2-867/1 (Senaat)
DOC 50 **1434/001 (Kamer)**

Belgische Senaat en Kamer van volksvertegenwoordigers

ZITTING 2001-2002

10 OKTOBER 2001

Activiteitenverslag 2000 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 HEREN
COVELIERS (K) EN **VANDENBERGHE** (S)

(1) Samenstelling van de commissie:
Voorzitters:

A. Senaat:

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

B. Kamer van volksvertegenwoordigers:

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

2-867/1 (Sénat)
DOC 50 **1434/001 (Chambre)**

Sénat et Chambre des représentants de Belgique

SESSION DE 2001-2002

10 OCTOBRE 2001

Rapport d'activité 2000 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 MM.
COVELIERS (Ch) ET **VANDENBERGHE** (S)

(1) Composition de la commission:
Présidents:

A. Sénat:

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

B. Chambre des représentants:

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

De begeleidingscommissies van de Senaat en de Kamer van volksvertegenwoordigers hebben het activiteitenverslag 2000 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (Comité I) besproken tijdens hun vergaderingen van 18 april, 21 mei en 1 juni 2001.

1. Inleidende uiteenzetting door de voorzitter van het Comité

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, meldt dat het Comité I op vraag van de begeleidingscommissies van Kamer en Senaat blijvend aandacht heeft gehad voor de vragen die zijn gerezen na het toezichtsonderzoek over de manier waarop de inlichtingendiensten de zaak «Echelon» hebben gevolgd. Het Comité I zal op dezelfde manier verder werken en zal de begeleidingscommissies op de hoogte brengen als er nieuwe elementen opduiken.

Deze problematiek hangt nauw samen met de verdediging van het economische potentieel van het land tegen eventuele bedreigingen. Tijdens het voorbije jaar heeft het Comité I daaraan dan ook veel aandacht besteed. Het Comité heeft in de praktijk gecontroleerd hoe de Belgische inlichtingendiensten de opdrachten uitvoeren die de wet houdende regeling van de inlichtingen- en veiligheidsdienst hen geeft.

Dit onderwerp is niet louter in het algemeen behandeld maar ook naar aanleiding van een bijzonder onderzoek naar een Belgisch onderzoekcentrum.

Er moet worden benadrukt dat de minister van Justitie heeft voorgesteld het deel van het algemeen verslag van het Comité I dat het economisch potentieel behandelt, over te zenden aan de eerste minister opdat het Ministerieel Comité voor inlichting rekening kan houden met de inhoud ervan.

Het bijzonder onderzoek naar een Belgisch onderzoekcentrum heeft in de eerste plaats aangetoond dat dergelijke gevallen zich ook in ons land kunnen voordoen.

Het toont ook aan dat er niet alleen een dreiging uitgaat van een algemeen systeem voor het onderscheppen van informatie — hoe het ook wordt genoemd — maar dat in België gevestigde bedrijven ook het slachtoffer kunnen worden van doelgerichte aanvallen die voornamelijk om economische en commerciële redenen worden uitgevoerd.

Een van de nieuwe opdrachten van de Veiligheid van de Staat is de bescherming van het wetenschappe-

Les commissions de suivi du Sénat et de la Chambre des représentants ont examiné le rapport d'activité 2000 du Comité permanent de contrôle des services de renseignements et de sécurité (Comité R) au cours de leurs réunions des 18 avril, 21 mai et 1er juin 2001.

1. Exposé introductif du président du Comité R

M. Jean-Claude Delepière, président du Comité permanent R, stipule que les questions soulevées par l'enquête de contrôle concernant la manière dont les services de renseignements avaient suivi le problème «Echelon» ont continué à retenir l'attention du Comité R, comme les commissions de suivi de la Chambre et du Sénat le lui avaient d'ailleurs demandé. Il poursuivra dans ce sens et informera les commissions de suivi si des éléments nouveaux importants devaient être mis en lumière.

Cette problématique étant étroitement liée à celle de la défense du potentiel économique du pays contre d'éventuelles menaces, le Comité R a notamment concentré davantage sa réflexion, au cours de l'exercice écoulé, sur ce dernier sujet, abordant de cette manière dans la pratique le contrôle sur la façon dont les services de renseignements belges accomplissent les missions qui leur ont été confiées par la loi organique des services de renseignements et de sécurité.

