrekking tot de controle van de gewerkte uren. Enerzijds is er inderdaad sprake van een reële malaise die de doeltreffende werking van de diensten kan schaden, anderzijds is het niet zonder betekenis en zonder belang vast te stellen dat binnen een sectie een bijzonder compensatiesysteem werd opgezet dat blijkbaar niet geldt voor de andere buitendiensten van de Veiligheid van de Staat.

In verband hiermee herhaalt de administrateur-generaal *ad interim* dat een strengere controle nood-

aussi que ce type de situation pourrait être solutionné si les services pouvaient disposer de plus de personnel.

Par courrier du 18 janvier 2000, Mme l'administrateur général *ad interim* a communiqué ses observations relatives au compte rendu de la réunion du 3 décembre 1999.

Elle rappelle « avoir été plus précise quant à la base légale pour la compensation financière des heures de « stand-by » qui pour elle sont les suivantes :

— la directive (CE) 93/104 du 23.11 1993 du Conseil concernant certains aspects de l'aménagement du temps de travail;

L'article 2 de cette directive définit la notion « temps de travail », comme « toute période durant laquelle le travailleur est au travail, à la disposition de l'employeur et dans l'exercice de son activité ou de ses fonctions, conformément aux législations et/ou pratiques nationales »;

— l'article 19 de la loi du 16.03 1971 sur le travail.

Cet article définit la durée du travail, à savoir « le temps pendant lequel le personnel est à la disposition de l'employeur ». Cet article peut être appliqué par analogie au secteur public.

— La jurisprudence précise en matière de repos compensatoire, qu'il n'est pas nécessaire que la personne travaille effectivement, qu'elle soit sur le lieu de travail. De plus, la loi ne prévoit pas le mode de paiement. Les parties sont libres de déterminer le mode de compensation.

— L'arrêté ministériel du 23 juin 1997, octroyant aux membres du personnel des services extérieurs de l'administration de la Sûreté de l'État une allocation pour service irrégulier, notamment pour les services effectifs requis pour l'exécution d'une mission précise ordonnée par le commissaire en chef, l'administrateur général adjoint ou l'administrateur général. »

Mme l'administrateur général *ad interim* précise dans le même courrier que si elle « a déclaré que l'enquête sur le fonctionnement de la section « protection », crée un malaise au sein de cette section et du service, c'est parce que cette enquête a pris plusieurs mois et a eu lieu suite à une dénonciation anonyme émanant d'un membre des services extérieurs (faisant partie ou proche de la section « protection »). »

6. CONCLUSIONS DU COMITÉ R

6.1. Sur la base des faits dénoncés dans la lettre anonyme du 16 février 1999, ainsi que de ceux mis en lumière au cours des investigations du Service

zakelijk is. Ze zegt ook dat dit soort situaties zouden kunnen worden opgelost indien de diensten over meer personeel zouden kunnen beschikken.

In haar brief d.d. 18 januari 2000 heeft mevrouw de administrateur-generaal *ad interim* kennis gegeven van haar opmerkingen over het verslag van de vergadering van 3 december 1999.

Ze wijst erop « dat ze preciezer is geweest in haar verklaring over de wettelijke grondslagen voor het geldelijk compenseren van stand-by-uren die volgens haar de volgende zijn :

— de richtlijn (EG) 93/104 d.d. 23 november 1993 van de Raad betreffende een aantal aspecten van de organisatie van de arbeidstijd;

Artikel 2 van deze richtlijn omschrijft het begrip « arbeidstijd » als « de tijd waarin de werknemer werkzaam is, ter beschikking van de werkgever staat en zijn werkzaamheden of functie uitoefent, overeenkomstig de nationale wetten en/of gebruiken »;

— artikel 19 van de wet d.d. 16 maart 1971 op de arbeid.

Dit artikel omschrijft de arbeidsduur als « de tijd waarin het personeel ter beschikking staat van de werkgever ». Dit artikel kan naar analogie worden toegepast op de overheidssector.

— Met betrekking tot compenserende rust bepaalt de rechtspraak dat het niet noodzakelijk is dat de betrokkene effectief werkt, dat hij op de werkplaats aanwezig is. Bovendien voorziet de wet geen wijze van betaling. De partijen zijn vrij om de wijze van compensatie te bepalen.

— Het ministerieel besluit d.d. 23 juni 1997, dat aan de personeelsleden van de buitendiensten van het Bestuur van de Veiligheid van de Staat een toelage toekent voor onregelmatige dienst, met name voor effectieve diensten vereist voor de uitvoering van een precieze opdracht bevolen door de hoofdcommissaris, de adjunct-administrateur-generaal of de administrateur-generaal. »

In dezelfde brief preciseert mevrouw de administrateur-generaal *ad interim* dat indien ze « heeft verklaard dat het onderzoek over de werking van de sectie « bescherming » binnen deze sectie en binnen de dienst een malaise creëert, dat komt omdat dit onderzoek maanden heeft aangesleept en gevoerd is tengevolge van een anonieme aangifte van een lid van de buitendiensten (dat deel uitmaakt van de sectie « bescherming » of er nauw mee verbonden is). »

6. CONCLUSIES VAN HET COMITÉ I

6.1. Op grond van de feiten die worden aangeklaagd in de anonieme brief van 16 februari 1999 en van de feiten die aan het licht zijn gekomen tijdens het

d'enquêtes le Comité permanent R, constate à ce niveau l'existence d'indices sérieux selon lesquels un système d'octroi d'avantages indus, reposant sur des pratiques peu transparentes et donc difficilement contrôlables, aurait été mis en place au sein de la section « protection » de la Sûreté de l'État.

6.2. Certaines de ces pratiques ont conduit à l'altération matérielle incontestable de certains documents devant servir de justification à l'octroi de rémunérations pour prestations irrégulières.

6.3. Sur le plan de l'organisation interne de la Sûreté de l'État, le Comité permanent R constate que de telles situations ont été rendues possibles :

— par l'absence de notes internes et de directives suffisamment précises et réactualisées;

— par l'absence corrélative d'un système de contrôle interne efficace et vigilant.

6.4. Sur le plan du fonctionnement et de l'efficacité des services, le Comité permanent R constate que les faits repris dans le présent rapport, par leur persistance dans le temps, ont provoqué pour le moins des sentiments d'injustice et d'impuissance suffisamment exacerbés pour justifier le recours à une dénonciation anonyme, adressée à l'extérieur de l'Administration de la Sûreté de l'État.

On peut s'interroger enfin sur les influences négatives qu'un tel climat peut avoir non seulement sur le fonctionnement de la section concernée elle-même, mais aussi sur l'ensemble des agents des autres services extérieurs de la Sûreté de l'État.

On doit rappeler en effet qu'un des problèmes soulevés au cours du présent contrôle concerne essentiellement le paiement des heures de « stand-by » sans base réglementaire mais fondé sur le mode de rémunération prévu par l'arrêté ministériel du 23 juin 1997, octroyant aux membres du personnel des services extérieurs de la Sûreté de l'État une allocation pour service irrégulier.

En Belgique, seul le personnel de la section « protection » de la Sûreté de l'État semble bénéficier d'une interprétation extensive de l'Arrêté ministériel précité et ce avec l'accord de sa hiérarchie.

Cette attitude conduit inexorablement au constat d'un traitement dissemblable entre des fonctionnaires d'une même administration travaillant par ailleurs dans des conditions identiques.

En effet, la disponibilité dont doit faire preuve le personnel de service de semaine (en dehors de sa présence obligatoire dans les locaux de cette administration) ou certaines sections particulières soumises à

onderzoek van de Dienst enquêtes stelt het Comité I vast dat er ernstige aanwijzingen bestaan van het feit dat binnen de sectie « bescherming » van de Veiligheid van de Staat een systeem is ingevoerd waarbij ten onrechte voordelen worden toegekend en dat steunt op weinig transparante en bijgevolg moeilijk controleerbare praktijken.

6.2. Sommige van deze praktijken hebben geleid tot de onbetwistbare materiële wijziging van bepaalde documenten die moeten dienen tot staving voor de toekenning van toelagen voor onregelmatige prestaties.

6.3. Met betrekking tot de interne organisatie van de Veiligheid van de Staat stelt het Comité I vast dat dergelijke situaties mogelijk zijn gemaakt :

— door het ontbreken van bijgewerkte interne nota's en voldoende duidelijke richtlijnen;

— door het daarmee gepaard gaand ontbreken van een doeltreffend en waakzaam systeem van intern toezicht.

6.4. Met betrekking tot de werking en de doelmatigheid van de diensten stelt het Comité I vast dat de in dit rapport beschreven feiten, ingevolge hun landurig bestaan, op zijn minst hebben geleid tot gevoelens van onrechtvaardigheid en onmacht die zodanig zijn geescaleerd dat toevlucht werd genomen tot een anonieme aangifte die ze hebben verstuurd naar een organisme buiten het Bestuur van de Veiligheid van de Staat.

Tot slot kan men vragen stellen over de negatieve invloed die een dergelijk klimaat kan hebben, niet alleen op de werking van de betrokken sectie zelf maar ook op alle agenten van de andere buitendiensten van de Veiligheid van de Staat.

Immers, een van de problemen die in het kader van deze controle naar voren zijn gekomen betreft in hoofdzaak de vergoeding van stand-by-uren, waarvoor geen reglementaire basis bestaat maar die steunt op de wijze van vergoeding bedoeld in het ministerieel besluit d.d. 23 juni 1997 houdende toekenning van een toelage voor onregelmatige dienst aan de personeelsleden van de buitendiensten van de Veiligheid van de Staat.

In België lijkt alleen het personeel van de sectie « bescherming » van de Veiligheid van de Staat een uitgebreide interpretatie van voornoemd ministerieel besluit te genieten, met de goedkeuring van de hiërarchie.

Een dergelijke houding heeft onvermijdelijk tot gevolg dat er sprake is van een ongelijke behandeling van ambtenaren van eenzelfde administratie die overigens onder identieke voorwaarden werken.

Immers, de beschikbaarheid waarvan het personeel met weekdienst (buiten de verplichte aanwezigheid in de lokalen van dit bestuur) blijk moet geven, alsook bepaalde bijzondere secties onderworpen aan soort-

des obligations de disponibilités semblables en cas de « stand-by » prestés le week-end, ne se distingue nullement de la disponibilité dont les membres de la section protection doivent faire preuve.

Les uns sont rémunérés tandis que les autres ne le sont pas, alors qu'ils appartiennent à la même administration.

De plus, comme il a été constaté au cours de cette enquête, ce type de gestion particulière basé sur un « consensus oral » aboutit immanquablement à des dérives dans lesquelles la limite avec des comportements pénalement répréhensibles n'est plus très loin.

7. LES RECOMMANDATIONS DU COMITÉ R

7.1. Il convient d'une manière générale d'actualiser, et le cas échéant, de réécrire certaines notes de services et particulièrement celles dont le caractère obsolète risque de contribuer au glissement rapide d'une phase d'estompement de la norme vers celle de l'instauration d'un contexte d'anomie.

7.2. Il convient aussi de rappeler et d'exiger le strict respect des notes de service tout en instaurant (ou en restaurant ...?) un contrôle interne plus efficace, c'est-à-dire moins formel plus approprié et plus approfondi (ne serait-ce que par coups de sondes).

7.3. Enfin, en ce qui concerne la problématique des heures de stand-by, il conviendrait que la Sûreté de l'État élabore définitivement un texte normatif applicable à l'ensemble de ses fonctionnaires.

N.B. **Dans un souci d'objectivité, il convient de signaler que le président du Comité R a été informé le 21 mars 2000, par Mme l'administrateur général *ad interim* que, dès le 18 janvier 2000, des mesures ont été prises allant dans le sens des présentes recommandations.**

CHAPITRE 2

Rapport relatif à l'enquête de contrôle sur base d'une plainte d'un particulier concernant une habilitation de sécurité

1. PROCÉDURE

Le 23 juillet 1999, le Comité R a reçu une lettre d'un particulier se plaignant d'avoir, dès mars 1999, perdu son emploi de chauffeur au cabinet du ministre de la Défense nationale à la suite de la modification du degré de son habilitation de sécurité, celle-ci passant du niveau « secret » à celui de « confidentiel ».

D'après le plaignant, ce changement aurait été décidé à la suite d'une « grosse enquête effectuée au

gelijke verplichtingen inzake beschikbaarheid in geval van « stand-by » tijdens het weekend, verschilt in niets van de beschikbaarheid waarvan de leden van de sectie bescherming blijk moeten geven.

De enen worden vergoed, de anderen niet, ook al maken ze deel uit van dezelfde administratie.

Bovendien, zoals tijdens dit onderzoek is vastgesteld, leidt dit soort bijzonder beheer op grond van een « mondelinge consensus » onvermijdelijk tot afwijkingen waarbij men gevaarlijk dicht in de buurt komt van op penaal vlak strafbare gedragingen.

7. AANBEVELINGEN VAN HET COMITÉ I

7.1. Het is, in het algemeen, aangewezen om bepaalde dienstnota's te actualiseren en eventueel te herschrijven, in het bijzonder de dienstnota's waarvan het verouderd karakter het gevaar meebrengt dat ze bijdragen tot het snelle afglijden van een fase van normvervaging naar een fase van normeloosheid.

7.2. Voorts past het erop te wijzen en te eisen dat de dienstnota's strikt moeten worden nageleefd, en tegelijk een doeltreffender intern toezicht in te voeren (of opnieuw in te voeren ...?), dat wil zeggen minder formeel, adequater en grondiger (al was het maar steekproefsgewijs).

7.3. Tot slot, met betrekking tot het probleem van de stand-by-uren, zou het passen dat de Veiligheid van de Staat eens en voorgoed een normatieve tekst opstelt die voor al haar ambtenaren van toepassing is.

N.B. **In een streven naar objectiviteit, past het te vermelden dat mevrouw de administrateur-generaal *ad interim* de voorzitter van het Comité I op 21 maart 2000 heeft gemeld dat ze reeds op 18 januari 2000, maatregelen heeft genomen die tegemoet komen aan de huidige aanbevelingen.**

HOOFDSTUK 2

Verslag over het toezichtsonderzoek naar aanleiding van een klacht van een particulier betreffende een veiligheidsmachtiging

1. PROCEDURE

Op 23 juli 1999 ontving het Comité I een brief van een particulier die zich erover beklaagde dat hij vanaf maart 1999 zijn baan als chauffeur op het kabinet van de minister van Landsverdediging had verloren tengevolge van de wijziging van zijn veiligheidsmachtiging, die van het niveau « geheim » naar het niveau « vertrouwelijk » was gedaald.

Volgens de klager was deze wijziging het gevolg van een « groot onderzoek op het kabinet », dat door

sein du cabinet » par le SGR, sans que l'intéressé soit informé par ailleurs, à un moment quelconque, d'une éventuelle sanction prise à son égard.

Le 27 juillet 1999, le Comité R a décidé d'ouvrir une enquête sur la base de cette plainte. Un membre a été désigné pour suivre le déroulement de ce dossier.

Le 29 juillet 1999, en application de l'article 32 de la loi organique du contrôle des services de police et de renseignements, monsieur le président du Sénat a été avisé de l'ouverture de cette enquête. Le même jour une apostille était transmise au chef du Service d'enquêtes du Comité R dans le but de procéder au préalable à l'audition circonstanciée du plaignant et d'informer le Comité du résultat de cette audition.

Le 9 août 1999, les résultats de cette audition ont été transmis au président du Comité R.

L'intéressé n'a pas souhaité garder l'anonymat, comme cela peut lui être garanti par l'article 40, 2e alinéa de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le 15 septembre 1999, il était demandé par apostille complémentaire adressée au chef du Service d'enquêtes de se rendre au SGR dans le but de prendre connaissance et éventuellement copie du dossier de l'intéressé et de vérifier pour quelles raisons et dans quelles circonstances celui-ci avait vu son certificat de sécurité OTAN du degré « secret » remplacé par un certificat de sécurité OTAN de niveau « confidentiel ».

Le 16 septembre 1999, le chef du Service d'enquêtes du Comité R avertissait le ministre de la Défense nationale de l'enquête relative au SGR, conformément à l'article 43,§ 1, de la loi organique du contrôle des services de police et de renseignements.

Le 20 octobre 1999, le chef du Service d'enquêtes transmettait les résultats de la consultation du dossier de l'intéressé au Comité R.

Le présent rapport a été approuvé par les membres du Comité R lors de la réunion du 3 mai 2000.

2. LA PLAINTE DE MONSIEUR M

Dans son courrier, monsieur M, militaire de carrière, rappelle qu'il occupe une fonction au secrétariat administratif et technique au cabinet de la Défense nationale depuis de très nombreuses années.

Il reconnaît avoir fait établir à son attention, alors qu'il était en indisponibilité pour maladie à la fin de l'année 1998, un ordre de marche OTAN injustifié lui permettant de se rendre en Allemagne dans une base

de SGR werd gevoerd. Overigens zou de betrokkene op geen enkel moment kennis hebben gekregen van enige sanctie tegen hem.

Op 27 juli 1999 besliste het Comité I een onderzoek te openen naar aanleiding van deze klacht. Een lid van het Comité kreeg de opdracht het verloop van dit dossier te volgen.

Op 29 juli 1999 werd de heer voorzitter van de Senaat, overeenkomstig artikel 32 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten, op de hoogte gebracht van de opening van dit onderzoek. Diezelfde dag werd een kantschrift verzonden naar het hoofd van de Dienst Enquêtes van het Comité I, teneinde vooraf over te gaan tot het omstandig verhoor van de klager en het Comité kennis te geven van het resultaat van dit verhoor.

Op 9 augustus 1999 werden de resultaten van dit verhoor bezorgd aan de voorzitter van het Comité I.

De betrokkene wenste niet anoniem te blijven, hoewel hij daartoe het recht had krachtens artikel 40, 2e lid van de wet d.d. 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten.

Op 15 september 1999 werd een aanvullend kantschrift bezorgd aan het hoofd van de Dienst Enquêtes, met het verzoek zich naar de SGR te begeven teneinde er het dossier van de betrokkene in te zien en het eventueel te kopiëren, alsmede om na te gaan waarom en in welke omstandigheden het NAVO-veiligheidscertificaat van het niveau « geheim » van de betrokkene was vervangen door een NAVO-veiligheidscertificaat van het niveau « vertrouwelijk ».

Op 16 september 1999 bracht het hoofd van de Dienst Enquêtes van het Comité I de minister van Landsverdediging op de hoogte van het onderzoek met betrekking tot de SGR, overeenkomstig artikel 43, § 1, van de wet tot regeling van het toezicht op de politie- en inlichtingendiensten.

Op 20 oktober 1999 bezorgde het hoofd van de Dienst Enquêtes de resultaten van de inzage van het dossier van de betrokkene aan het Comité I.

De leden van het Comité I hebben het onderhavige verslag goedgekeurd op de vergadering van 3 mei 2000.

2. DE KLACHT VAN DE HEER M

In zijn brief schrijft de heer M, die beroepsmilitair is, dat hij sinds vele jaren een functie bekleedt op het administratief en technisch secretariaat van het kabinet van Landsverdediging.

Hij geeft toe dat hij eind 1998, hoewel hij toen arbeidsonbekwaam was wegens ziekte, een ongerechtvaardigd NAVO-marsorder heeft laten opmaken waarmee hij naar een geallieerde basis in Duitsland

militaire alliée pour effectuer des achats à moindre coût.

Il signale également que ces faits ont donné lieu à une enquête judiciaire, mais qu'à sa connaissance, il n'y a eu ni sanction pénale, ni sanction disciplinaire à son égard.

En mars 1999, le plaignant recevait cependant une lettre recommandée l'informant qu'il était remis à disposition de l'armée. Se renseignant sur les raisons de cette décision, monsieur M signale qu'il lui fut répondu sans plus que son renvoi du cabinet de la Défense nationale était la conséquence du retrait de son degré de sécurité « secret ».

Le plaignant continue cependant à s'interroger sur les raisons de ce retrait et il évoque la possibilité que celles-ci soient en relation avec des difficultés financières personnelles.

Il pense que le SGR aurait eu connaissance de celles-ci à l'occasion d'une mission effectuée à la demande du ministre par ce service au cabinet de la Défense nationale.

Considérant qu'il reçoit une « punition de la part du SGR », il demande l'intervention du Comité R pour le défendre.

3. L'AUDITION DU PLAIGNANT PAR LE SERVICE D'ENQUÊTES DU COMITÉ R

Cette audition, ainsi que les documents qui ont été spontanément remis par le plaignant, ont permis de confirmer, tout en les précisant davantage, les éléments de la plainte.

Il ressort clairement de cette audition que l'intéressé est convaincu que ses ennuis financiers sont seuls à l'origine de la perte de son habilitation de sécurité du degré « secret ».

Monsieur M reconnaît d'autre part qu'étant en congé de maladie, il a fait établir, par une tierce personne, un faux ordre de marche OTAN dans le but de se rendre en Allemagne, dans une base militaire alliée pour y faire des achats de Noël.

Il ressort d'une copie d'un procès-verbal de la police judiciaire auprès de la justice militaire, remise spontanément par le plaignant, que celui-ci fut interpellé, selon ses propres termes, « par les américains » à la sortie du magasin.

En ce qui concerne ces derniers faits, monsieur M ne semble pas les considérer, aussi bien dans sa plainte écrite que dans son audition, comme suffisants pour constituer une/ou des raison(s) susceptible(s) de justifier la perte de son degré de sécurité « secret ». Il conclut d'ailleurs ses déclarations par cette constatation : « Malgré mes efforts, je n'arrive pas à connaître les raisons qui justifient ce déclassement. Je souhaite

kon gaan om er tegen voordelige prijzen inkopen te doen.