Ce sujet a ainsi été abordé non seulement d'une manière générale, mais également à l'occasion d'une enquête particulière concernant un centre belge de recherche.

En ce qui concerne d'une part le rapport général du Comité R concernant le potentiel économique, il convient de souligner que le ministre de la Justice a proposé de le transmettre au premier ministre afin que le Comité ministériel du renseignement tienne compte de son contenu.

En ce qui concerne d'autre part l'enquête particulière concernant un centre belge de recherche, celle-ci met d'abord en évidence que de tels cas ne sont pas que théoriques et qu'ils touchent également notre pays.

Le cas d'espèce démontre également qu'il ne faut pas uniquement craindre les menaces d'un système global d'interception, quel que soit par ailleurs son nom de code, mais qu'il y a lieu également de prendre conscience de la réalité des attaques ciblées dont peuvent être victimes — et principalement faut-il le souligner pour des raisons économiques et commerciales — des entreprises situées sur le territoire national.

Dans le domaine de l'identification des menaces, le cas du centre de recherche montre aussi qu'il a fallu

lijk of economisch potentieel van het land. Bij het identificeren van de bedreigingen heeft het geval van het onderzoekcentrum aangetoond dat de informatie niet noodzakelijk dankzij de toepassing van gestructureerde en duidelijke procedures terechtkomt bij de Veiligheid van de Staat.

Volgens de dienst zijn de operationele moeilijkheden waar hij momenteel mee kampt, te wijten aan een gebrek aan middelen en aan het uitblijven van duidelijke rechtlijnen van het Ministerieel Comité. Met de bestaande middelen is wel al een systeem ontwikkeld om met de betrokken bedrijven contact te hebben en hen bewust te maken van het probleem.

Zonder de toestand op het vlak van spionageactiviteiten te dramatiseren, zou de voorlopige conclusie kunnen zijn dat er op operationeel vlak — buiten het theoretische kader — soortgelijke gevallen zouden kunnen bestaan die onze inlichtingendiensten met hun huidige middelen niet kunnen opsporen.

Tijdens het onderzoek naar «Echelon» hebben de inlichtingendiensten toegegeven dat zij niet wisten of er in België gevallen bestonden die te vergelijken zijn met de gevallen in Frankrijk (namelijk Airbus en Thomson die markten verloren hadden).

De cyclus van de inlichtingen houdt in dat de informatie, eens dat ze wordt ingewonnen, dient te worden bewerkt en doorgegeven aan de bestemmelingen die elk op hun bevoegheidsdomein — zij het uitvoerend of gerechtelijk — de nodige beslissingen nemen. «*Regeren betekent voorbereid zijn*», en om voorbereid te zijn, dient men ingelicht te zijn.

In het geval van het onderzoekscentrum, dat het voorwerp was van vaststellingen door het Comité I, wordt geconstateerd dat de informatie vakkundig door agenten van de Veiligheid van de Staat werd behandeld maar is tevens aan het licht gekomen dat (geclassificeerde) rapporten, waarin de juiste vragen worden gesteld, geen enkel verder gevolg kenden.

De inlichtingencyclus werd dus binnen de Veiligheid van de Staat niet onderbroken maar evenmin verdergezet door rapportering van de nuttige gegevens naar externe bestemmelingen.

In het kader van hetzelfde onderzoek wordt bovendien vastgesteld dat de grenzen tussen de opdrachten van een zelfde dienst (verdediging van het economisch potentieel en contraspionage), evenals die tussen de specifieke opdrachten van beide diensten (Veiligheid van de Staat en Algemene Dienst inlichting en veiligheid), niet altijd duidelijk omlijnd zijn. Het concreet voorbeeld toont aan dat militaire en civiele belangen elkaar kunnen overlappen.

De verplichting tot de meest doelmatige samenwerking en gegevensuitwisseling tussen de diensten, even-

un concours de circonstances qui ne relève pas nécessairement de la mise en œuvre de procédures structurées et précises en la matière pour que l'information dans sa totalité arrive à la connaissance de la Sûreté de l'État dont une des missions légales est aujourd'hui de s'occuper de la défense du potentiel scientifique et économique du pays.