Hij verklaart ook dat deze feiten aanleiding hebben gegeven tot een gerechtelijk onderzoek, maar dat er voor zover hij weet geen strafrechtelijke sanctie noch een tuchtstraf tegen hem is uitgesproken.

Niettemin ontving de klager in maart 1999 een aangetekende brief waarin hem werd gemeld dat hij opnieuw ter beschikking van het leger werd gesteld. De heer M verklaart dat hij heeft gepoogd te achterhalen wat de redenen van deze beslissing waren en dat hij alleen heeft vernomen dat zijn ontslag op het kabinet van Landsverdediging het gevolg was van de intrekking van zijn veiligheidsniveau « geheim ».

De klager blijft echter met vragen zitten over de redenen van deze intrekking. Volgens hem bestaat de mogelijkheid dat deze redenen verband houden met zijn persoonlijke financiële problemen.

Hij denkt dat de SGR weet zou hebben gekregen van zijn problemen toen deze dienst op verzoek van de minister een opdracht uitvoerde op het kabinet van Landsverdediging.

Overwegende dat « de SGR hem een straf oplegt », vraagt hij aan het Comité I tussen te komen en hem te verdedigen.

3. VERHOOR VAN DE KLAGER DOOR DE DIENST ENQUÊTES VAN HET COMITÉ I

Dit verhoor en de documenten die de klager uit eigen beweging heeft overhandigd, hebben het mogelijk gemaakt de elementen van de klacht te bevestigen, alsook ze preciezer te omschrijven.

Uit het verhoor blijkt duidelijk dat de betrokkene ervan overtuigd is dat zijn financiële problemen de enige reden zijn van het verlies van zijn veiligheidsmachtiging op het niveau « geheim ».

Anderzijds geeft de heer M toe dat hij, toen hij met ziekteverlof was, aan een derde heeft gevraagd om voor hem een vals NAVO-marsorder op te maken waarmee hij naar een geallieerde militaire basis in Duitsland kon gaan om er zijn kerstinkopen te doen.

Uit een kopie van een proces-verbaal van de gerechtelijke politie bij het militair gerecht, die de klager spontaan heeft overhandigd, blijkt dat hij bij het verlaten van de winkel « door de Amerikanen », zoals hij zelf zegt, werd tegengehouden.

In zijn schriftelijke klacht en in zijn verhoor blijkt nergens dat de heer M deze laatste feiten als voldoende lijkt te beschouwen om een van de redenen of dé reden te vormen die het verlies van zijn veiligheidsniveau « geheim » rechtvaardigt (rechtvaardigen). Overigens besluit hij zijn verklaringen met de volgende vaststelling : « Ondanks mijn inspanningen slaag ik er niet in de redenen te achterhalen die deze

que vos services se renseignent sur les motifs de ce « déclassement. »

4. LA CONSULTATION AU SGR DU DOSSIER DU PLAIGNANT

Il résulte de la consultation du dossier de monsieur M par le Service d'enquêtes du Comité R les constatations suivantes.

Le plaignant a reçu son premier certificat de sécurité de niveau « confidentiel » en 1980 pour une période allant jusqu'en 1985.

En 1997, un document émanant de l'état-major général fait état de l'existence de problèmes financiers dans le chef de l'intéressé.

Cette information n'empêche pas qu'en janvier 1998, sur demande du cabinet du ministre de la Défense nationale et après l'enquête de sécurité menée par le SGR, le certificat de sécurité de l'intéressé soit porté du degré « confidentiel » au degré « secret ».

Ce n'est qu'après avoir eu connaissance en 1999 de l'existence d'une procédure judiciaire à charge du plaignant qu'interviendra la communication par le SGR au cabinet de la Défense nationale de la déclassification du certificat de sécurité de monsieur M de « secret » en « confidentiel ».

5. LES CONSTATATIONS ET COMMENTAIRES

5.1. Concernant la plainte de monsieur M

Les règles générales à suivre en matière de sécurité militaire tiennent compte des textes légaux, des circulaires ministérielles, des règlements, ordres généraux et autres directives qui trouvent leur origine dans les conventions interalliées. Ces dispositions sont applicables à toutes les forces armées et à tous les organismes qui dépendent du ministère de la Défense nationale.

Selon ces règles, le certificat de sécurité est un document qui atteste que la personne identifiée par ce document peut avoir accès à l'information dont la classification est identique ou inférieure à celle mentionnée sur le certificat.

Il est également précisé en cette matière que « toute personne, civile ou militaire, appelée, dans l'exercice de ses fonctions, à avoir accès à des renseignements classifiés « confidentiel » ou au dessus devrait faire l'objet au préalable d'une habilitation de sécurité » et que « lorsque des personnes telles que les huissers, les gardiens de nuit, etc ... sont employés dans des conditions qui leur fournissent l'occasion spéciale d'avoir involontairement accès à des renseignements classi-

declassering rechtvaardigen. Ik wens dat uw diensten inlichtingen inwinnen over de redenen van deze « declassering. »

4. INZAGE VAN HET DOSSIER VAN DE KLAGER BIJ DE SGR

De inzage van het dossier van de heer M heeft de Dienst Enquêtes van het Comité I toegelaten de volgende vaststellingen te maken.

In 1980 ontving de klager zijn eerste veiligheidscertificaat van het niveau « vertrouwelijk »; het certificaat was geldig tot in 1985.

In 1997 stelde de generale staf een document op waarin te lezen staat dat de betrokkene met financiële moeilijkheden kampt.

Toch werd het niveau van het veiligheidscertificaat van de betrokkene in januari 1998 op verzoek van het kabinet van de minister van Landsverdediging, en nadat de SGR een veiligheidsonderzoek had gevoerd, verhoogd van « vertrouwelijk » tot « geheim ».

Pas nadat de SGR in 1999 had vernomen dat tegen de klager een gerechtelijke procedure werd gevoerd, meldde de SGR aan het kabinet van Landsverdediging dat het veiligheidscertificaat van de heer M was gedeclasseerd van het niveau « geheim » naar het niveau « vertrouwelijk ».

5. VASTSTELLINGEN EN COMMENTAAR

5.1. Betreffende de klacht van de heer M

De algemene regels die inzake militaire veiligheid moeten worden nageleefd, houden rekening met de wetteksten, ministeriële omzendbrieven, reglementen, algemene orders en andere richtlijnen die hun oorsprong vinden in de verdragen tussen de geallieerden. Deze bepalingen zijn van toepassing op alle strijdkrachten en alle organen die onder de bevoegdheid van het ministerie van Landsverdediging vallen.

Overeenkomstig deze regels is het veiligheidscertificaat een document dat bevestigt dat de in het document geïdentificeerde persoon bevoegd is om toegang te hebben tot de informatie waarvan de classificatie gelijk is aan of lager dan de classificatie vermeld op het certificaat.

In deze materie wordt eveneens bepaald dat « eender wie, burger of militair, die in de uitoefening van zijn functies toegang moet hebben tot inlichtingen geklasseerd als « vertrouwelijk » of daarboven, voorafgaand het voorwerp zou moeten zijn van een veiligheidsmachtiging » en dat « wanneer personen zoals portiers, nachtwakers enz. worden tewerkgesteld in omstandigheden die hen de bijzondere gelegenheid bieden onvrijwillig toegang te hebben tot

fiés, il faudrait qu'elles soient titulaires d'une habilitation de sécurité comme si elles étaient en fait autorisées à avoir accès à ces renseignements».

Il convient, à ce propos, de souligner que monsieur M lui-même déclare en fin de son audition: «Souvent, je transportais des documents destinés à l'OTAN. Nous avions d'ailleurs, mes collègues et moi-même, une carte donnant accès à l'OTAN.»

Dans la formulation de sa plainte monsieur M attribue la diminution du degré de son certificat de sécurité à la consultation de son dossier personnel par un officier du SGR, lors de l'exécution par celui-ci, fin 1998, d'une autre mission de sécurité au cabinet de la Défense nationale, révélant ainsi au SGR l'existence des dettes de l'intéressé.

Il convient de souligner que l'existence de dettes est considérée comme un risque pour la sécurité qui doit être évalué et traité en tant que tel.

L'hypothèse du plaignant est cependant infirmée par les constatations faites lors de l'examen par le Service d'enquêtes du Comité R de son dossier au SGR puisque, comme mentionné ci-dessus, nonobstant la connaissance lors de l'enquête de sécurité de sa situation financière difficile, un degré de sécurité «secret» supérieur à celui qu'il possédait précédemment lui a été attribué par le SGR en 1998.

Il faut remarquer que le présent cas illustre paradoxalement le fait que des difficultés financières constituent bel et bien un facteur de risques au niveau de la sécurité puisque le plaignant lui-même fait référence à sa situation financière précaire pour expliquer sa demande d'établissement d'un faux ordre de marche OTAN devant lui permettre de faire des achats à moindre coût dans une base militaire en Allemagne.

Ce ne sera cependant qu'à la suite de l'interpellation de l'intéressé en Allemagne et de l'enquête consécutive ouverte par l'Auditorat militaire que le degré de sécurité «secret» du plaignant lui sera retiré. Il faut constater à ce sujet que la consultation des pièces par le Service d'enquêtes du Comité R révèle que l'officier en charge du dossier avait, dans un premier temps, proposé le retrait pur et simple du certificat de sécurité. Cette proposition n'a toutefois pas été suivie par la hiérarchie du SGR qui a décidé de réduire à «confidentiel» le degré du certificat de sécurité de monsieur M en attendant les suites du dossier judiciaire. Le cabinet du ministre de la Défense nationale a cependant considéré que l'intéressé ne pouvait plus de ce fait y rester en fonction.

Le retrait du degré de sécurité «secret» ne peut en aucun cas être considéré comme une sanction. Il

geklasseerde inlichtingen, zij houder zouden moeten zijn van een veiligheidsmachtiging alsof ze in feite gemachtigd waren om toegang te hebben tot deze inlichtingen».

In verband hiermee past het op te merken dat de heer M op het einde van zijn verhoor zelf verklaart: «Ik vervoerde vaak documenten bestemd voor de NAVO. Mijn collega's en ikzelf hadden trouwens een kaart die ons toegang gaf tot de NAVO.»

In zijn klacht schrijft de heer M de vermindering van het niveau van zijn veiligheidscertificaat toe aan het feit dat een officier van de SGR kennis heeft genomen van zijn persoonlijk dossier toen hij eind 1998 een andere veiligheidsopdracht uitvoerde op het kabinet van Landsverdediging. Op die manier kwam de SGR te weten dat de betrokkene schulden had.

Het past erop te wijzen dat het bestaan van schulden wordt beschouwd als een risico voor de veiligheid, dat als zodanig moet worden beoordeeld en behandeld.

Deze hypothese van de klager wordt echter ontkracht door de vaststellingen die de Dienst Enquêtes van het Comité I maakte bij het onderzoek van het dossier van de betrokkene bij de SGR. Immers, zoals hierboven al vermeld, kende de SGR hem in 1998 een veiligheidsniveau «geheim» toe, dit is hoger dan het niveau dat hij voorheen had, ook al had de SGR bij het verrichten van het veiligheidsonderzoek kennis gekregen van de moeilijke financiële situatie waarin de betrokkene verkeerde.

We merken op dat dit geval op paradoxale wijze een illustratie is van het feit dat financiële problemen wel degelijk een risicofactor vormen met betrekking tot de veiligheid, aangezien de klager zelf verwijst naar zijn precaire financiële situatie als verklaring voor zijn verzoek om een vals NAVO-marsorder op te maken waarmee hij tegen voordelige prijzen inkopen kon doen op een militaire basis in Duitsland.

Echter, pas na de interpellatie van de betrokkene in Duitsland en het navolgend onderzoek door het Krijgsauditoraat werd het veiligheidsniveau «geheim» van de klager afgenomen. In verband hiermee stellen we vast dat uit de inzage van de stukken door de Dienst Enquêtes van het Comité I is gebleken dat de officier die met het dossier was belast aanvankelijk had voorgesteld het veiligheidscertificaat zelf in te trekken. De hiërarchie van de SGR is niet op dit voorstel ingegaan, maar besliste het veiligheidscertificaat van de heer M te verminderen tot het niveau «vertrouwelijk» en voor het overige het vervolg van het gerechtelijk dossier af te wachten. Niettemin oordeelde het kabinet van de minister van Landsverdediging dat de betrokkene er niet langer in dienst kon blijven als gevolg van de verlaging van zijn veiligheidsniveau.

Het afnemen van het veiligheidsniveau «geheim» kan in geen geval als een sanctie worden beschouwd.

résulte tout simplement de l'application des règles de sécurité.

Dans le cas d'espèce on doit même souligner que cette application a toujours été faite dans un sens plutôt favorable au plaignant.

Une décision défavorable constitue une mesure administrative préventive prise dans le cadre de la sécurité militaire. Cette mesure ne doit pas être considérée comme une sanction et ne peut, en principe, porter aucun préjudice à la carrière militaire de l'intéressé. En l'espèce, le Comité R constate que si l'intéressé a perdu, suite à son renvoi du cabinet du ministre de la Défense nationale les indemnités spécifiques à ce détachement, il n'a encouru aucun préjudice au niveau de sa carrière militaire puisque remis à disposition de sa force d'origine, il y a conservé le même grade et la même fonction de chauffeur.

Comme on l'a vu d'autre part, la mesure de sécurité prise par le SGR résulte de l'ouverture par l'Auditorat militaire d'un dossier judiciaire à charge du plaignant entraînant la constatation du manque de fiabilité de ce dernier.

A cet égard, la réglementation en vigueur rappelle qu'en ce qui concerne la responsabilité individuelle dans le domaine de la sécurité militaire et en dehors des responsabilités de commandement et des tâches spécifiques attribuées à l'officier de sécurité, il importe que chaque membre des forces armées, quels que soient sa catégorie, son rang ou son grade, assume une responsabilité individuelle dans cette matière. Cela implique qu'il soit au courant des règlements, directives et normes applicables à lui-même et à son entourage et qu'il les applique dans la pratique.

5.2. Concernant le dossier du SGR

Le Service d'enquêtes du Comité R a constaté à l'occasion de cette enquête que le SGR n'a pas encore commencé la numérotation chronologique des pièces contenues dans ces dossiers, comme cela avait déjà été recommandé par le Comité R en 1996 à la suite de l'enquête de contrôle relative à la destruction des archives.

Il a également été constaté à la lecture du dossier du SGR qu'on ne retrouve la trace d'aucun suivi concernant la validité dans le temps du certificat de sécurité de monsieur M. C'est ainsi qu'au cours d'une période allant de 1985 à 1998, l'intéressé n'était apparemment plus en possession d'un certificat valable.

En effet, le premier certificat de sécurité de monsieur M fut délivré en 1980 avec une durée de validité

Het is gewoon het gevolg van de toepassing van de veiligheidsregels.

In het onderhavige geval moeten we zelfs benadrukken dat deze toepassing telkens is gebeurd eerder in het voordeel van de klager.

Een ongunstige beslissing is een preventieve administratieve maatregel genomen met het oog op de militaire veiligheid. Deze maatregel moet niet als een sanctie worden beschouwd en kan in principe geen schade toebrengen aan de militaire loopbaan van de betrokkene. In het onderhavige geval stelt het Comité I vast dat ook al heeft de betrokkene, als gevolg van zijn ontslag op het kabinet van de minister van Landsverdediging, de specifieke vergoedingen verloren die aan deze detachering zijn verbonden, hij geen enkel nadeel heeft opgelopen in het kader van zijn militaire loopbaan, aangezien hij opnieuw ter beschikking van zijn oorspronkelijke macht is gesteld waar hij dezelfde graad en dezelfde functie als chauffeur heeft behouden.

Anderzijds is de veiligheidsmaatregel die de SGR heeft genomen, zoals we hebben gezien, het gevolg van het feit dat het Krijgsauditoraat een gerechtelijk dossier tegen de klager heeft geopend, hetgeen leidt tot de vaststelling dat er in zijn hoofde sprake is van een gebrek aan betrouwbaarheid.

In verband hiermee wijst de geldende reglementering er op, met betrekking tot de individuele verantwoordelijkheid inzake militaire veiligheid en buiten de verantwoordelijkheden van gezag en de specifieke opdrachten waarmee de veiligheidsofficier is belast, dat het belangrijk is dat elk lid van de strijdkrachten, ongeacht zijn categorie, zijn rang of zijn graad, ter zake individuele verantwoordelijkheid op zich neemt. Dit impliceert dat hij kennis heeft van de reglementen, richtlijnen en normen die gelden voor hemzelf en zijn omgeving en dat hij ze in de praktijk toepast.

5.2. Betreffende het dossier van de SGR

In het kader van dit onderzoek heeft de Dienst Enquêtes van het Comité I vastgesteld dat de SGR nog geen begin heeft gemaakt met het chronologisch nummeren van de stukken in zijn dossiers, hoewel het Comité I reeds in 1996 een aanbeveling in deze zin had geformuleerd tengevolge van het toezichtsonderzoek betreffende het vernietigen van archieven.

Voorts heeft het Comité I bij het lezen van het SGR-dossier vastgesteld dat er geen spoor is van enige opvolging met betrekking tot de geldigheid in de tijd van het veiligheidscertificaat van de heer M. Zo was de betrokkene gedurende een periode gaande van 1985 tot 1998 blijkbaar niet meer in het bezit van een geldig certificaat.

Immers, het eerste veiligheidscertificaat van de heer M werd in 1980 uitgereikt en was geldig tot in 1985.

expirant en 1985. Il faudra attendre début 1998 pour trouver une nouvelle demande du cabinet du ministre de la Défense nationale visant à relever le degré du certificat de l'intéressé au niveau «secret». Après enquête, cette requête fut rencontrée par la délivrance du certificat de sécurité demandé avec une durée de validité expirant en 2003.

Selon les dispositions en la matière, un certificat de sécurité est valable cinq ans. À condition qu'un tel certificat soit toujours exigé et qu'une demande de renouvellement soit introduite dans les six mois précédant l'échéance, la validité du certificat antérieur est prorogée jusqu'à la décision concernant la demande de renouvellement.

Dans le cas d'espèce, on se trouve donc en présence d'une période de 13 années pendant laquelle le plaignant a conservé ses fonctions au cabinet de la Défense nationale avec un certificat de sécurité périmé et donc non valable aux termes des règles en vigueur.

Il faut cependant relever d'emblée que cette constatation ne peut apporter à monsieur M dans le contexte de sa plainte aucun argument utile, les faits et les mesures de sécurité concernés étant intervenus au cours de la période de validité du certificat de sécurité «secret» délivré en 1998.

On peut toutefois s'interroger sur les causes et sur les responsabilités d'une telle absence de suivi qui seraient à investiguer plus avant s'il devait résulter d'un contrôle ultérieur du Comité R que le présent cas ne constitue pas une exception.

À ce stade, rappelons qu'en la matière la demande de renouvellement devait être adressée par l'officier de sécurité du cabinet de la Défense nationale: le contrôle de l'application des règlements, directives et normes de sécurité préventive notamment auprès du cabinet du ministre de la Défense nationale, incombe au chef du SGR.

Enfin, lors de la consultation par le Service d'enquêtes du dossier du SGR concernant monsieur M, il ne lui est apparu aucune mention des motifs justifiant l'avis négatif rendu par l'officier en charge de l'affaire. Si en l'espèce devant l'évidence des éléments contenus dans le dossier, cette motivation peut paraître formelle, elle n'en constitue pas moins une exigence répondant à un principe général applicable à toute décision(1).

(1) Voir supra, page 5, 2e alinéa, ainsi que la loi relative à la motivation formelle des actes administratifs du 19 juillet 1991 (*Moniteur belge* du 12 septembre 1991).

Pas begin 1998 werd een nieuwe aanvraag bij het kabinet van de minister van Landsverdediging ingediend om het niveau van het certificaat van de betrokkene te verhogen tot het niveau «geheim». Er werd een onderzoek gevoerd, waarna gunstig gevolg werd gegeven aan dit verzoek en het gevraagde veiligheidscertificaat werd uitgereikt; dit certificaat was geldig tot in 2003.

Krachtens de bepalingen ter zake is een veiligheidscertificaat vijf jaar geldig. Op voorwaarde dat een dergelijk certificaat nog steeds vereist is en een aanvraag tot vernieuwing wordt ingediend binnen de zes maanden die aan de vervaldatum voorafgaan, wordt de geldigheid van het vorige certificaat verlengd tot een beslissing is genomen met betrekking tot de aanvraag tot vernieuwing.

In het onderhavige geval stelt het Comité I vast dat de klager gedurende een periode van 13 jaar zijn functie op het kabinet van Landsverdediging heeft behouden, hoewel de duur van zijn veiligheidscertificaat was verstreken en hij dus niet over een geldig certificaat beschikte overeenkomstig de geldende regels.

We merken echter onmiddellijk op dat deze vaststelling de heer M geen enkel nut kan opleveren in de context van zijn klacht, aangezien de bewuste feiten en veiligheidsmaatregelen zich hebben voorgedaan in een periode toen zijn veiligheidscertificaat van het niveau «geheim», dat in 1998 is uitgereikt, geldig was.

Niettemin kan men zich vragen stellen bij de oorzaken van en de verantwoordelijkheid voor een dergelijk gebrek aan opvolging. Dit zou nader onderzocht moeten worden indien uit een latere controle van het Comité I zou blijken dat het onderhavige geval geen uitzondering vormt.

In deze fase wijzen we erop dat ter zake het verzoek tot vernieuwing door de veiligheidsofficier van het kabinet van Landsverdediging moet worden aangevraagd: het toezicht op de toepassing van de reglementen, richtlijnen en normen inzake preventieve veiligheid, in het bijzonder op het kabinet van de minister van Landsverdediging, is een taak van het hoofd van de SGR.

Tot slot heeft de Dienst Enquêtes, bij het raadplegen van het dossier van de heer M bij de SGR, geen enkele vermelding gevonden van de redenen die verklaren waarom de officier die met de zaak was belast een negatief advies heeft verleend. Ook al kan deze motivering in het onderhavige geval, gelet op de duidelijkheid van de elementen in het dossier, formeel lijken, toch vormt ze een vereiste die beantwoordt aan een algemeen principe dat van toepassing is telkens wanneer een beslissing wordt genomen(1).

(1) Zie supra, pagina 5, lid 2, alsook de wet d.d. 19 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen (*Belgisch Staatsblad* van 12 september 1991).

La réglementation prévoit d'ailleurs, que seul le chef de corps de l'intéressé peut être informé oralement et personnellement à sa demande des raisons qui ont fondé une décision de sécurité.

Pourquoi pas dès lors l'intéressé? En l'occurrence, on ne voit pas quels étaient les motifs qui ne pouvaient pas être dévoilés à l'intéressé pour des raisons tenant à une quelconque confidentialité ou à un quelconque secret justifié par la sécurité de l'État, par la protection des sources ou de la vie privée. De plus, la notification au plaignant du motif de la décision lui aurait sans doute permis de mieux la comprendre et de mieux évaluer l'opportunité de faire intervenir le Comité R. Rappelons comme déjà signalé plus haut que le plaignant souhaitait en effet que le Comité R se renseigne sur les motifs du déclassement de son certificat, lui-même malgré ses efforts n'arrivant pas à en connaître les raisons.

Dorénavant, la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, qui entrera en vigueur le 1er juin 2000, répondra à ce type de situation puisqu'elle dispose dans son article 22 relatif à l'octroi et au retrait de l'habilitation de sécurité que: «La notification d'un refus d'octroi ou d'un retrait de l'habilitation de sécurité reprend les motifs justifiant cette décision, à l'exception de toute information dont la communication serait de nature à porter atteinte à la défense de l'intégrité du territoire national, aux plans de défense militaires, à l'accomplissement des missions des forces armées, à la sûreté intérieure de l'État, y compris dans le domaine de l'énergie nucléaire, à la pérennité de l'ordre démocratique et constitutionnel à la sûreté extérieure de l'État et aux relations internationales au potentiel scientifique ou économique du pays ou tout autre intérêt fondamental à l'État, à la sécurité des ressortissants belges à l'étranger, au fonctionnement des organes décisionnels de l'État, à la protection des sources ou à la protection de la vie privée de tiers.»

6. CONCLUSIONS ET RECOMMANDATIONS

Le retrait en 1999, du degré de sécurité «secret» attribué antérieurement au plaignant, résulte de l'application normale et en l'espèce justifiée des règles de sécurité en vigueur dans les forces armées, ainsi que dans tous les organismes qui dépendent du ministère de la Défense nationale.

Cette décision de retrait ne constitue pas juridiquement une sanction à l'égard du plaignant, même si elle

Overigens bepaalt de reglementering dat alleen de korpschef van de betrokkene, op zijn verzoek, mondeling en persoonlijk op de hoogte mag worden gebracht van de redenen op grond waarvan een beslissing inzake veiligheid is genomen.

Waarom dan niet de betrokkene zelf? In het onderhavige geval zien we niet welke beweegredenen niet aan de betrokkene mochten worden onthuld om redenen van vertrouwelijkheid of geheimhouding gerechtvaardigd door de veiligheid van de Staat, de bescherming van de bronnen of van de persoonlijke levenssfeer. Bovendien zou de kennisgeving aan de klager van de reden van de beslissing hem wellicht hebben toegelaten deze beslissing beter te begrijpen en beter in te schatten of het opportuun was een beroep te doen op het Comité I. We herhalen dat de klager inderdaad wenst dat het Comité I inlichtingen inwint over de redenen van de declassering van zijn certificaat, aangezien hijzelf geen kennis krijgt van deze redenen, in weerwil van zijn inspanningen daartoe.

De wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, die op 1 juni 2000 in werking treedt, komt tegemoet aan dit soort situaties, aangezien artikel 22 betreffende de toekenning en de intrekking van de veiligheidsmachtiging bepaalt: «De kennisgeving van de weigering van het verlenen van een veiligheidsmachtiging of van de intrekking van een veiligheidsmachtiging vermeldt de beweegredenen die deze beslissing rechtvaardigen, behoudens elke inlichting waarvan de mededeling schade zou kunnen toebrengen aan de verdediging van de onschendbaarheid van het nationaal grondgebied, aan de militaire defensieplannen, aan de vervulling van de opdrachten van de strijdkrachten, aan de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, aan het voortbestaan van de democratische en grondwettelijke orde, aan de uitwendige veiligheid van de Staat en de internationale betrekkingen, aan het wetenschappelijk of economisch potentieel van het land of aan elk ander fundamenteel belang van de Staat, aan de veiligheid van de Belgische onderdanen in het buitenland, aan de werking van de besluitvormingsorganen van de Staat, aan de bescherming van de bronnen of aan de bescherming van het privé-leven van derden.»

6. BESLUITEN EN AANBEVELINGEN

De intrekking, in 1999, van het veiligheidsniveau «geheim» dat voordien aan de klager was toegekend, is het gevolg van de normale en in het onderhavige geval gerechtvaardigde toepassing van de veiligheidsregels die gelden bij de strijdkrachten en bij alle organen die onder de bevoegdheid van het ministerie van Landsverdediging vallen.

Deze beslissing tot intrekking is juridisch gezien geen sanctie tegen de klager, ook al kon de betrok-

a pu être ressentie comme telle par l'intéressé dans ses conséquences directes à savoir, la fin de son détachement en qualité de chauffeur au cabinet du ministre de la Défense nationale et la perte consécutive des indemnités liées à cette situation. L'intéressé n'a toutefois subi aucun préjudice au niveau de sa carrière militaire puisque remis à disposition de sa force d'origine, il y a conservé le même grade et la même fonction de chauffeur militaire. Il a d'autre part été constaté qu'à tout moment l'application par le SGR des règles de sécurité par rapport à la situation et au comportement personnels de l'intéressé a été faite dans un sens plutôt favorable à ce dernier.

L'absence de motivation formelle et de notification au plaignant du motif de la décision de retrait soulève toutefois une objection de principe de la part du Comité R, compte tenu du fait qu'il ne perçoit pas en la cause les motifs qui ne pouvaient pas être dévoilés à l'intéressé pour des raisons tenant à «la sûreté extérieure de l'État, à l'ordre public, au respect de la vie privée, aux dispositions en matière de secret professionnel» (1).

Le Comité R recommande à ce propos que le Règlement IF 5 soit mis en conformité avec les dispositions de l'article 22, ci-dessus énoncé, de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité qui entrera en vigueur le 1er juin 2000.

Le Comité R recommande aussi, dans le même contexte, que dans les dossiers d'enquête du SGR une motivation explicite soit reprise à l'appui de l'avis rendu en matière d'habilitation de sécurité.

Le Comité R réitère enfin au SGR ses recommandations faites en 1996 et en 1999 de coter les pièces qui constituent un dossier et d'en faire l'inventaire dans chaque dossier. Il souligne la particulière importance de mettre en application et de respecter dans l'avenir une telle procédure eu égard aux dispositions des lois du 11 décembre 1998 «relative à la classification et aux habilitations de sécurité» et «portant création d'un organe de recours en matière d'habilitations de sécurité» ainsi qu' à celles de «l'arrêté royal du 24 mars 2000 déterminant la procédure à suivre devant l'organe de recours en matière d'habilitations de sécurité».

(1) Voir article 4 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs (*Moniteur belge* du 12 septembre 1991).

kene de beslissing als zodanig ervaren wat de onmiddellijke gevolgen ervan betreft. De beslissing betekende immers het einde van zijn detachering als chauffeur op het kabinet van de minister van Landsverdediging en had tot gevolg dat hij geen recht meer had op de vergoedingen die aan deze functie verbonden waren. De betrokkene heeft echter geen schade opgelopen met betrekking tot zijn militaire loopbaan, aangezien hij opnieuw ter beschikking van zijn oorspronkelijke macht is gesteld en er dezelfde graad en dezelfde functie van militair chauffeur heeft behouden. Anderzijds heeft het Comité I vastgesteld dat de manier waarop de SGR de veiligheidsregels met betrekking tot de persoonlijke situatie en het gedrag van de betrokkene heeft toegepast eerder in zijn voordeel is geweest.

Het Comité I heeft echter principieel bezwaar tegen het ontbreken van elke uitdrukkelijke motivering en van de betekening aan de klager van de reden van de beslissing tot intrekking, aangezien het Comité in deze zaak geen redenen vindt waarvan de betrokkene geen kennis mocht hebben omdat ze te maken zouden hebben met de «uitwendige veiligheid van de Staat, de openbare orde, de eerbied voor het privé-leven, de bepalingen inzake beroepsgeheim» (1).

In verband hiermee beveelt het Comité I aan dat Reglement IF 5 conform zou worden gemaakt met de bepalingen van artikel 22 van de wet d.d. 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, die op 1 juni 2000 in werking treedt.

In dezelfde context raadt het Comité I aan dat de SGR in zijn onderzoeksdossiers een uitdrukkelijke motivering zou opnemen ter staving van het advies dat inzake veiligheidsmachtigingen wordt verleend.

Tot slot herhaalt het Comité I aan de SGR zijn aanbevelingen uit 1996 en 1999 om de stukken te nummeren die samen een dossier vormen en in elk dossier een inventaris van deze stukken op te nemen. Het Comité I benadrukt dat het van het grootste belang is een dergelijke procedure voortaan toe te passen en na te leven, gelet op de bepalingen van de wetten d.d. 11 december 1998 «betreffende de classificatie en de veiligheidsmachtigingen» en «tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen», alsook op de bepalingen van «het koninklijk besluit van 24 maart 2000 tot regeling van de rechtspleging voor het beroepsorgaan inzake veiligheidsmachtigingen».

(1) Zie artikel 4 van de wet d.d. 29 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen (*Belgisch Staatsblad* van 12 september 1991).

CHAPITRE 3

Rapport relatif à l'enquête de contrôle suite à la plainte d'un ancien informateur

1. PROCÉDURE

Au mois d'août 1999, le Comité R réceptionne un courrier du collège des médiateurs fédéraux, l'informant de la « clôture à défaut d'objet » d'une procédure de médiation intervenue entre la Sûreté de l'État et un sieur « H ».

Il ressort de ce courrier que l'avis ainsi fait au Comité R résulte d'un vœu exprimé par le demandeur, « H », arguant à la fois du harcèlement dont il ne cesserait de faire l'objet de la part de personnes qu'il identifie comme agents de la Sûreté de l'État et de la compétence du Comité R en sa qualité de contrôleur externe des services de renseignement, chargé par la loi de veiller à la protection que la Constitution et la loi confèrent aux personnes ainsi que d'enquêter sur la coordination, l'efficacité, les activités et les méthodes des services de renseignement.

Le Comité R invite aussitôt le chef du Service d'enquêtes à entendre le sieur « H » en confirmation de plainte et cette demande est exécutée le jour-même.

Lors d'une réunion plénière immédiatement ultérieure, le Comité R décide à l'unanimité d'ouvrir une enquête de contrôle intitulée « enquête suite à la plainte d'un ancien informateur ». Deux membres sont spécifiquement chargés du suivi de cette enquête.

Notification en est adressée au président du Sénat, M. De Decker, conformément à l'article 32 de la loi organique du 18 juillet 1991.

Une apostille est adressée au chef du Service d'enquêtes, l'invitant à procéder à l'audition des personnes qui, à la Sûreté de l'État, auraient été en contact avec le plaignant, ainsi qu'à prendre connaissance du contenu de l'éventuel dossier d'informateur de celuici et de tout autre document dans lequel son nom serait relevé.

Le chef du Service d'enquêtes adresse à son tour notification de l'ouverture de l'enquête à M. Verwilghen, ministre de la Justice.

Le Comité R a ultérieurement reçu une lettre signée d'une mandataire politique signalant que le plaignant s'était adressé à ses services. En annexe étaient jointes les copies de divers documents, dont deux lettres de plainte à destination respective des ministres de la

HOOFDSTUK 3

Verslag over het toezichtsonderzoek betreffende een klacht van een gewezen informant

1. PROCEDURE

In de maand augustus 1999 ontving het Comité I een brief van het College van federale ombudsmannen, waarin werd meegedeeld dat een bemiddelingsprocedure tussen de Veiligheid van de Staat en de heer « H » werd afgesloten « bij gebrek aan voorwerp ».

Uit de brief blijkt dat de kennisgeving aan het Comité I het gevolg is van een vraag van de verzoeker, « H », die beweert dat hij voortdurend wordt achtervolgd door personen die volgens hem agenten van de Veiligheid van de Staat zijn, en die zich tevens beroept op de bevoegdheid van het Comité I als extern toezichtsorgaan van de inlichtingendiensten, belast door de wet teneinde de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, te waarborgen, alsook de coördinatie, de doelmatigheid, de activiteiten en de methodes van de inlichtingendiensten te onderzoeken.

Het Comité I heeft onmiddellijk het hoofd van de Dienst Enquêtes gevraagd om over te gaan tot het verhoor van de heer « H », en hem te vragen zijn klacht te bevestigen. Dit verhoor vond dezelfde dag nog plaats.

Op zijn plenaire vergadering van 31 augustus 1999 besliste het Comité I eenparig een controleonderzoek te openen, getiteld « Onderzoek ingevolge de klacht van een gewezen informant ». Twee leden werden in het bijzonder belast met de opvolging van dit onderzoek.

De voorzitter van de Senaat, de heer De Decker werd op de hoogte gebracht van het onderzoek, overeenkomstig artikel 32 van de wet van 18 juli 1991 houdende regeling van het toezicht op de politie- en inlichtingendiensten.

Een kantschrift werd aan het hoofd van de Dienst Enquêtes gericht, met het verzoek over te gaan tot het verhoor van de personen die bij de Veiligheid van de Staat contact zouden gehad hebben met de klager, alsmede kennis te nemen van de inhoud van het eventueel dossier van hem als informant, en van eender welk ander document waarin zijn naam zou voorkomen.

Het hoofd van de Dienst Enquêtes heeft de heer Verwilghen, minister van Justitie, op de hoogte gebracht van de opening van het onderzoek.

Het Comité I heeft daarna een brief ontvangen van een politiek mandataris waarin deze meldde dat de klager contact had opgenomen met haar diensten. Bij haar brief had ze kopieën van diverse documenten gevoegd, waaronder twee klachtenbrieven, respectie-

Justice et de l'Intérieur, attestant de la constance des griefs formulés par M. « H ».

Le Comité R a également réceptionné une lettre de la direction générale de la Police générale du Royaume, à laquelle était annexée copie de la plainte adressée par M. « H » au ministre de l'Intérieur.

Le Service d'enquêtes a déposé son rapport final en date du 29 octobre 1999.

Le présent rapport a été approuvé par le Comité R en date du 10 avril 2000.

2. CONSULTATION DU DOSSIER DÉTENU PAR LA SÛRETÉ DE L'ÉTAT

Le Service d'enquêtes du Comité R s'est rendu dans les locaux de la Sûreté de l'État, afin d'y prendre connaissance du dossier ouvert au nom du plaignant.

Il y est effectivement répertorié comme informateur.

La dernière pièce indique la radiation de l'informateur en 1999, consécutive à l'intervention du médiateur fédéral.

3. AUDITION

Le chef du Service d'enquêtes a entendu l'agent chargé de suivre le plaignant. Selon ce dernier, la rupture interviendra au printemps 1998, l'informateur ne fournissant plus de renseignements et manifestant — selon lui — un comportement psychologiquement perturbé. L'éventualité d'une reprise ultérieure des relations avait été néanmoins ménagée. Il déclare encore avoir reçu un appel téléphonique de la part de l'informateur lui-même, par lequel ce dernier lui dénonçait le harcèlement dont il faisait l'objet et son intention d'introduire un recours.

Selon ses dires, l'agent de la Sûreté de l'État a fidèlement rendu compte de sa mission à sa hiérarchie. Il dépeint le plaignant sous les traits d'un être soupçonneux, en permanence persuadé d'être suivi. Il a essayé de le convaincre de ce que la Sûreté de l'État n'avait pas les moyens, l'eût-elle voulu, de se livrer à des filatures de ce type.

4. SYNTHÈSE DE L'ENQUÊTE

Le Service d'enquêtes du Comité R s'est rendu à la Sûreté de l'État pour consulter le dossier du plaignant

velijk gericht aan de minister van Justitie en de minister van Binnenlandse Zaken, ter bevestiging van het voortduren van de grieven geformuleerd door de heer « H ».

Het Comité I heeft eveneens een brief ontvangen van de algemene directie van de Algemene Rijkspolitie, waarbij een kopie was gevoegd van de klacht die de heer « H » aan de minister van Binnenlandse Zaken had gericht.

Op 29 oktober 1999 heeft de Dienst Enquêtes zijn eindverslag neergelegd.

Het Comité I heeft dit verslag op 24 maart 2000 goedgekeurd.

2. INZAGE VAN HET DOSSIER IN HET BEZIT VAN DE VEILIGHEID VAN DE STAAT

De Dienst Enquêtes van het Comité I heeft zich naar de Veiligheid van de Staat begeven om er kennis te nemen van het dossier dat was geopend op naam van de klager.

Hij staat er inderdaad geregistreerd als informant.

Uit het laatste stuk blijkt dat de informant in 1999 is geschrapt, volgend op de tussenkomst van de federale ombudsman.

3. DE VERHOREN

Het hoofd van de Dienst Enquêtes is overgegaan tot het verhoor van de agent die de opdracht had gekregen de klager te volgen. Volgens deze agent kwam het tot een breuk in de lente van 1998, toen de informant geen inlichtingen meer bezorgde en — volgens hem — blijk gaf van psychisch gestoord gedrag. Niettemin had hij rekening gehouden met een mogelijke hervatting van de relatie. Hij verklaarde ook nog dat hij was opgebeld door de informant zelf om te zeggen dat hij aangifte zou doen van het « geterg » waarvan hij het slachtoffer was, en zich voornam stappen tegen hem te ondernemen.

De agent van de Veiligheid van de Staat verklaarde dat hij bij zijn hiërarchie trouw verslag heeft uitgebracht van zijn opdracht. Hij beschreef de klager als een achterdochtig persoon, die ervan overtuigd was dat hij voortdurend werd gevolgd. Hij had gepoogd hem duidelijk te maken dat de Veiligheid van de Staat niet over de middelen beschikte om dit soort schaduwopdrachten uit te voeren, indien ze dat al zou hebben gewild.

4. SAMENVATTING VAN HET ONDERZOEK

De Dienst Enquêtes van het Comité I heeft zich naar de kantoren van de Veiligheid van de Staat bege-

et a procédé à l'audition de la personne qui en était responsable.

Il n'a découvert dans ce dossier, sur lequel l'attention de la Sûreté de l'État est attirée depuis la mise en œuvre de la procédure de médiation, aucune mention relative à des filatures, mises en garde ou différends intervenus entre le responsable de la Sûreté de l'État et le plaignant, pas plus qu'il n'y était question d'intimidation ou de menaces de mort, intervenues en Belgique comme à l'étranger, à l'initiative de quelque personne que ce soit.

En définitive, le seul élément objectif de convergence susceptible d'être retenu entre les déclarations constantes contenues dans les plaintes successivement formulées par M. « H » auprès de diverses autorités ou personnes privées ou publiques, le contenu du dossier de la Sûreté de l'État et l'audition du responsable concerné, consiste en la constatation, à partir de 1998, d'une réticence manifeste dans le chef du plaignant à collaborer désormais, conjuguée à la crainte permanente de faire l'objet de menaces et de filature.

5. CONCLUSIONS

Le dossier consulté à la Sûreté de l'État par le Service d'enquêtes du Comité R ne contenait aucune indication allant dans le sens des affirmations du plaignant.

Avisée de la plainte déposée entre les mains du président du Collège des médiateurs fédéraux dès avant la saisine du Comité R, la Sûreté de l'État avait déjà radié l'informateur.

Ultérieurement entendu dans le cadre de la présente enquête de contrôle l'agent responsable a déclaré que l'état psychique du plaignant s'était, à son estime, dégradé dès avril 1998, tandis que ce dernier refusait toute nouvelle collaboration avec la Sûreté de l'État.

L'enquête menée par le Comité R n'a donc pas permis de démontrer la véracité des allégations — graves — du plaignant. Elle n'a pas non plus permis de déceler le moindre indice permettant d'établir que la Sûreté de l'État aurait violé les droits que la Constitution et les lois belges confèrent aux citoyens.

Les dispositions légales fondant la compétence du Comité R ne l'autorisent pas à procéder à des investigations complémentaires qui eussent éventuellement pu permettre de tirer des conclusions plus complètes. Le chef du Service d'enquêtes a donc relaté les circonstances de la plainte de M. « H » à M. le procureur du

ven om inzage te nemen van het dossier van de klager. Vervolgens heeft de Dienst Enquêtes de verantwoordelijke personen verhoord.