Le manque de moyens et l'attente des directives du Comité ministériel en la matière sont mis en avant par ce service pour expliquer les difficultés opérationnelles auxquelles il est confronté en l'espèce. Un dispositif a toutefois été mis en place avec les moyens actuels pour préparer le terrain au niveau des contacts et de la sensibilisation des entreprises concernées.

On serait donc tenté de conclure provisoirement qu'en dehors du cadre théorique et sur le plan opérationnel — sans dramatiser la situation dans ce domaine particulièrement sensible des activités d'espionnage — il pourrait exister d'autres cas de ce genre que nos services de renseignements ne peuvent pas détecter aujourd'hui faute de disposer des capacités nécessaires.

À l'occasion de l'enquête concernant «Echelon», ces derniers avaient d'ailleurs répondu qu'ils ignoraient si des cas semblables à ceux cités par les Français existaient en Belgique (à savoir les cas Airbus et Thomson qui avaient perdu des marchés).

Le cycle des renseignements implique qu'une fois recueillie, l'information doit être traitée et transmise aux destinataires qui prennent les décisions nécessaires, chacun dans leur domaine de compétence, qu'il soit exécutif ou judiciaire. «Gouverner signifie être préparé» et, pour être préparé, il faut être informé.

Dans le cas du centre de recherche qui a fait l'objet des constatations du Comité R, on a constaté que l'information était traitée de manière compétente par des agents de la Sûreté de l'État, mais il est apparu également qu'aucune suite n'avait été donnée à certains rapports (classifiés) dans lesquels on posait les bonnes questions.

Le cycle des renseignements n'a donc pas été interrompu au sein de la Sûreté de l'État, mais il n'a pas non plus été prolongé par des rapports communiquant les données utiles à ces destinataires extérieurs.

Dans le cadre de la même enquête, on a constaté en outre que la frontière entre les missions d'un même service (défense du potentiel économique et contre-espionnage), ainsi que la frontière entre les missions spécifiques des deux services (Sûreté de l'État et Service général du renseignement et de la sécurité) ne sont pas toujours clairement tracées. L'exemple concret montre que les intérêts militaires et civils peuvent se recouvrir.

De manière générale, il y a donc lieu de rappeler, d'une part, l'obligation de parvenir à une collabora-

als de mededeling aan andere overheden — die in dit geval blijkbaar achterwege bleef — moet dus op algemene wijze in herinnering gebracht worden.

Uit andere verslagen van onderzoeken in andere domeinen, bijvoorbeeld georganiseerde criminaliteit of contraspionage, blijkt dat deze uitwisseling en communicatie niet altijd even vlot verlopen of soms zelf totaal achterwege blijven.

De redenen die de diensten (en dan voornamelijk de Veiligheid van de Staat) aanhalen voor deze leemten, lijken erg « ad hoc » en ingegeven door de omstandigheden.

Het is dus erg moeilijk voor het Comité I om een overzicht te hebben van de samenwerking tussen de diensten en van de uitwisseling van informatie met andere diensten (overheid, politie, gerecht). Een dergelijk algemeen beeld is nochtans noodzakelijk om de efficiëntie van en de coördinatie tussen de diensten te beoordelen.

De toezichtsonderzoeken van concrete gevallen kunnen echter als basis dienen voor een dieper inzicht in de problemen die rijzen bij de samenwerking tussen diensten en bij de uitwisseling van de verwerkte informatie.

Hierop voortgaand stelt het Comité I zich bijvoorbeeld vragen over de mate waarin de « regel van de derde », ook genoemd « regel van de derde dienst », kan aanvaard worden. Die regel houdt in dat men inlichtingen, afkomstig van een andere dienst — het gaat dan vooral over gevoelige informatie afkomstig van buitenlandse inlichtingendiensten — niet verder verspreidt zonder de toestemming van de dienst van oorsprong.

Het Comité I erkent het belang van dit principe (elke inlichtingendienst die deze regel negeert, zet zichzelf trouwens buitenspel) maar stelt zich vragen — mede ingegeven door enkele concrete vaststellingen die terug zijn te vinden in het huidige verslag — over de grenzen van een dergelijke regel in verhouding met de verplichtingen die rusten op een nationale overheidsdienst, zij het een inlichtingendienst.