De Dienst Enquêtes heeft in het dossier, waarop de aandacht van de Veiligheid van de Staat werd gevestigd sinds de inwerkingtreding van de bemiddelingsprocedure, geen enkele vermelding gevonden betreffende schaduwoperaties, waarschuwingen of geschillen tussen de verantwoordelijke personen bij de Veiligheid van de Staat enerzijds en de klager anderzijds. Evenmin was er sprake van intimidatie of doodsbedreigingen, in België en in het buitenland, vanwege wie dan ook.

Uiteindelijk is het enige objectieve element van overeenstemming dat in aanmerking kan worden genomen tussen de constante verklaringen in de opeenvolgende klachten van de heer « H » bij diverse overheden of bij particuliere of publieke personen, de inhoud van het dossier van de Veiligheid van de Staat en de verhoren van de betrokken verantwoordelijken, de vaststelling dat de betrokkene vanaf 1998 duidelijk blijk gaf van zijn terughoudendheid om nog langer samen te werken, gepaard gaand met zijn niet aflatende vrees te worden bedreigd of geschaduwd.

5. BESLUITEN

Het dossier dat de Dienst Enquêtes van het Comité I bij de Veiligheid van de Staat heeft ingezien, bevatte geen enkele aanwijzing die de verklaringen van de klager zou kunnen bevestigen.

Nadat de Veiligheid van de Staat kennis had gekregen van de klacht die bij de voorzitter van het College van federale ombudsmannen was ingediend voorafgaand aan de aanhangigmaking bij het Comité I, heeft ze de informant geschrapt.

Toen hij later werd verhoord in het kader van het onderhavige toezichtsonderzoek, verklaarde de verantwoordelijke agent dat, volgens hem, de psychische staat van de klager vanaf april 1998 was verslechterd. De betrokkene weigerde nog langer samen te werken met de Veiligheid van de Staat.

Het onderzoek van het Comité I heeft het bijgevolg niet mogelijk gemaakt aan te tonen of de — ernstige — aantijgingen van de klager enige waarheid bevatten. Het heeft evenmin enige aanwijzingen aan het licht gebracht op grond waarvan men zou kunnen bewijzen dat de Veiligheid van de Staat de rechten zou hebben geschonden die de Belgische Grondwet en wetten aan de burgers verlenen.

De wettelijke bepalingen, die de grondslag zijn van de bevoegdheid van het Comité I, laten dit Comité niet toe bijkomend onderzoek te verrichten, dat eventueel had toegelaten vollediger gevolgtrekkingen te maken. Het hoofd van de Dienst Enquêtes heeft bijgevolg bij de procureur des Konings van Brussel verslag

Roi de Bruxelles qui, confronté à des indices éventuels d'infraction résultant notamment des dires répétitifs du plaignant, dispose de la possibilité d'aller plus avant, suivant un mode judiciaire. Si tel devait être le cas, dans l'hypothèse où des dysfonctionnements devaient ultérieurement apparaître, le Comité R ne manquerait pas de lancer d'initiative une enquête de contrôle consécutive.

TITRE II

COMMENTAIRES DU COMITÉ PERMANENT R SUR LA RECOMMANDATION 1402 DU CONSEIL DE L'EUROPE

« CONTRÔLE DES SERVICES DE SÉCURITÉ INTÉRIEURE DANS LES ÉTATS MEMBRES DU CONSEIL DE L'EUROPE »

INTRODUCTION

Par sa lettre du 26 août 1999, le conseiller général du ministère de la Justice, Daniel Flore, (Direction générale de la législation pénale et des droits de l'homme) agissant au nom du ministre, a adressé au Comité R le texte de la recommandation 1402 (1999) adoptée le 26 avril 1999 par le Conseil de l'Europe dans une version provisoire. Cette recommandation concerne le contrôle des services de sécurité intérieure dans les États membres du Conseil de l'Europe.

Il s'agit d'une recommandation que le comité des ministres du Conseil de l'Europe a pris la décision d'examiner le 9 juin 1999 afin d'y apporter une réponse, pour la fin de l'année, à la lumière de trois rapports : le premier de ceux-ci s'attachant aux droits de l'homme, le second aux problèmes de déontologie de la police et le troisième à la protection des données à caractère personnel.

Au niveau national, un conseiller-adjoint du ministère de la Justice a été désigné pour préparer le rapport portant sur les aspects de protection des données à caractère personnel, ce document devant être achevé pour la mi-octobre 1999.

Dans la lettre qu'il adresse au Comité R, le conseiller général indique : « Tout commentaire qu'il plairait au Comité R de formuler à l'égard de la recommandation précitée serait du plus haut intérêt en vue de l'élaboration du rapport de mon collaborateur. Aussi, je vous saurai gré de bien vouloir les lui faire parvenir pour le 1er octobre au plus tard » (1).

(1) Traduction libre.

uitgebracht over de omstandigheden van de klacht van de heer « H ». Gelet op de eventuele aanwijzingen van inbreuk die met name voortvloeien uit de herhaaldelijke verklaringen van de klager, kan de procureur het onderzoek op gerechtelijk vlak voortzetten. Indien hij deze beslissing zou nemen, in de veronderstelling dat later disfuncties aan het licht zouden komen, zal het Comité I niet nalaten om ambtshalve een navolgend toezichtsonderzoek te openen.

TITEL II

COMMENTAAR VAN HET VAST COMITE I BIJ DE AANBEVELING 1402 VAN DE RAAD VAN EUROPA

TOEZICHT OP DE INTERNE VEILIGHEIDSDIENSTEN IN DE LIDSTATEN VAN DE RAAD VAN EUROPA

INLEIDING

Met zijn brief van 26 augustus 1999, zond de adviseur-generaal van het ministerie van Justitie (Directoraat-generaal strafwetgeving en rechten van de mens), de heer Daniël Flore, namens de minister aan het Comité I de tekst toe van de « aanbeveling 1402 » (1999), die op 26 april 1999 door de Raad van Europa werd goedgekeurd (in een voorlopige versie).

Deze aanbeveling betreft het toezicht op de binnenlandse veiligheidsdiensten van de lidstaten van de Raad van Europa. Ter zake besliste het ministerieel comité van de Raad van Europa op 9 juni 1999 de aanbeveling te onderzoeken en een antwoord hierop te verschaffen voor het einde van het jaar in het licht van drie rapporten : het eerste handelend over de mensenrechten, het tweede over de politiedeontologie en het derde aangaande de bescherming van persoonlijke gegevens.

Een aspirant-adviseur van het ministerie van Justitie werd op het nationaal niveau aangewezen om het rapport over de bescherming van de persoonlijke gegevens voor te bereiden. Dit document moest voor medio oktober 1999 afgewerkt zijn.

In zijn brief gericht aan het Comité I geeft de adviseur-generaal aan dat : « Elke commentaar die het Comité I wenst in te brengen met betrekking tot voornoemde aanbeveling zou van het grootste belang zijn met het oog op het opstellen van het rapport van mijn medewerker. Ik zou het op prijs stellen deze hem toe te zenden ten laatste op 1 oktober » (1).

(1) Vrije vertaling.

L'article 33, alinéa 7, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, modifiée par la loi du 1er avril 1999, indique :

« Le Comité permanent R ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toute nature exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants, du Sénat, ou du ministre compétent. »

S'agissant en l'occurrence d'une demande d'avis introduite au nom du ministre de la Justice, le Comité R a décidé d'y répondre favorablement.

Le présent commentaire du Comité R a été adressée à la Direction générale de la législation pénale et des droits de l'homme le 30 septembre 1999.

ANALYSE DE LA RECOMMANDATION 1402

NB : le lecteur trouvera ci-après le texte, en italique et suivi des commentaires du comité R, de chacune des recommandations du Conseil de l'Europe.

1. *« L'assemblée reconnaît que les services de sécurité intérieure rendent un service précieux aux sociétés démocratiques en protégeant la sécurité nationale et l'ordre démocratique libre de l'État »* (1).

Commentaire :

Le Comité R adhère pleinement à cette reconnaissance du rôle des services de sécurité pourvu qu'ils fonctionnent dans un cadre légal et démocratique tel que celui défini par la loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité ou par d'autres lois similaires comme il en existe dans d'autres pays de l'Europe occidentale (Grande-Bretagne, Pays-Bas, Portugal, etc.).

Le Comité R pense qu'une définition préalable de la notion de *« services de sécurité intérieure »* aiderait à clarifier la portée et l'enjeu de la recommandation.

Il conviendrait par ailleurs de faire une distinction claire entre les services de renseignement et de sécurité et les services de police.

2. *« Toutefois, l'assemblée s'inquiète que les services de sécurité intérieure de pays membres placent souvent des intérêts qui leur paraissent être ceux de la sécurité nationale et de leurs pays au-dessus du respect des droits de l'individu. »* (1)

(1) Traduction libre.

Artikel 33, lid 7, van de wet van 18 juli 1991 houdende regeling van het toezicht op de politie- en inlichtingendiensten, zoals gewijzigd door de wet van 1 april 1999, bepaalt dat :

« Het Vast Comité I mag enkel op verzoek van de Kamer van volksvertegenwoordigers, van de Senaat of van de bevoegde minister advies uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd. »

Gezien het hier handelt over een verzoek om advies, aangevraagd namens de minister van Justitie, besloot het Comité I hierop in te gaan.

Dit commentaar werd door het Comité I aan het Directoraat-generaal strafwetgeving en rechten van de mens toegezonden op 30 september 1999.

ANALYSE VAN DE AANBEVELING 1402

NB : de lezer vindt hierna de tekst van elke aanbeveling van de Raad van Europa, cursief gedrukt, gevolgd door de commentaar van het Comité I.

1. *« De vergadering erkent dat de interne veiligheidsdiensten een waardevolle dienst verlenen aan democratische samenlevingen door de nationale veiligheid en de vrije democratische orde van de Staat te beschermen. »* (1)

Commentaar :

Het Comité I gaat volledig akkoord met deze erkenning van de rol van de veiligheidsdiensten, op voorwaarde dat ze functioneren binnen een wettelijk en democratisch kader zoals dat bepaald wordt door de Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst of door andere vergelijkbare wetten zoals ze bestaan in andere West-Europese landen (Groot-Brittannië, Nederland, Portugal, enz.).

Het Comité I is van mening dat een voorafgaande definitie van het begrip *« binnenlandse veiligheidsdiensten »* kan helpen de reikwijdte en het belang van de aanbeveling toe te lichten.

Overigens zou het passen een duidelijk onderscheid te maken tussen de inlichtingen- en veiligheidsdiensten, enerzijds, en de politiediensten, anderzijds.

2. *« De vergadering maakt zich echter zorgen over het feit dat de binnenlandse veiligheidsdiensten van de lidstaten vaak meer waarde hechten aan de belangen die volgens hen belangen van nationale veiligheid en van hun land zijn, dan aan de eerbied voor de rechten van het individu. »* (1)

(1) Vrije vertaling.

Commentaire :

Une telle affirmation aussi catégorique doit être relativisée; elle ne paraît pas de mise *a priori* en ce qui concerne notamment les services de renseignement qui font l'objet d'un contrôle strict des autorités et dont les missions, ainsi que les méthodes, sont réglementées par une loi organique. Tels est notamment le cas des services de renseignement belges soumis au contrôle du Comité R depuis la loi du 18 juillet 1991 et à la loi organique du 30 novembre 1998.

« Ces services étant par ailleurs souvent insuffisamment contrôlés, le risque d'abus de pouvoir et de violations des droits de l'homme est élevé, à moins que des sauvegardes législatives et constitutionnelles ne soient prévues. »

Commentaire :

Idem, une telle formulation, tout aussi catégorique, méconnaît l'encadrement légal des services de renseignement ainsi que les mécanismes de contrôle dont ils font l'objet dans certains pays démocratiques tels que la Belgique.

3. *« L'assemblée estime qu'une telle situation est potentiellement dangereuse. Si les services de sécurité intérieure doivent être habilités à atteindre leurs objectifs légitimes, à savoir protéger la sécurité nationale et l'ordre démocratique libre de l'État contre toute menace visible et réelle, ils ne doivent pas pour autant avoir carte blanche pour violer les libertés et les droits fondamentaux. »* (1)

Commentaire :

Le Comité R ne peut concevoir que la mission des services de sécurité soit limitée aux menaces visibles et réelles qui, elles, sont plutôt du ressort des services de police, des autorités judiciaires et administratives. Le Comité R pense quant à lui que débusquer les menaces occultes est une tâche essentielle des services de renseignement. La loi organique belge des services de renseignement et de sécurité leur a par ailleurs confié la mission *« de rechercher, d'analyser et de traiter le reseignement relatif à toute activité qui menace ou pourrait menacer »* la Sûreté de l'État, celle des Forces

(1) Traduction libre.

Commentaar :

Deze categorische verklaring moet worden gerelativeerd; *a priori* lijkt ze niet op haar plaats met betrekking tot de inlichtingendiensten die onder streng toezicht van de overheid staan en waarvan de opdrachten en de methodes in een (organieke) wet worden gereglementeerd. Met name de Belgische inlichtingendiensten verkeren in dit geval en staan, krachtens de wet d.d. 18 juli 1991 en de wet d.d. 30 november 1998, onder het toezicht van het Comité I.

« Aangezien er daarenboven vaak onvoldoende toezicht op deze diensten wordt uitgeoefend, is het risico op machtsmisbruik en schendingen van de mensenrechten groot, tenzij de wet en de grondwet waarborgen verlenen. »

Commentaar :

Hier geldt dezelfde opmerking. Een dergelijke categorische formulering houdt geen rekening met het wettelijk kader van de inlichtingendiensten noch met de controlemechanismen waarvan deze diensten in sommige democratische landen zoals België het voorwerp zijn.

3. *« De vergadering is van mening dat een dergelijke situatie potentieel gevaarlijk is. Ook al moet men binnenlandse veiligheidsdiensten de bevoegdheid verlenen om hun wettige doelstellingen te verwezenlijken, namelijk het beschermen van de nationale veiligheid en de vrije democratische orde van de Staat tegen elke zichtbare en reële bedreiging, betekent dit niet dat men hun « carte blanche » moet geven om de fundamentele vrijheden en rechten te schenden. »* (1)

Commentaar :

Het Comité I kan zich niet voorstellen dat de opdracht van de veiligheidsdiensten zou worden beperkt tot zichtbare en reële bedreigingen, die veeleer tot de bevoegdheid behoren van de politiediensten, de gerechtelijke en de administratieve autoriteiten. Het Comité I daarentegen meent dat het opsporen van onzichtbare bedreigingen tot de essentiële opdrachten van de inlichtingendiensten behoort. Overigens heeft de Belgische wet houdende regeling van de inlichtingen- en veiligheidsdienst deze diensten belast met de opdracht : *« het inwinnen, analyseren en verwerken*

(1) Vrije vertaling.

armées, etc., en y incluant ainsi la notion de menace potentielle.

4. *« Il convient de trouver le juste équilibre entre le droit d'une société démocratique à la sécurité nationale et les droits de l'individu. (...). »* (1)

Commentaire :

Le Comité R ne peut qu'adhérer à l'ensemble de cette recommandation. Il pense que trois principes doivent être pris en considération à cet effet : la légalité, la proportionnalité et la subsidiarité.

5. *« Il existe un risque accru d'abus de pouvoir de la part des services de sécurité intérieure, et donc de violations graves des droits de l'homme, lorsque ces services possèdent une organisation spécifique, exercent certains pouvoirs comprenant des méthodes préventives et répressives qui impliquent la coercition (par exemple, celui d'effectuer des perquisitions et des fouilles, des enquêtes judiciaires, des arrestations et incarcérations), sont insuffisamment contrôlés (par les pouvoirs exécutif, législatif et judiciaire) et comprennent un trop grand nombre d'agences. »* (1)

Commentaire :

Le Comité R adhère pleinement à cette évaluation du risque accru d'abus de pouvoir. Toutefois il estime que l'organisation spécifique des services de sécurité ne constitue pas en soi un tel risque si elle s'inscrit dans un cadre constitutionnel et légal d'une part, si elle est soumise à un contrôle externe d'autre part.

6. *« L'assemblée propose par conséquent que les services de sécurité intérieure ne soient pas autorisés à mener des enquêtes judiciaires, à arrêter ou incarcérer des individus, ... »* (1)

Commentaire :

Le Comité R adhère globalement à cette recommandation. Il convient de distinguer clairement les services de police et les services de sécurité dont les

(1) Traduction libre.

van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het ministerieel comité, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het ministerieel comité, bedreigt of zou kunnen bedreigen »; deze formulering bevat dus het begrip potentiële bedreiging.

4. *« Het past het juiste evenwicht te vinden tussen het recht van een democratische samenleving op nationale veiligheid enerzijds en de rechten van het individu anderzijds. (...) »* (1).

Commentaar :

Het Comité I kan niet anders dan deze aanbeveling volledig onderschrijven en is van mening dat daartoe rekening moet worden gehouden met drie beginselen : wettelijkheid, proportionaliteit en subsidiariteit.

5. *« Het risico op machtsmisbruik vanwege de binnenlandse veiligheidsdiensten, en bijgevolg op ernstige schendingen van de mensenrechten, neemt toe wanneer deze diensten een specifieke structuur bezitten, bepaalde bevoegdheden uitoefenen, met inbegrip van preventieve en repressieve methodes die met dwang gepaard gaan (bijvoorbeeld : de bevoegdheid huiszoekingen te verrichten en te fouilleren, gerechtelijke onderzoeken te voeren, personen aan te houden en op te sluiten), onvoldoende worden gecontroleerd (door de uitvoerende, de wetgevende en de rechterlijke macht) en een te groot aantal afdelingen omvatten. »* (1)

Commentaar :

Het Comité I is het volledig eens met deze beoordeling van een verhoogd risico tot machtsmisbruik. Het is echter van mening dat de specifieke organisatie van de veiligheidsdiensten op zichzelf geen dergelijk risico inhoudt indien ze enerzijds past in een grondwettelijk en wettelijk kader en anderzijds aan een extern toezicht is onderworpen.

6. *« Bijgevolg stelt de vergadering voor de binnenlandse veiligheidsdiensten niet de bevoegdheid te verlenen om gerechtelijke onderzoeken te voeren, personen aan te houden of op te sluiten, (...) »* (1)

Commentaar :

In het algemeen gaat het Comité I akkoord met deze aanbeveling. Er moet een duidelijk onderscheid worden gemaakt tussen de politiediensten en de vei-

(1) Vrije vertaling.

agents ne doivent pas être revêtus de la qualité d'officier de police judiciaire. Une telle confusion des rôles comporte effectivement un risque d'abus contre les libertés.

Le Comité R fait toutefois remarquer que lorsqu'un service de sécurité est chargé d'une mission opérationnelle anti-terroriste, ou lorsqu'il est investi d'une mission de protection de personnes ou d'installations, il est nécessaire que ses agents puissent retenir les auteurs de faits graves et flagrants pour les livrer dans les plus brefs délais aux forces de police. Ce principe est d'ailleurs admis par la loi belge du 20 juillet 1990 relative à la détention préventive puisque, même un particulier, peut retenir une personne prise en flagrant crime ou flagrant délit pour dénoncer immédiatement les faits à un agent de la force publique.

En Belgique, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité accorde certains pouvoirs coercitifs de police administrative aux agents de la Sûreté de l'État qui, en dehors de toute mission judiciaire, mais en qualité d'officiers de protection, sont chargé de la protection des personnes.

«..., ni associés à la lutte contre la criminalité organisée, sauf dans des cas très particuliers, lorsque le crime organisé constitue une menace réelle pour l'ordre démocratique libre de l'État.» (1)

Commentaire :

Le Comité R ne peut adhérer à cette recommandation qui serait de nature à affaiblir la lutte contre le crime organisé tant sur le plan national qu'international. Le Comité R pense en effet que les organisations criminelles représentent bien un danger pour l'ordre démocratique et l'intégrité de l'État et qu'il convient par conséquent d'encourager la collaboration des services de sécurité avec les services de police en vue de prévenir et de combattre cette forme de criminalité.

Ainsi que le dit l'éminent juriste britannique David Bickford, «*fighting crime, successfully, relies on information. First of all, gathering information which can be turned into evidence to support proceedings against suspects, both private and corporate. This information comes from public sources and secret*

(1) Traduction libre.

ligheidsdiensten, waarvan de agenten niet de hoedanigheid van officier van gerechtelijke politie moeten bezitten. Een dergelijke verwarring van de opdrachten brengt inderdaad een risico van misbruik tegen de fundamentele vrijheden met zich mee.

Het Comité I merkt evenwel op dat, wanneer een veiligheidsdienst belast is met een operationele opdracht inzake terrorismebestrijding of bekleed is met een opdracht tot het beschermen van personen of installaties, het noodzakelijk is dat de agenten van deze dienst de daders van ernstige en feiten op heterdaad kunnen vasthouden teneinde hen zo snel mogelijk aan de politiediensten over te dragen. Dit principe is overigens opgenomen in de Belgische wet d.d. 20 juli 1990 betreffende de voorlopige hechtenis aangezien zelfs een privé-persoon iemand die hij op heterdaad betrapt bij het plegen van een misdaad of wanbedrijf kan vasthouden teneinde de feiten onmiddellijk aan te geven bij een agent van de openbare macht.

In België kent de wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst een aantal bevoegdheden tot het uitoefenen van dwangmaatregelen van bestuurlijke politie toe aan de agenten van de Veiligheid van de Staat, die buiten het kader van enige gerechtelijke opdracht, maar in de hoedanigheid van beschermingsofficieren belast zijn met het beschermen van personen.