Wat houdt dit bijvoorbeeld in bij de toepassing van artikel 29 van het Wetboek van strafvordering ?

Komt het aan een inlichtingendienst toe om, op eigen initiatief of *a posteriori*, het ontbreken van kennisgeving aan gerechtelijke overheden te rechtvaardigen door, in toepassing van de « regel van de derde dienst », er van uit te gaan dat bepaalde feiten

tion et à un échange de données les plus efficaces possible entre les services, et, d'autre part, l'obligation de communiquer les données à d'autres autorités, ce qui, en l'espèce, a manifestement fait défaut.

D'autres rapports d'enquêtes relatifs à d'autres domaines comme celui de la criminalité organisée et du contre-espionnage montrent d'ailleurs qu'il existe dans la pratique des raisons de penser que cet échange et cette communication ne sont pas toujours les plus efficaces possibles quand ils ne sont pas tout bonnement inexistants.

Les explications avancées par les services (principalement la Sûreté de l'État) pour justifier certaines lacunes constatées dans ces domaines semblent résulter des circonstances et du « cas par cas ».

Il est donc aussi très difficile aujourd'hui pour le Comité R d'avoir une vue d'ensemble du phénomène de la coopération entre services et de celui de la communication des informations utiles à d'autres instances (administratives, politiques ou judiciaires) et de pouvoir apporter une appréciation globale sur ce qui peut être considéré comme des éléments essentiels de l'évaluation de l'efficacité et de la coordination des services.

Les enquêtes de contrôle portant sur des cas concrets permettent toutefois de servir de base à des réflexions qui se recoupent et cernent de plus près les problèmes liés notamment à la coopération entre services et à la communication des informations après traitement.

Partant de cela, le Comité R se pose par exemple des questions sur la mesure dans laquelle la « règle du tiers », qui est également appelée « règle du service tiers », peut être admise. Cette règle veut que les informations en provenance d'un autre service — il s'agit en l'espèce essentiellement d'informations sensibles provenant de services de renseignements étrangers — ne sont pas transmises à d'autres instances sans l'autorisation du service d'origine.

Le Comité R reconnaît l'importance de ce principe (en effet, tout service de renseignements qui méconnaîtrait cette règle se mettrait lui-même hors jeu), mais il se pose des questions — lesquelles sont fondées en partie sur des constatations concrètes qu'on retrouve dans le rapport actuel — sur les limites d'une telle règle eu égard aux obligations qui s'imposent à un service public national, fût-il un service de renseignements.

Par exemple, quelle sont les implications en ce qui concerne l'application de l'article 29 du Code d'instruction criminelle ?

Est-ce qu'un service de renseignements peut, d'initiative ou *a posteriori*, justifier l'absence de communication aux autorités judiciaires en considérant, dans le cadre de l'application de la « règle du service tiers », que certains faits ne constituent pas des

geen inbreuken betekenen of verder nog, dat de vastgestelde inbreuken reeds verjaard zijn?

In algemene zin kan men zich de vraag stellen of het aan een inlichtingendienst toekomt om te beoordelen dat — indien hij in het bezit is van materiaal of gegevens die verband houden met hangende gerechtelijke dossiers — deze van geen enkel belang zijn voor deze dossiers, en aldus het bestaan ervan zelfs niet meldt aan de gerechtelijke overheden?

Dit leidt dan ook tot de volgende vragen:

• op welk niveau worden deze opportuniteitsbeslissingen in een dergelijk geval genomen?

• volgens welke procedures?

• welk toezicht wordt er binnen de inlichtingendienst uitgeoefend op dergelijke beoordelingen?

Volgens artikel 20, § 3, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, bepaalt het Ministerieel Comité de in artikel 19, eerste lid, bedoelde voorwaarden waaronder de inlichtingen worden meegedeeld en de voorwaarden van de in § 1 van hetzelfde artikel 20 bedoelde samenwerking.

Als de voorwaarden bepaald zullen zijn, acht het Comité het noodzakelijk te kunnen beschikken over deze bepalingen om zijn controle uit te oefenen.