«(...) en ze niet te betrekken bij de strijd tegen de georganiseerde misdaad, behalve in heel speciale gevallen, wanneer de georganiseerde misdaad een reële bedreiging vormt voor de vrije democratische orde van de Staat.» (1)

Commentaar :

Het Comité I kan niet akkoord gaan met deze aanbeveling die nadelig zou zijn voor de strijd tegen de georganiseerde misdaad, zij het nationaal of internationaal. Het Comité I is inderdaad van mening dat misdadige organisaties een gevaar betekenen voor de democratische orde en de integriteit van de Staat en dat het bijgevolg past de samenwerking tussen de veiligheidsdiensten en de politiediensten te bevorderen teneinde deze vorm van criminaliteit te voorkomen en te bestrijden.

David Bickford, een eminent Brits jurist, zegt: «*Fighting crime, successfully, relies on information. First of all, gathering information which can be turned into evidence to support proceedings against suspects, both private and corporate. This information comes from public sources and secret sources,*

(1) Vrije vertaling.

sources, such as informants and electronic surveillance. This information must be shared not only amongst the various state agencies fighting crime but also internationally between such bodies and also between the juridical bodies supervising the prosecutions or other proceedings (1). »

C'est bien l'option qu'a retenue la loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité. L'activité des *« organisations criminelles »* y est par ailleurs considérée comme une menace collective qui ressort des attributions de la Sûreté de l'État (article 8, 1º, *f)*).

Le Comité R estime donc que la mission des services de renseignement est bien de recueillir et de traiter des informations sur la criminalité organisée (par exemple dans certains secteurs économiques). C'est aussi le rôle des services de renseignement d'évaluer si la criminalité organisée constitue réellement une menace pour la sécurité nationale ou l'ordre démocratique (par exemple, dans le cadre de la passation de certains contrats publics).

Le Comité R ne partage pas davantage les considérations qui justifient la recommandation susmentionnée (III. Exposé des motifs, points 35 à 41).

Ainsi, *« les représentants des organisations non gouvernementales (...) notent également que les méthodes employées par ces services (de sécurité) ne sont pas adaptées aux procédures judiciaires »* (exposé des motifs, point 37). *« (...) Les méthodes employées par les services de sécurité intérieure ne sont pas vraiment adaptées aux exigences procédurales en matière d'enquête judiciaire et de procès au pénal »* (exposé des motifs, point 40) (2).

Commentaire :

De telles constatations n'ont de valeur que là où les services de sécurité ont aussi une compétence judiciaire. Le Comité R estime pour sa part que les agents des services de renseignement ne doivent pas recevoir la compétence d'effectuer des perquisitions, ni d'autres mesures d'instruction à des fins judiciaires; ces prérogatives doivent rester des attributions des services de police. Le Comité R souligne en outre que ces derniers services travaillent de plus en plus avec des méthodes empruntées aux services de renseignement (exemples : recherche pro-active, utilisation d'informateurs, ...)

(1) *« Balanced secrecy in the new informatiion age »* intervention de David Bickford au colloque « Secret d'État ou transparence ? » organisé le 20 janvier 1999 par le Comité R.

(2) Traduction libre.

such as informants and electronic surveillance. This information must be shared not only amongst the various state agencies fighting crime but also internationally between such bodies and also between the juridical bodies supervising the prosecutions or other proceedings. » (1)

De Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst heeft deze optie gekozen. De activiteit van de « criminele organisaties » wordt er overigens beschouwd als een collectieve bedreiging die onder de bevoegdheden valt van de Veiligheid van de Staat (artikel 8, 1º, *f)*).

Het Comité I is dus van mening dat de inlichtingendiensten wel degelijk de opdracht hebben informatie te verzamelen en te verwerken over de georganiseerde misdaad (bijvoorbeeld in bepaalde economische sectoren). Voorts moeten de inlichtingendiensten nagaan of de georganiseerde misdaad werkelijk een bedreiging vormt voor de nationale veiligheid of de democratische orde (bijvoorbeeld bij het afsluiten van sommige overheidscontracten).

Het Comité I gaat evenmin akkoord met de overwegingen waarop de bovenstaande aanbeveling steunt (III. Memorie van toelichting, punten 35 tot 41).

Bijvoorbeeld : *« de vertegenwoordigers van niet-gouvernementele organisaties (...) merken ook op dat de methodes die deze (veiligheids)diensten gebruiken, niet aangepast zijn aan de gerechtelijke procedures »* (Memorie van toelichting, punt 37). *« (...) De methodes die de binnenlandse veiligheidsdiensten gebruiken zijn niet echt aangepast aan de procedurevereisten inzake gerechtelijke onderzoeken en processen in strafzaken »* (Memorie van toelichting, punt 40) (2).

Commentaar :

Dergelijke vaststellingen bezitten slechts waarde indien de veiligheidsdiensten ook gerechtelijke bevoegdheid bezitten. Het Comité I vindt echter dat de agenten van de inlichtingendiensten niet de bevoegdheid moeten krijgen om huiszoekingen te verrichten noch om over te gaan tot andere onderzoeksmaatregelen met gerechtelijke doeleinden; deze prerogatieven moeten tot de bevoegdheden van de politiediensten blijven behoren. Bovendien onderstreept het Comité I dat de politiediensten steeds vaker methodes gebruiken die ze ontlenen aan de inlichtingendiensten (voorbeelden : pro-actief onderzoek, gebruiken van tipgevers, ...)

(1) *« Balanced secrecy in the new information age »*, exposé van David Bickford op het colloqiuim « Staatsgeheim of transparantie ? » dat het Comité I op 20 januari 1999 organiseerde.

(2) Vrije vertaling.

La mission des services de renseignement doit être de nature essentiellement préventive et informative, c'est-à-dire de prévenir les autorités politiques et administratives des menaces en cours de manière à leur permettre de prendre les décisions adéquates dans le cadre de leurs compétences.

Mais si les services de sécurité n'ont pas pour mission de poursuivre eux-mêmes les auteurs de crimes et de délits devant les tribunaux, le Comité R estime néanmoins qu'ils doivent collaborer avec les autorités judiciaires. En Belgique, l'article 29 du Code d'instruction criminelle fait obligation à *« toute autorité constituée, tout fonctionnaire ou officier public »* de donner avis sur-le-champ au ministère public de tout crime ou délit dont il acquiert connaissance dans l'exercice de ses fonctions. C'est cette disposition qui a fondé la Sûreté de l'État à conclure un protocole d'accord avec les procureurs généraux pour déterminer les modalités de communication de l'information. Ce protocole détermine aussi comment les agents de ce service peuvent apporter leur concours à des enquêtes judiciaires en qualité d'experts, notamment dans les domaines du contre-espionnage et du terrorisme.

« Toute limitation aux droits de l'homme et aux libertés protégés par la Convention européenne des droits de l'homme découlant d'activités menées par ces services doit être autorisée » (1)

— *« par la loi, ... »* (1)

Commentaire :

Le Comité R adhère pleinement à cette recommandation qui est conforme à la jurisprudence de la Cour européenne des droits de l'homme.

— *« ... et de préférence par un juge, préalablement à la conduite des opérations. »* (1)

Commentaire :

Les missions des services de sécurité n'étant pas de nature judiciaire, le Comité R est réticent à l'idée de l'intervention préalable d'un juge dans la conduite de leurs opérations.

Ceci ferait de lui un acteur trop étroitement associé aux prises de décisions des services de sécurité et l'empêcherait donc de pouvoir exercer sur eux son contrôle *a posteriori*.

(1) Traduction libre.

De opdracht van de inlichtingendiensten moet essentieel van preventieve en informatieve aard zijn, dit wil zeggen dat ze de politieke en bestuurlijke overheden moeten waarschuwen voor bestaande bedreigingen teneinde hen in staat te stellen in het kader van hun bevoegdheden de gepaste maatregelen te nemen.

Ook al hebben de veiligheidsdiensten niet de opdracht zelf de daders van misdaden en wanbedrijven voor de rechtbanken te vervolgen, moeten ze volgens het Comité I samenwerken met de gerechtelijke overheden. In België bevat artikel 29 van het Wetboek van Strafvordering de verplichting *« voor iedere gestelde overheid, ieder openbaar officier of ambtenaar »* het openbaar ministerie onmiddellijk op de hoogte te brengen van elke misdaad of elk wanbedrijf waarvan hij in de uitoefening van zijn ambt kennis krijgt. Op grond van deze bepaling heeft de Veiligheid van de Staat met de procureurs-generaal een protocolakkoord gesloten waarin de voorwaarden betreffende het meedelen van de informatie worden vastgesteld. Het protocol bepaalt voorts hoe de agenten van deze dienst als experten kunnen meewerken aan gerechtelijke onderzoeken, in het bijzonder op het gebied van contraspionage en terrorismebestrijding.

« Elke beperking van de mensenrechten en de vrijheden die door het Europees Verdrag over de rechten van de mens worden beschermd, als gevolg van activiteiten van deze diensten, moet worden toegelaten » (1)

— *« door de wet, (...) »* (1)

Commentaar :

Het Comité I is het volledig eens met deze aanbeveling, die conform is met de rechtspraak van het Europees Hof voor de rechten van de mens.

- *« (...) en bij voorkeur door een rechter, voorafgaand aan het uitvoeren van de operaties. »* (1)

Commentaar :

Aangezien de opdrachten van de veiligheidsdiensten niet van gerechtelijke aard zijn, staat het Comité I terughoudend tegen het idee dat een rechter van tevoren moet tussenkomen bij het uitvoeren van hun operaties.

In dit geval zou hij te nauw betrokken zijn bij de beslissingen die de veiligheidsdiensten nemen, waardoor hij zijn toezicht op deze diensten niet *a posteriori* zou kunnen uitoefenen.

(1) Vrije vertaling.

7. *«L'assemblée considère que chaque pays devrait prendre les mesures efficaces qui s'imposent pour satisfaire à ses propres exigences en matière de sécurité intérieure, tout en apportant la garantie de méthodes ...»* (1)

— *«de contrôle adaptées ...»* (1)

Commentaire :

Le Comité R adhère pleinement à cette recommandation ainsi qu'au point 33 de l'exposé des motifs dans lequel il est fait référence à l'exposé de l'expert M. Robin Robison pour qui *«toute instance de contrôle, que ce soit au niveau du pouvoir exécutif ou législatif (et même, ... du pouvoir judiciaire) doit — condition préalable essentielle — être dotée de personnel à plein temps disposant de ressources suffisantes»* (1).

Les moyens de contrôle décrits par M. Robison (accès aux dossiers, pouvoir de mener des enquêtes d'office, confidentialité ou capacité de rendre public les abus) sont d'ailleurs ceux dont dispose le Comité R.

— *«et conformes à une norme démocratique uniforme. (...)»* (1)

Commentaire :

Le Comité R pense que si la norme démocratique doit être commune, chaque État doit cependant disposer de la liberté d'organiser le contrôle de ses services de sécurité comme il l'entend.

8. *«L'assemblée recommande par conséquent au Comité des ministres de rédiger une convention-cadre relative aux services de sécurité intérieure, en tenant compte des lignes directrices ci-dessous, qui font partie intégrante de cette recommandation»* (1).

Commentaire :

Le Comité R adhère à cette recommandation sous réserve des remarques importantes qu'il formule à l'égard de certaines des lignes directrices ci-après. Il souhaite en outre que la Convention-cadre définisse la notion de *«service de sécurité intérieure»*.

(1) Traduction libre.

7. *«De vergadering vindt dat elk land de noodzakelijke doeltreffende maatregelen zou moeten nemen om te voldoen aan zijn eigen vereisten inzake interne veiligheid, en tegelijk moet instaan voor (...)»* (1)

— *«passende methodes van toezicht (...)»* (1)

Commentaar :

Het Comité I gaat volledig akkoord met deze aanbeveling, alsmede met punt 33 van de Memorie van toelichting waarin wordt verwezen naar het exposé van de expert Robin Robison, voor wie *«elke instantie die met toezicht is belast, op het niveau van de uitvoerende of wetgevende macht (en zelfs, ... van de rechterlijke macht), uitgerust moet zijn — dit is een essentiële voorafgaande voorwaarde — met voltijds tewerkgesteld personeel dat over voldoende middelen beschikt»* (1).

De middelen van toezicht die de heer Robison beschrijft (toegang tot dossiers, ambtshalve bevoegdheid om onderzoeken te voeren, vertrouwelijkheid of vermogen om misbruiken openbaar te maken), zijn overigens de middelen waarover het Comité I beschikt.

— *«die beantwoorden aan een uniforme democratische norm (...)»* (1)

Commentaar :

Het Comité I is van oordeel dat ook al moet de democratische norm gemeenschappelijk zijn, elke Staat over de vrijheid moet beschikken om het toezicht op zijn veiligheidsdiensten naar eigen goeddunken te organiseren.

8. *«Bijgevolg beveelt de vergadering het Ministerieel Comité aan een kaderovereenkomst op te stellen betreffende de binnenlandse veiligheidsdiensten, rekening houdend met de onderstaande richtlijnen die volledig deel uitmaken van de onderhavige aanbeveling.»* (1)

Commentaar :

Het Comité I gaat akkoord met deze aanbeveling, onder voorbehoud van de belangrijke opmerkingen met betrekking tot sommige van de hierna beschreven richtlijnen. Voorts wenst het Comité I dat de kaderovereenkomst een duidelijke definitie bevat van het begrip *«binnenlandse veiligheidsdienst»*.

(1) Vrije vertaling.

LIGNES DIRECTRICES

A. Concernantl'organisationdesservicesdesécurité intérieure

i. « Tout service de sécurité intérieure doit être organisé et fonctionner sur des bases légales, c'est-à-dire conformément à des lois nationales adoptées par le Parlement suivant la procédure législative normale et publiées dans leur intégralité. » (1)

Commentaire :

Le Comité R ne peut qu'adhérer à cette recommandation.

ii. « Les services de sécurité intérieure doivent avoir pour seule mission de protéger la sécurité nationale. Celle-ci consiste à combattre toute menace visible et réelle pour l'ordre démocratique de l'État et la société. Les objectifs économiques ou la lutte contre le crime organisé en soi ne devraient pas faire partie de cette mission. Ils ne devraient s'occuper d'objectifs économiques ou de crime organisé que lorsqu'ils représentent un danger réel et présent pour la sécurité nationale. » (1)

Commentaire :

Le Comité R a déjà expliqué aux points 3 et 6 ses remarques concernant les mots « menace visible et réelle » et la mission des services de sécurité en rapport avec le crime organisé. En ce qui concerne les objectifs économiques, le Comité R estime qu'il est légitime de confier aux services de sécurité une mission de protection des intérêts économiques nationaux contre l'espionnage, le sabotage ou la prise en main par des organisations criminelles. Cette mission doit être exercée dans l'intérêt général, l'intérêt particulier d'une entreprise ne peut être confondu avec l'intérêt général. Le Comité R estime aussi qu'il est contraire au droit de confier des missions d'espionnage économique aux services de sécurité.

iii. « L'exécutif ne peut être autorisé à élargir la mission de ces services; (...) » (1)

(1) Traduction libre.

RICHTLIJNEN

A. Over de organisatie van de binnenlandse veiligheidsdiensten

i. « Elke binnenlandse veiligheidsdienst moet georganiseerd zijn en functioneren overeenkomstig wettelijke grondslagen, dat wil zeggen krachtens de nationale wetten die het parlement volgens de normale wetgevende procedure heeft goedgekeurd en die volledig zijn gepubliceerd. » (1)

Commentaar :

Het Comité I is het volledig eens met deze aanbeveling.

ii. « De enige opdracht van de binnenlandse veiligheidsdiensten moet erin bestaan de nationale veiligheid te beschermen. Dit betekent dat ze elke zichtbare en reële bedreiging voor de democratische orde van de Staat en de samenleving bestrijdt. Economische doelstellingen of de strijd tegen de georganiseerde misdaad op zich zouden geen deel mogen uitmaken van deze opdracht. Binnenlandse veiligheidsdiensten zouden zich slechts moeten bekommeren om economische doelstellingen of om de georganiseerde misdaad wanneer ze een reëel en bestaand gevaar vormen voor de nationale veiligheid. » (1)

Commentaar :

In de punten 3 en 6 heeft het Comité I reeds kennis gegeven van zijn bedenkingen bij het begrip « zichtbare en reële bedreiging », en over de opdracht van de veiligheidsdiensten inzake de georganiseerde misdaad. Met betrekking tot de economische doelstellingen is het Comité I van mening dat het wettig is de veiligheidsdiensten te belasten met het beschermen van de nationale, economische belangen tegen spionage, sabotage of tegen het inpalmen van deze belangen door misdadige organisaties. Deze opdracht moet in het algemeen belang worden uitgeoefend en het particuliere belang van een onderneming mag niet worden verward met het algemeen belang. Het Comité I is ook nog van mening dat het toekennen van opdrachten van economische spionage aan de veiligheidsdiensten strijdig is met het recht.

iii. « De uitvoerende macht mag geen toelating krijgen om de opdracht van deze diensten uit te breiden; (...) » (1)

(1) Vrije vertaling.

Commentaire :

Cette recommandation est contraire à la faculté dont dispose le pouvoir législatif de déléguer des compétences à l'exécutif. Elle s'oppose au principe retenu par la loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité qui laisse au « Roi sur proposition du Comité ministériel » (du renseignement) le soin de définir « tout autre intérêt fondamental du pays » dont la Sûreté de l'État aurait à s'occuper. Lors de la discussion du projet de loi, la majorité gouvernementale a rejeté un amendement présenté par un député de l'opposition qui visait à supprimer cette compétence de l'exécutif (1).

— « (...) leurs objectifs doivent être définis par la loi (...) » (2)

Commentaire :

Le Comité R adhère à cette ligne directrice.

— « (...) et interprétés, en cas de conflit d'interprétation, par les juges (et non par les différents gouvernements). » (2)

Commentaire :

Le Comité R estime que la présente ligne directrice confond le rôle du juge et celui de l'exécutif en matière d'application et d'interprétation de la loi. Les attributions de l'un ne peuvent exclure celles de l'autre. Le gouvernement ayant pour tâche d'appliquer la loi dispose nécessairement d'une marge d'appréciation générale. Le pouvoir judiciaire, quant à lui, est juge de la constitutionnalité et de la légalité des actes de l'exécutif dans les litiges ponctuels qui lui sont soumis. En Belgique, le juge peut porter les conflits de compétence entre les diverses autorités publiques devant la Cour d'arbitrage.

— « Les services de sécurité intérieure ne doivent pas servir d'instrument d'oppression de partis politiques, de minorités nationales, de groupes religieux ou d'autre catégories particulières de la population. » (2)

Commentaire :

Le Comité R ne peut qu'adhérer à une telle déclaration de principe. Il souligne toutefois qu'une telle

(1) Chambre des représentants — s.o. 1998/1999 — 27 octobre 1998 — 638/19 — 95/96.

(2) Traduction libre.

Commentaar :

Deze aanbeveling is strijdig met het vermogen van de wetgevende macht om bevoegdheden toe te kennen aan de uitvoerende macht. De aanbeveling verzet zich tegen het principe opgenomen in de Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, dat het overlaat aan « de Koning, op voorstel van het Ministerieel Comité » (inzake inlichtingen), « eender welk ander fundamenteel belang van het land » te definiëren waarmee de Veiligheid van de Staat zich zou moeten bemoeien. Bij de bespreking van het wetsvoorstel verwierp de meerderheid een amendement van een lid van de oppositie waarmee hij deze bevoegdheid van de uitvoerende macht wilde afschaffen (1).

— « (...) hun doelstellingen moeten bij wet worden bepaald (...) » (2)

Commentaar :

Het Comité I gaat akkoord met deze richtlijn.

— « (...) en, in geval van conflict bij de interpretatie, door de rechters worden geïnterpreteerd (en niet door de verschillende regeringen). » (2)

Commentaar :

Het Comité I meent dat deze richtlijn de taak van de rechter en de taak van de uitvoerende macht verwart met betrekking tot het toepassen en interpreteren van de wet. De bevoegdheden van de ene kunnen de bevoegdheden van de ander niet uitsluiten. De regering heeft de opdracht de wet toe te passen en beschikt noodzakelijkerwijze over een algemene beoordelingsmarge. Van haar kant oordeelt de gerechtelijke macht over de grondwettelijkheid en de wettelijkheid van de handelingen van de uitvoerende macht in de specifieke geschillen die haar worden voorgelegd. In België kan een rechter bevoegdheidsconflicten tussen de diverse overheden voor het Arbitragehof brengen.

— « De binnenlandse veiligheidsdiensten mogen niet dienen om politieke partijen, nationale minderheden, religieuze groeperingen of andere specifieke bevolkingsgroepen te onderdrukken. » (2)

Commentaar :

Het Comité I kan niet anders dan akkoord gaan met een dergelijke principeverklaring. Het onder-

(1) Kamer van volksvertegenwoordigers — gewone zitting 1998/1999 — 27 oktober 1998 — 638/19 — 95/96.

(2) Vrije vertaling.

recommandation ne peut être interprétée dans le sens qu'un parti politique extrémiste, ou qu'un mouvement religieux quelconque, pratiquant des activités illégales, prônant la violence, l'instauration d'un régime totalitaire, théocratique ou autre qui violerait la dignité humaine, les droits de l'homme et les libertés fondamentales, ne pourrait faire l'objet d'aucune surveillance de la part des services de sécurité.

La loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité a ainsi inclus les « organisations sectaires nuisibles » parmi les menaces relevant des missions de surveillance de la Sûreté de l'État (article 8, 1º *e*).

iv. « Il est préférable que l'organisation des services de sécurité intérieure ne relève pas de structures militaires. Les services de sécurités civils ne devraient pas non plus fonctionner comme des structures militaires ou semi-militaires. » (1)

Commentaire :

Le Comité R n'adhère pas au caractère réducteur de cette recommandation; il considère que ce n'est pas l'organisation militaire, semi-militaire ou civile d'un service de sécurité qui est susceptible de poser problème, mais bien le cas échéant, l'insuffisance de son cadre légal et/ou de son contrôle.

v. « Les États membres ne doivent pas recourir à des sources de financement autres que gouvernementales pour leurs services de sécurité intérieure, les dépenses de ces derniers devant être imputées exclusivement au budget de l'État. » (1)

Commentaire :

Cette recommandation pêche par l'absence de définition des sources de financement « gouvernementales ». Elle a néanmoins le mérite d'attirer l'attention sur le problème du financement des services de sécurité. Le Comité R estime quant à lui que le financement de ces services doit être à charge du budget de l'État, organisé par la loi et contrôlé.

— « Les budgets présentés au Parlement pour approbation doivent être détaillés et explicites. » (1)

(1) Traduction libre.

streept echter dat een dergelijke aanbeveling niet kan worden geïnterpreteerd in de zin dat de veiligheidsdiensten geen toezicht mogen uitoefenen op een extremistische politieke partij, of eender welke religieuze beweging, die illegale activiteiten beoefent, voorstander is van geweld of van de invoering van een totalitair, een theocratisch of enig ander regime dat de menselijke waardigheid, de rechten van de mens en de fundamentele vrijheden zou schenden.

De Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst heeft de « schadelijke sektarische organisaties » opgenomen in de lijst van bedreigingen die tot de toezichtsopdrachten van de Veiligheid van de Staat behoren (artikel 8, 1º *e*).

iv. « Het is verkieslijk dat de binnenlandse veiligheidsdiensten geen militaire structuur krijgen. Burgerlijke veiligheidsdiensten zouden evenmin mogen functioneren als militaire of semi-militaire structuren. » (1)

Commentaar :

Het Comité I gaat niet akkoord met het beperkend karakter van deze aanbeveling; het is van mening dat het niet de militaire, semi-militaire of burgerlijke organisatie van een veiligheidsdienst is die voor problemen kan zorgen, maar wel de eventuele ontoereikendheid van het wettelijk kader van deze dienst en/of van het toezicht erop.

v. « De lidstaten moeten voor hun binnenlandse veiligheidsdiensten alleen gebruik maken van financieringsbronnen van de overheid; de uitgaven van deze diensten mogen uitsluitend op de begroting van de Staat worden geboekt. » (1)

Commentaar :

Deze aanbeveling blijft in gebreke door geen definitie te geven van de financieringsbronnen « van de overheid ». Ze heeft wel de verdienste de aandacht te vestigen op het probleem van de financiering van de veiligheidsdiensten. Het Comité I is van mening dat de financiering van deze diensten ten laste van de begroting van de Staat moet vallen, wettelijk geregeld en gecontroleerd moet worden.

— « De budgetten die ter goedkeuring aan het Parlement worden overgelegd moeten gedetailleerd en expliciet zijn. » (1)

(1) Vrije vertaling.

Commentaire :

Le Comité R adhère à cette recommandation avec nuance car elle ne peut faire obstacle à la nécessaire confidentialité qui est de mise lors de l'examen par le Parlement de certains budgets.

En effet, les fonds affectés à certaines opérations spéciales des services de sécurité doivent rester secrets pour ne pas en compromettre la sécurité. Les personnes chargées du contrôle de l'utilisation de ces fonds doivent être tenues à un strict devoir de secret professionnel.

B. Concernant les activités opérationnelles des services de sécurité intérieure

i. « Les services de sécurité intérieure doivent respecter la Convention européenne des droits de l'homme. » (1)

Commentaire :

Le Comité R ne peut qu'adhérer à cette recommandation.

ii. « Toute atteinte apportée par les activités opérationnelles des services de sécurité intérieure à la Convention européenne des droits de l'homme doit être autorisée par la loi. » (1)

Commentaire :

Le Comité R ne peut qu'adhérer à cette recommandation.

— « Les écoutes téléphoniques, mécaniques ou techniques, la surveillance auditive et visuelle et toute autre mesure opérationnelle comportant un risque important de limitation des droits de l'individu doivent être soumises à une autorisation préalable, délivrée par le pouvoir judiciaire. » (1)

Commentaire :

Cette recommandation confond les missions des services de sécurité avec des missions de nature judiciaire; elle entre dès lors en contradiction avec la recommandation nº 6 qui vise à ne pas donner de

(1) Traduction libre.

Commentaar :

Het Comité I is het eens met deze aanbeveling, maar brengt toch enige nuancering aan, aangezien ze geen hinderpaal mag vormen voor de noodzakelijke vertrouwelijkheid die in acht moet worden genomen bij het onderzoek van bepaalde budgetten door het Parlement.

Immers, de middelen die voor bepaalde bijzondere opdrachten van de veiligheidsdiensten worden aangewend moeten geheim blijven om de veiligheid ervan niet in het gedrang te brengen. De personen belast met het toezicht op het gebruik van deze middelen moeten gebonden zijn door een strikte plicht het beroepsgeheim te bewaren.

B. Over de operationele activiteiten van de binnenlandse veiligheidsdiensten

i. « De binnenlandse veiligheidsdiensten moeten het Europees Verdrag voor de rechten van de mens naleven. » (1)

Commentaar :

Het Comité I is het volledig eens met deze aanbeveling.

ii. « Elke schending van het Europees Verdrag voor de rechten van de mens, die het gevolg is van de operationele activiteiten van de binnenlandse veiligheidsdiensten, moet bij wet worden goedgekeurd. » (1)

Commentaar :

Het Comité I is het volledig eens met deze aanbeveling.

— « Telefonische, mechanische of technische afluisteroperaties, auditieve en visuele bewaking en eender welke andere operationele maatregel die een belangrijk risico inhoudt op beperking van de rechten van het individu moeten het voorwerp zijn van een voorafgaande goedkeuring vanwege de rechterlijke macht. » (1)

Commentaar :

Deze aanbeveling verwart de opdrachten van de veiligheidsdiensten met de opdrachten van gerechtelijke aard; ze is dan ook in tegenspraak met aanbeveling nr. 6 die tot doel heeft geen gerechtelijke

(1) Vrije vertaling.

compétence judiciaire aux services de sécurité. Le Comité R rappelle donc ici sa réticence à l'idée de l'intervention préalable d'un juge dans la conduite de leurs opérations. Dans les pays qui disposent d'une législation permettant les écoutes de sécurité, c'est une autorité politique qui en assume la responsabilité, même si la procédure d'autorisation varie d'un pays à l'autre.

Ainsi, l'autorisation de procéder à des écoutes de sécurité est donnée :

— le plus souvent par l'autorité politique elle-même que ce soit le chef de l'État, le premier ministre, le ministre de l'Intérieur ou celui de la Justice, plusieurs ministres agissant conjointement, etc ... (États-Unis, France, Grande-Bretagne, Irlande, Pays-Bas, ...);

— par une autorité judiciaire à la demande de l'autorité politique qui en assure la responsabilité (Canada, Espagne); en cas d'urgence, la mesure peut être décidée par un ministre ou par un haut fonctionnaire de sûreté à condition que le juge en soit immédiatement informé;

— par un organe indépendant sur demande d'un ministre (Grand Duché de Luxembourg).

— « La législation devrait normalement définir les paramètres à prendre en compte — avant toute autorisation de perquisition ou concernant ces activités — par des juges ou des magistrats, (...). » (1)

Commentaire :

Le Comité R rappelle ici qu'il n'est pas favorable à l'idée de permettre aux services de renseignement de procéder à des perquisitions. Dans les pays qui disposent d'une législation permettant les écoutes de sécurité, l'autorisation de procéder à de telles écoutes est assortie de conditions dont la réalisation fait l'objet d'un contrôle préalable. Le Comité R estime que la loi doit effectivement prévoir des paramètres à prendre en compte avant toute autorisation permettant à un service de sécurité d'intercepter des communications. Cependant, accorder à des juges ou à des magistrats ce pouvoir de fixer des conditions préalables en ce qui concerne les services de sécurité contredit la recommandation de ne pas leur donner de compétences judiciaires.

(1) Traduction libre.

bevoegdheid toe te kennen aan de veiligheidsdiensten. Het Comité I herhaalt dus dat het terughoudend staat tegen het idee dat een rechter van tevoren moet tussenkomen bij het uitvoeren van hun operaties. In landen met een wetgeving die het afluisteren uit veiligheidsoverwegingen toelaat, draagt een politieke overheid daarvoor de verantwoordelijkheid, ook al is de toelatingsprocedure verschillend van land tot land.

De toelating om over te gaan tot afluisteroperaties met het oog op de veiligheid wordt gegeven :

— meestal door de politieke overheid zelf, ongeacht of het gaat om het staatshoofd, de eerste minister, de minister van Binnenlandse Zaken of van Justitie, verschillende ministers die gezamenlijk optreden, enz. (Verenigde Staten, Frankrijk, Groot-Brittannië, Ierland, Nederland, ...);

— door een gerechtelijke overheid op verzoek van de politieke overheid die de verantwoordelijkheid blijft dragen (Canada, Spanje); in dringende gevallen kan een minister of een hoge veiligheidsambtenaar beslissen tot de maatregel over te gaan, op voorwaarde dat de rechter onmiddellijk op de hoogte wordt gebracht;

— door een onafhankelijk orgaan op verzoek van een minister (Groothertogdom Luxemburg).

— « Normaal zou de wetgeving de parameters moeten bepalen waarmee rechters of magistraten rekening moeten houden vóór ze een toelating tot huiszoeking of met betrekking tot deze activiteiten verlenen, (...). » (1)

Commentaar :

Het Comité I wijst erop dat het geen voorstander is van het idee om de inlichtingendiensten toe te laten huiszoekingen te verrichten. In landen met een wetgeving die het afluisteren uit veiligheidsoverwegingen toelaat, is de toelating om tot afluisteroperaties over te gaan verbonden aan bepaalde voorwaarden, waarvan vooraf wordt gecontroleerd of ze zijn vervuld. Het Comité I is van mening dat de wet inderdaad parameters moet vaststellen waarmee rekening moet worden gehouden vóór men een veiligheidsdienst de toelating verleent communicatie te onderscheppen. Wanneer men echter aan rechters of aan magistraten de bevoegdheid verleent om met betrekking tot de veiligheidsdiensten voorafgaande voorwaarden te bepalen, handelt men in strijd met de aanbeveling om aan deze diensten geen gerechtelijke bevoegdheden te verlenen.

(1) Vrije vertaling.

— « Ces paramètres devraient prendre en considération les exigences minimales ci dessous :

a. Il existe des raisons vraisemblables de croire qu'un individu a commis, commet ou est sur le point de commettre une infraction;

b. Il existe des raisons vraisemblables de croire que certaines communications ou preuves spécifiques en relation avec cette infraction pourront être obtenues par leur interception ou à l'occasion de visites domiciliaires, ou que la commission de l'infraction peut être évitée par le biais d'une arrestation;

c. Le recours aux procédures normales d'enquête a échoué ou apparaît soit peu susceptible d'aboutir, soit trop dangereux. » (1)

Commentaire :

Une fois de plus, cette recommandation confond les missions des services de sécurité avec des mission de nature judiciaire. Les paramètres proposés ne peuvent donc être appliqués aux services de sécurité sans contredire également la recommandation nº 6 qui tend à ne pas autoriser ces services à mener des enquêtes judiciaires.

— « L'autorisation d'entreprendre ce type d'activités doit être limitée dans le temps (trois mois au plus). Lorsque la surveillance ou l'interception des appels téléphoniques ont pris fin, l'intéressé doit être informé des mesures prises à son égard. » (1)

Commentaire :

Le Comité R adhère au principe d'une limitation dans le temps des mesures d'intrusion par les services de sécurité. Par ailleurs, dans son rapport d'activités de 1996, le Comité R a aussi souhaité que la décision de procéder à l'interception de communications individuelles soit notifiée aux particuliers qui ont fait l'objet de cette mesure trois ans après la fin de son exécution, comme cela se passe notamment en Allemagne.

La notification doit permettre aux personnes qui ont fait l'objet d'une telle surveillance d'exercer leur droit de recours éventuel. Le Comité R a cependant souligné qu'il ne devait pas y avoir obligation de notifier une écoute individuelle si cette formalité risquait de mettre en péril la mission pour laquelle elle a été effectuée.

(1) Traduction libre.

— « Deze parameters zouden de onderstaande minimale vereisten moeten bevatten :

a. Er bestaan aannemelijke redenen om te geloven dat een individu een inbreuk heeft gepleegd, pleegt of op het punt staat een inbreuk te plegen;

b. Er bestaan aannemelijke redenen om te geloven dat bepaalde communicaties of specifieke bewijzen in verband met deze inbreuk kunnen worden verkregen door hun interceptie of ter gelegenheid van huiszoekingen, of dat het plegen van de inbreuk kan worden voorkomen door middel van een arrestatie;

c. Het aanwenden van de normale onderzoeksprocedures heeft niets opgeleverd of lijkt weinig kans van slagen te hebben dan wel te gevaarlijk te zijn. » (1)

Commentaar :

Eens te meer verwart deze aanbeveling de opdrachten van de veiligheidsdiensten met opdrachten van gerechtelijke aard. De voorgestelde parameters kunnen niet op de veiligheidsdiensten worden toegepast zonder te handelen in strijd met aanbeveling nr. 6, die tot doel heeft deze diensten geen toelating te verlenen om gerechtelijke onderzoeken te voeren.

— « De toelating om dit type activiteiten te verrichten moet in de tijd worden beperkt (maximum drie maanden). Nadat een einde is gekomen aan de bewaking of de interceptie van telefoongesprekken, moet de betrokkene kennis krijgen van de maatregelen die jegens hem zijn genomen. » (1)

Commentaar :

Het Comité I is voorstander van het principe om de maatregelen van indringing door de veiligheidsdiensten in de tijd te beperken. In zijn activiteitenverslag van 1996 formuleerde het Comité I de aanbeveling dat personen die het voorwerp zijn van de interceptie van individuele communicatie drie jaar na het einde van de uitvoering van deze opdracht kennis zouden krijgen van de bewuste beslissing, zoals dat met name in Duitsland gebeurt.

Deze kennisgeving laat de personen die het voorwerp zijn geweest van een dergelijke bewaking toe hun recht op eventueel beroep uit te oefenen. Het Comité I benadrukte echter dat deze verplichting om kennis te geven van een individuele afluisteroperatie niet zou gelden indien de opdracht in het kader waarvan deze operatie plaatsvond daardoor in het gedrang zou komen.

(1) Vrije vertaling.

Dans l'arrêt de référence en matière d'écoutes téléphoniques (« Klass c/RFA » du 6 septembre 1978), la Cour européenne des droits de l'homme a expressément admis que « la nécessité d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble » pouvait justifier que la personne écoutée ne soit pas avisée des mesures de surveillance auxquelles elle a été antérieurement soumise et qu'elle ne puisse recourir aux tribunaux quand on lève ces mesures.

iii. « Les services de sécurité intérieure ne doivent pas être autorisés à accomplir des actions de poursuites pénales, telles des enquêtes criminelles, (...) » (1)

Commentaire :

Le Comité R adhère à cette recommandation en soulignant toutefois qu'elle ne peut être interprêtée comme interdisant toute forme de collaboration entre les service de sécurité et les autorités judiciaires. Comme il l'a dit à propos de la recommandation nº 6, le Comité R est favorable à une telle collaboration.

— (...), des arrestations ou la mise en détention. » (1)

Commentaire :

Le Comité R adhère à cette recommandation en faisant toutefois remarquer que lorsqu'un service de sécurité est chargé d'une mission opérationnelle antiterroriste, ou lorsqu'il est investi d'une mission de protection de personnes ou d'installations, il est nécessaire que ses agents puissent retenir les auteurs de faits graves, pris en flagrant délit, pour les livrer dans les plus brefs délais aux forces de police.

C. Concernant le contrôle démocratique effectif des services de sécurité intérieure

i. « L'exécutif doit exercer un contrôle *a posteriori* des activités de ces services, (...) » (1)

Commentaire :

Le Comité R estime que l'exécutif ne peut se contenter d'exercer un contrôle a posteriori sur les services de sécurité. Il doit aussi contrôler la direction

(1) Traduction libre.

In het arrest dat inzake telefonische afluisteroperaties als referentie geldt (« Klass t/BRD » d.d. 6 september 1978), neemt het Europees Hof voor de Rechten van de Mens uitdrukkelijk aan dat « de noodzaak een geheim toezicht op te leggen teneinde het geheel van de democratische samenleving te beschermen » een gegronde reden kon zijn om de afgeluisterde persoon niet op de hoogte te brengen van de bewakingsmaatregelen waarvan hij in het verleden het voorwerp was en om de betrokkene niet de mogelijkheid te bieden verhaal te halen voor de rechtbank bij het opheffen van deze maatregelen.

iii. « Binnenlandse veiligheidsdiensten mogen geen toelating krijgen om handelingen van strafrechtelijke vervolgingen te stellen, zoals het voeren van criminele onderzoeken, (...) » (1)

Commentaar :

Het Comité I sluit zich aan bij deze aanbeveling, maar onderstreept dat ze niet kan worden geïnterpreteerd als een verbod op elke vorm van samenwerking tussen de veiligheidsdiensten en de gerechtelijke overheid. Zoals gezegd met betrekking tot aanbeveling nr. 6 is het Comité I voorstander van een dergelijke samenwerking.

— « (...), personen aan te houden of in hechtenis te nemen. » (1)

Commentaar :

Het Comité I sluit zich aan bij deze aanbeveling, maar merkt op dat wanneer een veiligheidsdienst belast is met een operationele opdracht van terrorismebestrijding of bekleed is met een opdracht tot het beschermen van personen of installaties, het noodzakelijk is dat zijn agenten de daders van ernstige feiten die ze op heterdaad betrappen kunnen vasthouden om hen zo snel mogelijk aan de politie over te dragen.

C. Over de effectieve democratische controle op de binnenlandse veiligheidsdiensten

i. « De uitvoerende macht moet *a posteriori* toezicht uitoefenen op de activiteiten van deze diensten, (..). » (1)

Commentaar :

Het Comité I meent dat de uitvoerende macht er geen genoegen mee mag nemen *a posteriori* toezicht uit te oefenen op de veiligheidsdiensten. Ze moet ook

(1) Vrije vertaling.

de ces services, leur assigner des missions prioritaires et assumer la responsabilité politique de leurs opérations. À ce titre, il appartient à un organe clairement identifié du pouvoir exécutif d'autoriser, dans le respect des conditions légales, le recours à des mesures exceptionnelles de coercition ou d'intrusion.

— «(...) en les obligeant par exemple à rédiger et présenter des rapports annuels détaillés sur leurs activités.»(1)

Commentaire :

La recommandation ne précise pas à qui ces rapports détaillés devraient être soumis. S'il s'agit de rapports destinés aux ministres responsables des services de sécurité, le Comité R y est favorable tout en soulignant la nécessité de classifier soigneusement ces documents.

S'il s'agit de rapports destinés à être publiés ou à faire l'objet d'une large diffusion, le Comité R estime alors que cette décision doit être entourée de garanties de nature à ne pas porter préjudice au bon fonctionnement des services, à la coopération internationale entre services, à la sécurité physique et à la protection de la vie privée des citoyens.

Le règlement d'ordre intérieur du Comité R définit d'ailleurs de cette manière les critères qu'il doit prendre en considération avant de prendre la décision de publier tout ou partie de ses rapports.

— «Il conviendrait de conférer à un seul ministre la responsabilité politique de contrôler et surveiller les services de sécurité intérieur, en lui donnant libre accès à ces services afin de permettre un contrôle effectif au quotidien.»(1)

Commentaire :

Cette ligne directrice ne parait pas en accord avec l'esprit général de la recommandation. Confier à un seul ministre la responsabilité politique des services de sécurité comporte les risques inhérents à toute concentration de pouvoir dans les mains d'un seul homme.

Cette ligne directrice n'est pas non plus en accord avec la double responsabilité ministérielle mise en oeuvre par la loi belge du 30 novembre 1998 organi-

(1) Traduction libre.

toezicht uitoefenen op de directie van deze diensten, hen met prioritaire opdrachten belasten en de politieke verantwoordelijkheid dragen voor hun operaties. In dit opzicht moet een duidelijk geïdentificeerd orgaan van de uitvoerende macht de bevoegdheid krijgen om, met naleving van de wettelijke voorwaarden, het gebruik toe te laten van uitzonderlijke maatregelen van dwang of indringing.

— «(...) door ze bijvoorbeeld te verplichten gedetailleerde jaarlijkse verslagen betreffende hun activiteiten op te stellen en over te leggen.»(1)

Commentaar :

De aanbeveling bepaalt niet aan wie deze verslagen moeten worden voorgelegd. Indien de verslagen bestemd zijn voor de ministers bevoegd voor de veiligheidsdiensten, is het Comité I het eens met deze aanbeveling, maar benadrukt ze dat deze documenten zorgvuldig moeten worden geclassificeerd.

Indien het de bedoeling is deze verslagen te publiceren of op grote schaal te verspreiden, is het Comité I van mening dat deze beslissing gepaard moet gaan met bepaalde garanties teneinde ervoor te zorgen dat er geen afbreuk wordt gedaan aan de goede werking van de diensten, aan de internationale samenwerking tussen diensten, aan de lichamelijke veiligheid en aan de bescherming van de persoonlijke levenssfeer van de burgers.