In hoofdstuk 3 van titel I van dit verslag wordt verwezen naar de nieuwe opdracht van het Comité als beroepsorgaan voor veiligsheidsmachtigingen. Daarnaast moet ook de nieuwe dimensie worden benadrukt inzake controle van de inlichtingendiensten, die vervat zit in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen.

Het belang van deze nieuwe dimensie kan worden aangetoond door het aantal keren dat beide thema's, samenwerking en mededeling, worden vermeld in het activiteitenverslag.

In het eerste geval moet bijvoorbeeld benadrukt worden dat het hoofd van de inlichtingendienst voor de eerste keer gebruikt heeft gemaakt van de procedure van verzet tegen de gerechtelijke inbeslagneming van geclassificeerde stukken door een onderzoeksrechter (artikel 38, § 2, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst).

Het Comité I blijft deze zaak volgen in het kader van zijn toezichtsbevoegdheid en zal rapporteren aan het Parlement.

In het tweede geval is het zo dat de inlichtingendiensten aan het Comité I geheime informatie hebben

infractions ou, mieux encore, que les infractions constatées sont déjà prescrites?

D'une manière générale, on peut se demander s'il appartient à un service de renseignements de juger que, s'il est en possession d'éléments ou d'informations relatifs à des affaires judiciaires en cours, ces éléments ou informations n'ont aucune importance pour les dossiers judiciaires en question, et donc même de s'abstenir d'en signaler l'existence aux autorités judiciaires.

L'on en vient dès lors aux questions suivantes:

• Dans ce genre de cas, à quel niveau y a-t-il lieu de prendre ces décisions d'opportunité?

• Suivant quelles procédures?

• Quel contrôle exerce-t-on au sein du service de renseignements sur ce genre d'appréciations?

La loi organique des services de renseignement et de sécurité du 30 novembre 1998 prévoit en son article 20, § 3, que c'est au Comité ministériel de définir les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du même article 20.

Lorsque ces conditions seront définies, le comité estime qu'il sera indispensable pour l'exercice de son contrôle qu'il puisse avoir connaissance de ces dispositions.

Enfin, outre la nouvelle mission du Comité R d'organe de recours en matière d'habilitations de sécurité à laquelle il est fait référence dans le chapitre 3 du titre 1er du présent rapport, il importe de mettre en évidence la dimension nouvelle apportée dans la matière du contrôle des services de renseignements par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

L'importance de cette dimension nouvelle peut être illustrée par les constatations reprises dans divers passages du présent rapport général d'activités relatifs aux deux thèmes dont il vient d'être question, à savoir la coopération et la communication.

Dans le premier cas, il faut souligner par exemple qu'il a été fait pour la première fois application par le chef d'un service de renseignement de la procédure d'opposition à une saisie judiciaire de documents classifiés par un juge d'instruction (article 38, § 2, de la loi du 30 novembre 1998 organique des services de renseignements et de sécurité).

Le Comité R ne manquera pas de suivre l'évolution de cette affaire dans le cadre de sa compétence de contrôle et de faire rapport à ce sujet au Parlement.

Dans le second cas, il suffit de rappeler, d'une manière générale, que des données classifiées ont été

doorgespeeld in het kader van een aantal onderzoeken die in dit activiteitenverslag vermeld staan.

Ongeacht wat het Comité I denkt over de wenselijkheid van geheimhouding (in een bepaald geval kan een dienst informatie geheim houden, in een ander geval dan weer niet; voorts slaan de opmerkingen van de minister van Justitie op twee onderzoeksrapporten die in het jaarverslag moesten verschijnen en gebaseerd zijn op algeheel geheime nota's (vertrouwelijk — wet van 11 december 1998) toch stond de wet het Comité niet toe deze vertrouwelijke informatie aan de bevoegde ministers mee te delen noch aan de begeleidingscommissie van de Senaat.

In één geval is het zelfs de vraag of het Comité zelf, waarvan de leden over de hoogste machtiging beschikken, toegang krijgt tot informatie die door «de regel van derden» worden beschermd. Het ziet ernaar uit dat de «*need to know*» voor te leggen is aan de buitenlandse dienst die de betrokken informatie heeft bezorgd.