Het huishoudelijk reglement van het Comité I definieert trouwens op deze wijze de criteria waarmee het rekening moet houden alvorens te beslissen zijn verslagen of een deel ervan te publiceren.

— «Het zou passen de politieke verantwoordelijkheid voor de controle van en het toezicht op de binnenlandse veiligheidsdiensten aan één enkele minister toe te kennen, door hem vrij toegang te verlenen tot deze diensten teneinde een doeltreffende dagelijkse controle mogelijk te maken.»(1)

Commentaar :

Deze richtlijn lijkt in strijd te zijn met de algemene geest van de aanbeveling. De politieke verantwoordelijkheid over de veiligheidsdiensten aan slechts één minister toevertrouwen brengt de risico's mee die inherent verbonden zijn aan elke machtsconcentratie bij één persoon.

Deze richtlijn komt evenmin overeen met het principe van dubbele ministeriële verantwoordelijkheid met betrekking tot de Veiligheid van de Staat, ont-

(1) Vrije vertaling.

que des services de renseignement et de sécurité à l'égard de la Sûreté de l'État. Alors que ce service est placé sous l'autorité du ministre de la Justice, le ministre de l'Intérieur dispose également du droit de réquérir la Sûreté de l'État pour certaines missions, notamment en vue du maintien de l'ordre et de la protection des personnes.

De même, le ministre de l'Intérieur est associé à l'organisation et à l'administration de la Sûreté de l'État dans ces matières.

Le Comité R estime aussi que la recommandation précitée ne peut s'opposer à ce qu'un organe ministériel collégial (tel le Comité ministériel du renseignement en Belgique) adresse des directives d'ordre général à un service de sécurité.

— « Le ministre doit adresser annuellement un rapport au Parlement sur les activités des services de sécurité intérieure. » (1)

Commentaire :

Le Comité R estime que cette recommandation ne doit pas faire obstacle à ce que le ministre responsable ait à répondre, à tout moment, aux questions et interpellations parlementaires relatives aux services de sécurité.

ii. « Le pouvoir législatif doit adopter des lois claires et appropriées qui donnent à ces services une base statutaire. Ces textes doivent préciser quelles catégories d'activités impliquant un risque élevé de violation des droits individuels peuvent être exercées, et dans quelles circonstances, et établir les garanties voulues contre les abus. Le pouvoir législatif doit également contrôler de façon stricte le budget de ces services, en obligeant entre autres ces derniers à lui soumettre des rapports annuels détaillés sur l'utilisation des ressources, et mettre en place de commissions spéciales de contrôle. »

Commentaire :

Le Comité R s'est déjà exprimé sur le contenu de cette ligne directrice.

iii. « Les juges doivent être autorisés à exercer un large contrôle *a priori* et *a posteriori,* notamment à délivrer des autorisations préalables concernant certaines activités présentant un grand risque pour les droits de l'homme. (...) » (1)

(1) Traduction libre.

wikkeld in de Belgische wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst. Terwijl deze dienst onder het gezag van de minister van Justitie staat, geniet de minister van Binnenlandse Zaken eveneens het recht de Veiligheid van de Staat te vorderen om bepaalde opdrachten uit te voeren, in het bijzonder met het oog op het handhaven van de orde en het beschermen van personen.

Bovendien wordt de minister van Binnenlandse Zaken betrokken bij de organisatie en de administratie van de Veiligheid van de Staat in de bovengenoemde materies.

Voorts meent het Comité I dat de voornoemde aanbeveling zich er niet tegen kan verzetten dat een collegiaal ministerieel orgaan (zoals het Ministerieel Comité voor inlichtingen in België) aan een veiligheidsdienst algemene richtlijnen verstrekt.

— « De minister moet jaarlijks een verslag over de activiteiten van de binnenlandse veiligheidsdiensten aan het Parlement bezorgen. » (1)

Commentaar :

Het Comité I is van mening dat deze aanbeveling niet mag verhinderen dat de verantwoordelijke minister te allen tijde moet antwoorden op parlementaire vragen en interpellaties betreffende de veiligheidsdiensten.

ii. « De wetgevende macht moet duidelijke en passende wetten goedkeuren die aan deze diensten statutaire grond verlenen. Deze teksten moeten duidelijk vermelden welke categorieën van activiteiten, die een hoog risico van schending van de individuele rechten meebrengen, mogen worden uitgevoerd, alsook onder welke voorwaarden, en de gewenste waarborgen tegen misbruiken vaststellen. Voorts moet de wetgevende macht streng toezicht houden op het budget van deze diensten, onder meer door hen ertoe te verplichten gedetailleerde jaarlijkse verslagen over het gebruik van de middelen over te leggen en door bijzondere commissies van toezicht te creëren. »

Commentaar :

Het Comité I heeft zijn mening al gegeven over de inhoud van deze richtlijn.

iii. « De rechters moeten de toelating krijgen om *a priori* en *a posteriori* in ruime mate toezicht uit te oefenen, in het bijzonder om voorafgaande toelatingen te verlenen met betrekking tot bepaalde activiteiten die een groot risico voor de mensenrechten inhouden (...). » (1)

(1) Vrije vertaling.

Commentaire :

Le Comité R a déjà expliqué pourquoi il estime que le contrôle *a priori* des services de sécurité doit d'abord ressortir du pouvoir exécutif, le contrôle *a posteriori*, du pouvoir judiciaire et d'organes de contrôle indépendants.

iv. « Les autres organes (par exemple : médiateurs et commissaires à la protection des données) doivent être autorisés, au cas par cas, à exercer un contrôle *a posteriori* des services de sécurité. » (1)

Commentaire :

Cette formulation ambigüe ne doit pas limiter le champ d'action des organes de contrôle indépendants. Le Comité R estime au contraire qu'une instance indépendante peut efficacement contrôler *a posteriori* l'exercice de certaines prérogatives des organes de sécurité intérieure.

C'est le cas notamment en Allemagne, en France et en Grande-Bretagne où il existe des organes de recours auxquels les particuliers peuvent s'adresser lorsqu'ils estiment avoir fait injustement l'objet de mesures d'écoutes de sécurité.

En Belgique, le Comité R peut également examiner les plaintes et dénonciations des particuliers qui ont été directement concernés par l'intervention d'un service de renseignement. Ce même comité a également été instauré comme organe de recours indépendant chargé de statuer en degré d'appel sur les refus et les retraits d'habilitations de sécurité, ce qui constitue un mode de contrôle *a posteriori* efficace des services de sécurité (2).

v. « Tout individu doit jouir d'un droit général d'accès aux informations collectées et mise en mémoire par le(s) service(s) de sécurité intérieure, sous réserve de dérogations clairement définies par la loi, liées à la sécurité nationale. » (1)

Commentaire :

Le Comité R n'est pas favorable à l'instauration d'un droit général d'accès aux informations collectées et traitées par les services de sécurité. En Belgique,

(1) Traduction libre.

(2) Voir la loi belge du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité; *Moniteur Belge* du 7 mai 1998 p. 15758.

Commentaar :

Het Comité I heeft al uitgelegd waarom het van mening is dat het toezicht *a priori* op de veiligheidsdiensten in de eerste plaats tot de bevoegdheden van de uitvoerende macht moet behoren en het toezicht *a posteriori* tot de bevoegdheden van de gerechtelijke overheid en van autonome toezichtsorganen.

iv. « Andere organen (bijvoorbeeld : bemiddelaars en commissarissen voor de bescherming van gegevens) moeten geval per geval de toelating krijgen om *a posteriori* toezicht uit te oefenen op de veiligheidsdiensten. » (1)

Commentaar :

Deze dubbelzinnige formulering mag het actieterrein van de autonome toezichtsorganen niet beperken. Het Comité I is daarentegen van mening dat een onafhankelijke instantie *a posteriori* doeltreffend kan toezien op de uitoefening van bepaalde prerogatieven van de binnenlandse veiligheidsorganen.

Dit gebeurt onder meer in Duitsland, in Frankrijk en in Groot-Brittannië, waar er beroepsorganen bestaan tot dewelke particulieren zich kunnen wenden wanneer ze van mening zijn dat ze ten onrechte het voorwerp zijn geweest van maatregelen van afluisteroperaties om veiligheidsredenen.

In België is het Comité I bevoegd om de klachten en aangiften te onderzoeken van particulieren die rechtstreeks betrokken waren bij de interventie van een inlichtingendienst. Het Comité I bezit ook de hoedanigheid van autonoom beroepsorgaan, dat in graad van beroep uitspraak moet doen over weigeringen en intrekkingen van veiligheidsmachtigingen. Dit is een doeltreffende manier om *a posteriori* toezicht uit te oefenen op de veiligheidsdiensten (2).

v. « Elk individu moet een algemeen recht genieten van toegang tot de gegevens die worden verzameld en opgeslagen door de binnenlandse veiligheidsdienst(en), onder voorbehoud van afwijkingen die de wet duidelijk omschrijft en die verband houden met de nationale veiligheid. » (1)

Commentaar :

Het Comité I is geen voorstander van de invoering van een algemeen recht van toegang tot informatie die de veiligheidsdiensten verzamelen en verwerken. In

(1) Vrije vertaling.

(2) Belgische wet d.d. 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen — *Belgisch Staatsblad* van 7 mei 1998, blz. 15758.

cette matière est réglée par la loi du 8 décembre 1992 sur la protection de la vie privée, ainsi que par la loi du 11 avril 1994 relative à la publicité de l'administration.

Ces dispositions instituent et organisent le droit des particuliers de consulter sur place et de recevoir une copie d'un document administratif d'une autorité administrative fédérale. Une série de motifs sont prévus pour rejeter une demande de consultation; il en est ainsi lorsque l'intérêt de la publicité ne l'emporte pas sur la protection d'intérêts tels que notamment, la sécurité de la population, l'ordre public, la sûreté ou la défense nationales.

En 1997, après avoir examiné l'application de ces dispositions, le Comité R a conclu que la possibilité d'accès direct d'un particulier à son dossier individuel auprès d'un service de renseignement n'existait que de manière théorique. Il a estimé qu'une personne faisant état d'un préjudice matériel ou moral vraisemblable en rapport avec des informations contenues sur elle dans un dossier des services de renseignements devrait pouvoir obtenir, sous certaines conditions mais de manière plus large qu'aujourd'hui, un droit de consulter ces documents. Pour le Comité R, l'opportunité de permettre ou de refuser cet accès ne doit pas être laissé à la seule appréciation des services de renseignements.

Le Comité R a préconisé à cet égard une procédure et des conditions d'accès inspirées par les législations suisse et française où il existe une « Commission consultative du secret de la Défense nationale ». Un organisme collégial tel que la Commission de la protection de la vie privée, ou le Comité R, en accord avec le ministre compétent, pourrait constater que la communication de certaines informations ne met pas en cause la sûreté de l'État, la défense et la sécurité publique et qu'il y aurait donc lieu de les transmettre en tout ou en partie au demandeur.

Certaines informations ne pourraient jamais être communiquées, notamment : le nom des membres des services de renseignements chargés de collecter et de traiter les informations personnelles, le nom des personnes ayant fourni de bonne foi les informations au service de renseignements, des informations relatives à la vie privée de tiers, des informations recueillies dans le cadre d'une procédure judiciaire en cours, des informations communiquées par un service de renseignement ou de sécurité étranger.

Lorsque des raisons de sûreté de l'État, de défense nationale et de sécurité publique s'opposent à la communication d'informations, l'organisme de

België wordt deze materie geregeld door de wet d.d. 8 december 1992 tot bescherming van de persoonlijke levenssfeer en door de wet d.d. 11 april 1994 betreffende de openbaarheid van bestuur.

Deze bepalingen creëren en organiseren het recht van particulieren om ter plaatse inzage te nemen van een administratief document van een federale bestuurlijke overheid en om daarvan een kopie te nemen. Ze stellen ook een aantal redenen vast om een verzoek tot inzage te verwerpen; dit gebeurt wanneer het belang van de openbaarheid het niet haalt op de bescherming van belangen zoals, in het bijzonder, de veiligheid van de bevolking, de openbare orde, de nationale veiligheid of 's lands defensie.

In 1997, na een onderzoek te hebben gevoerd naar de toepassing van deze bepalingen, kwam het Comité I tot het besluit dat de mogelijkheid van directe toegang van een particulier tot zijn individueel dossier bij een inlichtingendienst alleen in theorie bestond. Het Comité I vond dat wanneer iemand gewag maakte van een vermoedelijk materieel of moreel nadeel in verband met de gegevens over zijn persoon in een dossier van de inlichtingendiensten, hij onder bepaalde voorwaarden maar algemener dan vandaag het recht moest kunnen krijgen om deze documenten te raadplegen. Volgens het Comité I mag de beslissing om deze toegang goed te keuren of te weigeren niet alleen worden overgelaten aan het oordeel van de inlichtingendiensten.

In verband hiermee formuleerde het Comité I de aanbeveling om een procedure en voorwaarden van toegang te definiëren op grond van de Zwitserse en de Franse wetgeving. In deze landen bestaat er een « Adviescommissie inzake het geheim van landsverdediging ». Een collegiaal orgaan, zoals de Commissie voor de bescherming van de persoonlijke levenssfeer of het Comité I, in overleg met de bevoegde minister, zou kunnen vaststellen dat het meedelen van bepaalde gegevens de staatsveiligheid, de verdediging van het land en de openbare veiligheid niet in het gedrang brengt en dat er dus reden zou zijn om ze volledig of gedeeltelijk aan de aanvrager te bezorgen.

Sommige gegevens zouden echter nooit mogen worden meegedeeld, in het bijzonder : de naam van de leden van de inlichtingendiensten belast met het verzamelen en verwerken van persoonsgegevens, de naam van de personen die te goeder trouw gegevens aan de inlichtingendiensten hebben bezorgd, gegevens betreffende het privé-leven van derden, gegevens ingewonnen in het kader van een lopende gerechtelijke procedure, gegevens verstrekt door een vreemde inlichtingen- of veiligheidsdienst.

Wanneer redenen met betrekking tot de veiligheid van de Staat, de verdediging van het land en de openbare veiligheid verhinderen dat informatie wordt

contrôle se bornerait à informer le requérant qu'il a été procédé aux vérifications nécessaires.

— « Il serait également souhaitable que tous les litiges relatifs au pouvoir des services de sécurité d'interdire la divulgation d'informations fassent l'objet d'un contrôle judiciaire. » (1)

Commentaire :

Le Comité R estime que la classification des documents et informations secrets doit être réglé par la loi. En Belgique, la question vient d'être réglée par une loi du 11 décembre 1998.

Le Comité R est d'avis pour sa part que le pouvoir exécutif ne peut jamais être laissé seul juge d'une obligation de secret. Le Comité R estime aussi qu'une obligation de secret ne peut en aucun cas nuire au libre exercice des droits de la défense en justice.

Le Comité R a donc recommandé que le contrôle de l'obligation de secret soit confiée à une ou plusieurs instances indépendantes composées notamment, mais non exclusivement, de magistrats et dont les membres seraient titulaires d'une habilitation de sécurité.

Trois instances indépendantes existent en Belgique qui, chacune dans son domaine, pourraient exercer cette fonction, moyennant une adaptation de leurs compétences respectives :

— la Commission de protection de la vie privée, dans le cas où l'obligation de secret aurait pour motif de protéger cet intérêt;

— la Commission d'accès aux documents administratifs pour les documents de l'administration en général;

— le Comité permanent de contrôle des services de renseignements pour les documents de ces services (2).

(1) Traduction libre.

(2) Voir article 4 de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs (*Moniteur belge* du 12 septembre 1991).

bekendgemaakt, zou het toezichtsorgaan zich ertoe beperken aan de verzoeker te melden dat de vereiste controle is verricht.

— « Voorts zou het wenselijk zijn dat alle geschillen over de bevoegdheid van de veiligheidsdiensten om de verspreiding van gegevens te verbieden het voorwerp zouden zijn van een gerechtelijke controle. » (1)

Commentaar :

Het Comité I is van mening dat de classificatie van geheime documenten en informatie bij wet moet worden geregeld. In België is deze materie geregeld in een wet van 11 december 1998.

Anderzijds meent het Comité I dat de uitvoerende macht nooit als enige zou mogen beslissen over een verplichting tot geheimhouding. Voorts vindt het Comité I dat een verplichting tot geheimhouding in geen geval nadelig mag zijn voor de vrije uitoefening van de rechten van de verdediging in rechte.

Daarom formuleerde het Comité I de aanbeveling dat het toezicht op de verplichting tot geheimhouding wordt toevertrouwd aan een of meer onafhankelijke instanties waartoe in het bijzonder, maar niet uitsluitend, magistraten behoren en waarvan de leden houder zijn van een veiligheidsmachtiging.

In België bestaan er drie onafhankelijke instanties die, elk op haar gebied, deze functie zouden kunnen uitoefenen, op voorwaarde dat hun respectievelijke bevoegdheden worden aangepast :

— de Commissie voor de bescherming van de persoonlijke levenssfeer, indien de verplichting tot geheimhouding tot doel zou hebben dit belang te beschermen;

— de Commissie voor toegang tot bestuurlijke documenten, indien het gaat om documenten van de administratie in het algemeen;

— het Vast Comité van toezicht op de inlichtingendiensten, indien het gaat om documenten van deze diensten (2).

(1) Vrije vertaling.

(2) Zie artikel 4 van de wet d.d. 29 juli 1991 betreffende de uitdrukkelijke motivering van de bestuurshandelingen (*Belgisch Staatsblad* van 12 september 1991).

TITRE III

CONTACTS DU COMITÉ

CHAPITRE 1

Assises nationales du Haut Comité français pour la Défense civile

Le Comité R a été invité à participer aux assises nationales du Haut Comité français pour la Défense civile, qui se sont tenues à Marseille les 3 et 4 novembre 1999 en présence de délégations en provenance d'Argentine, du Brésil, du Chili, de Colombie, des États-Unis d'Amérique, du Mexique, de Pologne et du Vénézuela.

Le Haut Comité français pour la Défense civile se définit lui-même comme «une association loi 1901 (ndr: l'équivalent d'une ASBL en Belgique) qui, de manière indépendante, en partenariat avec l'ensemble des acteurs concernés, participe à la réflexion sur la doctrine, l'organisation et les techniques en matière de défense et de sécurité civiles».

Le Haut Comité a été fondé en 1981 et fût longtemps présidé par Maurice Schumann.

Le principe moteur de son activité est à rechercher, notamment, aux paragraphes 1 et 2 de la loi française nº 87-565 du 22 juillet 1987 relative à l'organisation de la sécurité civile, à la protection de la forêt contre l'incendie et à la prévention des risques majeurs (*Journal officiel* 23 juillet 1987 et rect. 29 août 1987) qui énoncent:

«Les citoyens ont un droit à l'information sur les risques majeurs auxquels ils sont soumis dans certaines zones du territoire et sur les mesures de sauvegarde qui les concernent.»

«Ce droit s'applique aux risques technologiques et aux risques naturels prévisibles.»

Deux membres du Comité R se sont rendus à cette invitation dont le programme, riche en thèmes directement transposables dans la réalité belge, rencontrait nombre de préoccupations d'actualité du Comité R en matière de contrôle des services de renseignement et de sécurité.

Parmi celles-ci, deux sont prioritaires aux yeux du Comité R: la manière dont la Sûreté de l'État met en œuvre les nouvelles missions lui dévolues, relatives à

TITEL III

CONTACTEN VAN HET COMITÉ I

HOOFDSTUK 1

«Assises nationales du Haut Comité français pour la Défense civile»

Het Comité I ontving een uitnodiging om deel te nemen aan het «Assises nationales du Haut Comité français pour la Défense civile» (1). Dit congres vond plaats op 3 en 4 november 1999 in Marseille en werd bijgewoond door delegaties afkomstig uit Argentinië, Brazilië, Chili, Colombia, de Verenigde Staten van Amerika, Mexico, Polen en Venezuela.

Het «Haut Comité français pour la Défense civile» omschrijft zichzelf als «een vereniging volgens de wet van 1901 (n.v.d.r.: het equivalent van een VZW in België) die autonoom, samen met alle betrokken actoren, deelneemt aan het denkproces over de doctrine, de organisatie en de technieken inzake civiele verdediging en veiligheid».

Het Hoog Comité is opgericht in 1981 en werd gedurende lange tijd voorgezeten door Maurice Schumann.

Het beginsel dat de stuwende kracht vormt van de activiteiten van dit Comité vinden we terug in de paragrafen 1 en 2 van de Franse wet nr. 87-565 d.d. 22 juli 1987 betreffende de organisatie van de civiele veiligheid, de bescherming van het woud tegen het vuur en het voorkomen van grote risico's (*Journal Officiel* 23 juli 1987 [sic] en verbeterd 29 augustus 1987). Deze paragrafen luiden als volgt:

«De burgers genieten een recht van informatie over de grote risico's waaraan ze in sommige delen van het grondgebied worden blootgesteld en over de beschermingsmaatregelen die op hen betrekking hebben.»

«Dit recht is van toepassing op technologische risico's en op voorzienbare natuurlijke risico's.»

Twee leden van het Comité I zijn op deze uitnodiging ingegaan. Op het programma van het congres stonden diverse thema's die rechtstreeks naar de Belgische realiteit kunnen worden overgezet. Voorts werden verschillende zaken behandeld waaraan het Comité I momenteel aandacht besteedt in het kader van het toezicht op de inlichtingen- en veiligheidsdiensten.

Twee van deze thema's krijgen van het Comité I absolute voorrang: de manier waarop de Veiligheid van de Staat de nieuwe opdrachten die haar zijn toe-

(1) Vrije vertaling: Franse Hoog Comité voor civile verdediging.

la lutte contre les organisations criminelles et à la sauvegarde des éléments essentiels du potentiel scientifique ou économique (articles 7 et 8 de la loi du 18 décembre 1998), de même que la manière dont le Service général du renseignement et de la sécurité s'acquitte de ses missions propres, notamment dans le cadre de la recherche et de l'analyse du renseignement relatif à « toute manifestation de l'intention de, par des moyens de nature militaire, porter atteinte à la protection ou à la survie de la population, au patrimoine national ou au potentiel économique du pays » (articles 10 et 11 de la loi du 18 décembre 1998).

On épinglera au passage, sans minimiser pour autant l'intérêt des autres exposés, les analyses de M. Xavier Raufer, criminologue, directeur des études et de la recherche du Centre universitaire de recherche sur les menaces criminelles contemporaines (Université Panthéon-Assas, Paris II), de Mme Irène Stoller, premier substitut du procureur de Paris, responsable de la section A6, en charge des affaires de terrorisme, ou encore de M. Steven Goodwin en matière de programme américain de contre-terrorisme NBC et de protection des infrastructures critiques.

Les membres du Comité R ont, entre autres, activement participé au séminaire consacré à ces mêmes infrastructures critiques, qu'il s'agisse de sites et réseaux physiques à caractère vital (réseau de distribution d'eau alimentaire, par exemple) ou encore de sites et réseaux informatiques, dont la vulnérabilité structurelle fait de plus en plus régulièrement la « une » des médias.

On peut résumer très succinctement le contenu de ces assises sous la forme d'un constat quasi-universel : les sociétés développées, c'est-à-dire industrialisées, urbaines, pratiquant à outrance la spécialisation des tâches, totalement dépendantes de leur approvisionnement en énergie et de leurs technologies pointues nécessitant toujours davantage d'intelligence artificielle, deviennent de plus en plus vulnérables au fur et à mesure de leur développement qui multiplie à l'infini les points faibles, ceux-là précisément que visent les terrorismes ou la criminalité organisée.

Qu'il s'agisse de cibler une gare ferroviaire de triage abritant quotidiennement des tonnes de solides et/ou liquides explosibles et/ou toxiques, dont les caractéristiques s'exposent de surcroît en rouge ou orange sur des conteneurs aisément accessibles; un « zoning scientifique » recelant des agents bactériologiques et/ou chimiques dangereux; une centrale atomique et ses

gekend uitoefent en die te maken hebben met de strijd tegen criminele organisaties en het beschermen van essentiële elementen van het wetenschappelijk of economisch potentieel (artikelen 7 en 8 van de wet d.d. 18 december 1998), alsmede de wijze waarop de Algemene Dienst Inlichting en Veiligheid zijn eigen opdrachten vervult, vooral op het gebied van het inwinnen en analyseren van inlichtingen met betrekking tot « eender welke uiting van het voornemen om, met middelen van militaire aard, afbreuk te doen aan de bescherming of het voortbestaan van de bevolking, het nationaal patrimonium of het economisch potentieel van het land » (artikelen 10 en 11 van de wet d.d. 18 december 1998).

Zonder daarom het belang van de overige exposés te willen minimaliseren, verwijzen we vooral naar de uiteenzettingen van de heer Xavier Raufer, criminoloog, directeur studies en onderzoek van het Universitair onderzoekscentrum inzake hedendaagse criminele bedreigingen (1) (Université Panthéon-Assas, Parijs II), van mevrouw Irène Stoller, eerste substituut van de procureur van Parijs, hoofd van de sectie A6 en belast met alle zaken die met terrorisme verband houden, of van de heer Steven Goodwin met betrekking tot het Amerikaans programma voor terrorismebestrijding NBC en voor de bescherming van belangrijke infrastructuur.

De leden van het Comité I hebben onder meer actief deelgenomen aan het seminarie over deze kwetsbare infrastructuur, die niet alleen essentiële fysieke sites en netwerken omvat (bijvoorbeeld waterleidingsnet) maar ook computersites en -netwerken die door hun structurele kwetsbaarheid steeds vaker de voorpagina halen.

We kunnen de inhoud van dit congres heel beknopt samenvatten in een zo goed als universele vaststelling : ontwikkelde, dit is geïndustrialiseerde, stedelijke samenlevingen die de specialisatie van de taken tot het uiterste doordrijven en volkomen afhankelijk zijn van hun bevoorrading in energie en van hun spitstechnologie, die in toenemende mate kunstmatige intelligentie vereist, worden steeds kwetsbaarder naargelang ze zich ontwikkelen en ze hun zwakke punten tot in het oneindige vermenigvuldigen; precies deze zwakke punten vormen het doelwit van terroristen of van de georganiseerde misdaad.

Ongeacht of het doelwit een rangeerstation is waar dagelijks tonnen ontplofbare en/of giftige vaste en vloeibare stoffen passeren, waarvan de kenmerken bovendien in het rood of oranje zijn aangeduid op gemakkelijk toegankelijke containers; een « wetenschappelijke zone » waar gevaarlijke bacteriologische en/of chemische stoffen worden opgeslagen; een

(1) Vrije vertaling van : *« Centre universitaire de recherche sur les menaces criminelles contemporaines »*

installations périphériques généralement moins sécurisées; une infrastructure routière, ferroviaire, fluviale ou portuaire de communications, ou encore un réseau de radio-télé communications, y compris informatique, etc. le terroriste potentiel et/ou le maître-chanteur organisé ne sont obligés de faire preuve ni d'imagination, ni d'audace, ni de savoir-faire technologique pour multiplier les dégâts matériels, financiers, économico-sociaux, écologiques, psychologiques, politiques etc.

L'intérêt de ces assises a consisté dans la stimulation de la réflexion en matière de sécurité, composante indissociable de la mission des services de renseignement.

Le principe de précaution si souvent évoqué ces derniers temps trouve ici amplement matière à s'appliquer. De ce principe découlent naturellement la projection des risques, leur évaluation, l'élaboration de la riposte et la planification de la mise en œuvre. C'est à ce dernier niveau qu'intervient la nécessité d'intégration, ou à tout le moins de coordination, des différents services publics concernés, y compris de renseignement, sans laquelle le chaos a toutes chances de s'installer une fois l'incident critique survenu, ce qui en amplifie généralement les conséquences dommageables.

Les services de renseignement et de sécurité belges sont par définition, tout comme leurs homologues étrangers, en première ligne, sinon aux avant-postes, face aux multiples menaces potentielles ressortissant de leur compétence.

Il leur incombe, dans la mesure des moyens qui leur sont donnés, de remplir efficacement les missions à haute responsabilité que le législateur leur a confiées au nom de la nation. À son niveau d'intervention, le Comité R n'aura de cesse de vérifier que la coopération mutuelle, légalement organisée (articles 9, 11, 4º, § 3, 14, deuxième alinéa, 16 et 20 de la loi du 18 décembre 1998) entre ces services et d'autres, soit assurée de manière aussi efficace que possible.

CHAPITRE 2

11e Salon international de la sécurité intérieure des États — Milipol

Le Comité R a reçu une invitation de M. Guillaume Dasquie, rédacteur en chef du bimensuel *Le Monde du Renseignement*, à se rendre à Paris, au onzième salon de la Sécurité intérieure des États, qui s'est tenu dans le Parc d'Expositions du Bourget, du 23 au 26 novembre 1999 et réunissait pas moins de 450 exposants spécialisés, de toutes origines nationales.

kerncentrale en de perifere installaties die gewoonlijk minder beveiligd zijn; een wegennet, spoor-, rivier- of haveninfrastructuur of een radio- en televisienetwerk inclusief informatica enzovoort, een georganiseerd kandidaat-terrorist of afperser moet niet van veel verbeelding, lef of technologische kennis blijk geven om enorme materiële, financiële, economisch-sociale, ecologische, psychologische, politieke ... schade aan te richten.

Dit congres was vooral belangrijk omdat het de deelnemers ertoe heeft aangezet na te denken over het aspect «veiligheid», dat een wezenlijk bestanddeel vormt van de opdracht van de diensten en onlosmakelijk verbonden is met hun taak inzake inlichtingen.

Het beginsel van voorzorg, dat de laatste tijd zo vaak wordt aangehaald, is hier volledig op zijn plaats. Het heeft heel natuurlijk tot gevolg dat de bevoegde diensten de risico's gaan vaststellen en evalueren, een reactie uitwerken en de tenuitvoerlegging daarvan plannen. In deze laatste fase wordt duidelijk dat het noodzakelijk is de diverse betrokken openbare diensten, met inbegrip van de inlichtingendiensten, te integreren of ten minste te coördineren. Bij gebrek aan dergelijke integratie of coördinatie is de kans immers groot dat er chaos ontstaat nadat het kritisch incident zich heeft voorgedaan, waardoor de schadelijke gevolgen gewoonlijk groter worden.

De Belgische inlichtingen- en veiligheidsdiensten bevinden zich per definitie, net als hun tegenhangers in het buitenland, op de frontlijn of zelfs in een vooruitgeschoven positie tegenover de vele potentiële bedreigingen die voortvloeien uit hun bevoegdheid.

Met de middelen die hun worden toegewezen, moeten ze de uiterst belangrijke opdrachten die de wetgever hun in naam van de natie heeft toevertrouwd doeltreffend vervullen. Op zijn niveau moet het Comité I er voortdurend op toezien dat de wettelijk georganiseerde onderlinge samenwerking (artikelen 9, 11, 4º, § 3, 14, lid 2, 16 en 20 van de wet d.d. 18 december 1998) tussen deze en andere diensten zo doeltreffend mogelijk verloopt.

HOOFDSTUK 2

11e Internationale Beurs over de inwendige veiligheid van Staten — «Milipol»

Het Comité I ontving een uitnodiging van de heer Guillaume Dasquie, hoofdredacteur van het halfmaandelijks tijdschrift *«Le Monde du Renseignement»*, om een bezoek te brengen aan de 11de beurs over de inwendige veiligheid van Staten die plaatsvond in het tentoonstellingspark van Le Bourget van 23 tot 26 november 1999. Aan de beurs namen niet minder dan 450 gespecialiseerde exposanten van overal ter wereld deel.

Encore imprégné du contenu technique de son rapport d'activités 1999 relatif au système planétaire d'interception de communications baptisé « Échelon », dont l'existence a depuis lors été admise par ses utilisateurs, le Comité R se devait de se pencher également sur les possibilités matérielles d'écoutes individuelles secrètes susceptible d'être mises en œuvre en violation des lois belges en vigueur.

Un membre du Comité R et le chef du Service d'enquêtes du Comité R ont donc fait l'aller-retour le 25 novembre 1999 avec l'intention d'y constater en personne, de visu, la réalité de l'existence — et des performances — de matériels de prise de vues, d'écoutes radio-téléphoniques de toutes natures ainsi que de piratage informatique.

La grande foule, affairée, à l'évidence composée de professionnels de la sécurité, très cosmopolite, qui se pressait en délégation souvent nombreuse à ce salon « Milipol », faisant l'objet aux entrées du hall comme à l'abord de certains stands sensibles d'une vérification électronique poussée d'accréditation, était d'emblée révélatrice de l'intérêt que nombres d'états et organismes concernés accordent aux technologies de pointe en matière de sécurité policière et militaire.

Le Comité R a pu constater, la sophistication ou la miniaturisation de certains matériels comme par exemple cet ensemble caméra-micro restituant, « à distance de sécurité suffisante », un son et une image de qualité, alors qu'il se trouve dissimulé dans une vis « domestique » de dimension usuelle, fixée à un endroit banal où elle n'attire pas l'attention, dont le logement de la caméra accepterait au mieux le passage d'un cure-dents. Ou encore cet accessoire électronique ultra-plat, destiné à être glissé sans difficulté à l'intérieur du boîtier d'un clavier d'ordinateur, afin d'y enregistrer chaque frappe, permettant ainsi de reconstituer ultérieurement le texte, à l'image de ce que permettaient précédemment les rubans encreurs. Ou encore tout le matériel d'émission, d'enregistrement, de poursuite électronique, de balises, de radiogoniométrie, de brouillage d'émissions radio ou de téléphones cellulaires et d'interceptions téléphoniques tous standards, disponible à des prix non dissuasifs.

Ce qui ne signifie pas qu'il ne faille « montrer patte blanche » au moment de l'acquisition ...

Il serait inopportun de passer en revue, dans le cadre du présent rapport, l'ensemble des techniques

Nog volledig doordrongen van de technische inhoud van zijn activiteitenverslag 1999 over het wereldomvattend systeem voor het intercepteren van communicatie, Echelon genoemd, waarvan de gebruikers het bestaan inmiddels hebben toegegeven, kon het Comité I niet anders dan ook aandacht besteden aan de materiële mogelijkheden voor geheime individuele afluisteroperaties. Dergelijke operaties kunnen technisch worden uitgevoerd en zijn, in de veronderstelling dat dit gebeurt, volkomen strijdig met de bestaande Belgische wetgeving.

Een lid van het Comité I en het hoofd van de Dienst enquêtes van het Comité I hebben de beurs bezocht op 25 november 1999 om er met eigen ogen vast te stellen of er enige waarheid schuilt in de vele beweringen over het bestaan — en de hoge prestaties — van toestellen om beeldopnames te maken, radiotelefonische communicatie van eender welke aard af te luisteren en computers te kraken.

De bezoekers, die heel bedrijvig en vanzelfsprekend professionelen inzake veiligheid waren, kwamen van overal ter wereld en begaven zich in vaak omvangrijke delegaties naar deze Milipol-beurs, waar ze, niet alleen aan de ingang maar ook bij sommige gevoelige stands, aan een grondige (elektronische) controle werden onderworpen. Het grote aantal bezoekers maakte al onmiddellijk duidelijk hoeveel belang een groot aantal betrokken staten en organismen hechten aan spitstechnologie op het gebied van politiële en militaire veiligheid.

Het Comité I heeft de technische perfectie of de uiterst minieme afmetingen van bepaalde toestellen kunnen vaststellen. Zo was er een toestelletje dat een camera en een micro combineerde en van op « voldoende veilige afstand » geluid en beeld van grote kwaliteit leverde, terwijl het verborgen zat in een gewone schroef van normale grootte die je in elk huis vindt en die wordt bevestigd op een plek waar hij niet opvalt; de voorziene ruimte voor de camera is nauwelijks groot genoeg voor een tandenstoker. Het Comité I zag ook een ultraplat elektronisch accessoire dat zonder enig probleem in het plastic omhulsel van een computerklavier wordt ingebracht en vervolgens elke aanslag registreert. Op die manier kan men later de tekst opnieuw samenstellen zoals vroeger gebeurde met inktlinten. En verder vond je op de beurs alle mogelijke toestellen voor het uitzenden, registreren, elektronisch achtervolgen, radiobakens, radiopeiling, het verstoren van radio-uitzendingen of draadloze telefoons en voor het intercepteren van alle vormen van telefoongesprekken, tegen prijzen die zeker niet afschrikken.

Dit betekent natuurlijk niet dat men op het ogenblik van de aankoop niet het wachtwoord moet geven ...

In het kader van het onderhavige rapport past het niet alle tentoongestelde technologieën te bespreken

proposées en relation avec l'interception secrète ou illicite d'informations, dont un dossier à toutefois été constitué.

Cependant le Comité R ne manquera pas d'approfondir sa connaissance du domaine des technologies dont l'exploitation à des fins abusives ou illicites serait de nature à compromettre les droits que la Constitution et les lois accordent aux citoyens ou encore à menacer le potentiel scientifique ou économique du pays.

CHAPITRE 3

Haut Comité français pour la Défense civile — «les proliférations»

Le Comité R a été associé à une «rencontre» organisée le 20 janvier 2000 au Palais du Luxembourg à l'initiative de M. Paul Girod, vice-président du Sénat de France, dont le thème était entièrement consacré aux «proliférations» (nucléaire, chimique, bactériologique ainsi qu'aux raisons et moyens de les limiter ou de les contrer.

S'agissant là de l'un des domaines traditionnels d'activité des services de renseignement, le Comité R a dépêché à Paris l'un de ses membres pour participer à cette réunion.

Ce fut également l'occasion d'y rencontrer brièvement un des élus français actuellement en charge d'une mission de réflexion collective sur l'opportunité de doter la République française d'un organe parlementaire externe de contrôle des services de renseignement.

Durant les deux heures de l'exposé et de l'entretien qui s'en est suivi, ont été notamment évoquées les circonstances de l'attentat au gaz sarin dans le métro de Tokyo et certaines modalités d'un programme militaire étranger d'armement nucléaire, bactériologique et chimique, surtout en guise d'illustration du processus coûteux, lent et semé d'embûches que constitue l'acquisition à l'étranger de technologies aussi potentiellement dévastatrices que malaisées à maîtriser.

La réflexion s'est ensuite naturellement orientée vers la nécessité d'un contrôle mondial crédible des flux de matières, composés chimiques, substances radiologiques, etc., susceptibles d'entrer dans la composition d'armes de destruction massive. Les options débattues en matière de limitation de la prolifération au sein de la communauté internationale ont été abordées et l'on a été surpris d'apprendre l'impact moral que les opinions publiques, nationale ou internationale, ont pu avoir en certaines circonstances sur

die te maken hebben met het geheim of onwettig intercepteren van informatie en waarover reeds een dossier werd aangelegd.

Het Comité I zal nochtans niet nalaten zijn kennis uit te diepen inzake technologieën waarvan de exploitatie met bedrieglijke of onwettige doeleinden schade kan toebrengen aan de rechten die de Grondwet en de wetten aan de burgers toekennen of een bedreiging kan vormen voor 's lands wetenschappelijk of economisch potentieel.

HOOFDSTUK 3

«Haut Comité français pour la Défense civile» — «de proliferaties»

Het Comité I heeft deelgenomen aan een bijeenkomst, die op 20 januari 2000 plaatsvond in het «Palais du Luxembourg» op initiatief van de heer Paul Girod, ondervoorzitter van de Franse senaat. De vergadering was volledig gewijd aan alle vormen van proliferatie (nucleair, chemisch, bacteriologisch), alsmede aan de redenen en de middelen om ze te beperken of te bestrijden.

Aangezien het om een van de traditionele actieterreinen van de inlichtingendiensten ging, stuurde het Comité I een van zijn leden naar Parijs om aan deze vergadering deel te nemen.

Het was tevens een geschikte gelegenheid om er, zij het zeer beknopt, één van de Franse volksvertegenwoordigers te ontmoeten die momenteel belast zijn met de opdracht om samen te onderzoeken of het al dan niet gepast lijkt in de Franse Republiek een extern parlementair organisme van toezicht op de inlichtingendiensten op te richten.

Tijdens de uiteenzetting van twee uur en in het onderhoud dat erop volgde, werd onder meer gesproken over de omstandigheden van de aanslag met sarin in de metro van Tokio en over bepaalde aspecten van een buitenlands militair programma voor nucleaire, bacteriologische en chemische bewapening. Aan de hand van deze voorbeelden werd vooral aangetoond dat het aankopen in het buitenland van potentieel verwoestende en moeilijk beheersbare procédés een bijzonder dure operatie is die traag verloopt en waarbij heel wat obstakels moeten worden overwonnen.

Vervolgens onderzochten de deelnemers de noodzaak om wereldwijd op geloofwaardige wijze toezicht te houden op de stromen grondstoffen, chemische verbindingen, radiologische stoffen enzovoort, die kunnen worden gebruikt bij de productie van massa-vernietigingswapens. Ze bespraken ook de opties inzake het beperken van de proliferatie binnen de internationale gemeenschap. We vernamen met verbazing dat niet democratisch verkozen leiders, die zich door het avontuur van de proliferatie hadden

des dirigeants non démocratiquement installés, tentés par l'aventure de la prolifération.

M. Claude Éon, chargé de mission auprès du directeur des relations internationales de la Délégation générale pour l'armement (DGA) et vice-président du collège des experts du Haut Comité français pour la Défense civile, a soumis à l'assistance une analyse nuancée de la situation tendant à relativiser la réalité de la menace d'acquisition par des «états-voyous», ou des groupements terroristes d'envergure, de systèmes d'arme de destruction massive véritablement opérationnels, en raison d'impératifs financiers et technologiques.

Au-delà des risques d'une prolifération sans doute ramenée à de plus justes proportions, il a néanmoins rappelé l'existence incontournable des risques déjà installés.

Le débat s'est achevé sur l'évocation du rôle majeur que jouent les services mondiaux de renseignement sur l'échiquier de la prolifération.

laten verleiden, in bepaalde omstandigheden rekening hadden gehouden met de publieke opinie, nationaal en internationaal.

De heer Claude Éon, opdrachthouder bij de directeur internationale betrekkingen van de algemene delegatie voor de bewapening(1) en ondervoorzitter van het College van deskundigen van het «Haut Comité français pour la Défense civile», legde aan de aanwezigen een genuanceerde analyse van de toestand voor. Daarin streeft hij ernaar de realiteit te relativeren van de dreiging dat staten met slechte bedoelingen of grote terroristische organisaties massavernietigingswapens aankopen die werkelijk operationeel zijn, rekening houdend met financiële en technologische imperatieven.

Ook al brengt hij de risico's van een proliferatie wellicht tot juistere verhoudingen terug, toch wijst hij op het onvermijdelijk bestaan van de reeds geïnstalleerde risico's.

Het debat werd afgesloten met een korte gedachtenwisseling over de belangrijke rol die de inlichtingendiensten overal ter wereld spelen op het schaakbord van de proliferatie.

(1) Vrije vertaling van *«Délégation générale pour l'armement»* (DGA)

57.708 — E. Guyot, s. a., Bruxelles