Uit wat voorafgaat, kunnen we afleiden dat deze materie niet alleen netelig maar ook belangwekkend is.

Het Comité I gaat ervan uit dat er inzake veiligheidsmachtigingen heel wat vooruitgang is geboekt in vergelijking met de vroegere regeling, meer bepaald wanneer personen vragen toegang te krijgen tot hun veiligheidsdossier via een beroep bij het Comité.

Voorts meent het Comité dat de vertrouwelijke informatie ook in de praktijk kan bijdragen tot ruimere en ongetwijfeld betere contacten tussen de inlichtingendiensten en de overige nationale overheden en diensten.

Vreemd genoeg draagt die gang van zaken ongetwijfeld op langere termijn ook bij tot een gunstige ontwikkeling van «de cultuur van geheimhouding» die tot heden bij de inlichtingendiensten bestond en ook alleen daar tot ontwikkeling is gekomen. Soms valt die geheimhouding te verantwoorden (*cf.* de organieke wet en de wetten van 11 december 1998) maar in andere gevallen staat ze haaks op het streven naar meer transparantie in onze maatschappij.

Voor de gebruikelijke ontvangers van vertrouwelijke informatie geldt als voorwaarde dat zij de nodige maatregelen nemen om aan de wet te voldoen. Zo krijgen zij toegang tot de informatie en kunnen zij met kennis van zaken op hun werkgebied de nodige beslissingen treffen en tegelijkertijd voor de doelmatige bescherming zorgen die de aard van de geheimhouding van de informatie wettelijk vereist.

transmises par les services de renseignements au Comité R dans le contexte d'enquêtes publiées dans le présent rapport général d'activités.

Quelle que soit l'appréciation que le Comité R puisse faire au sujet de l'opportunité de ces classifications (par exemple dans un cas, un service classifie, l'autre pas; dans un autre cas, les observations du ministre de la Justice concernant deux rapports d'enquête destinés à la publication dans le rapport annuel se basent sur des notes classifiées dans leur intégralité «Confidentiel — Loi du 11 décembre 1998»), il n'a pas été légalement en mesure de communiquer ces informations classifiées aux ministres compétents, ainsi qu'à la Commission sénatoriale de suivi.

Dans un cas, la question se pose même de savoir si le Comité lui-même, dont les membres disposent d'une habilitation du degré le plus élevé, pourrait avoir accès à des informations protégées par la «règle du tiers», le «*need to know*» étant semble-t-il à soumettre à l'appréciation du service étranger fournisseur des informations concernées.

Ces quelques exemples tirés du rapport d'activité montrent que la matière est aussi sensible qu'intéressante.

Le Comité R pense qu'en matière des habilitations de sécurité, un pas considérable vient d'être franchi par rapport au système antérieur, notamment dans le domaine de l'accès des requérants à leur dossier de sécurité par la voie du recours introduit devant le Comité.

La matière de la classification est de nature à apporter également dans la pratique des solutions à une plus grande et, sans doute, à une meilleure communication entre les services de renseignements et les autres autorités et services nationaux.

Paradoxalement, elle permettra sans doute également à plus ou moins long terme de faire évoluer positivement «la culture du secret» existant jusqu'à présent dans la communauté du renseignement (et qui s'y est développée en vase clos) qui, si elle est parfois justifiée (voir à ce sujet les dispositions de la loi organique de même que les dispositions des lois du 11 décembre 1998), ne correspond sans doute pas toujours à l'évolution de la société en général vers une plus grande transparence.

Une condition indispensable consiste cependant pour les destinataires naturels d'informations classifiées que ceux-ci prennent les mesures appropriées pour répondre aux exigences de la loi, et puissent avoir accès à ces données pour prendre en toute connaissance de cause les décisions propres à leur domaine de compétence et de souveraineté tout en continuant à assurer la protection effective qu'implique légalement le degré de classification de ces données.

Daar staat tegenover dat de burgers duidelijker zien welke belangrijke rol de inlichtingen- en veiligheidsdiensten vervullen bij het democratisch functioneren van de Staat.

2. Bespreking van de toezichtsonderzoeken

2.1. Verslag van het onderzoek betreffende de ADIV naar aanleiding van een klacht van een particulier (titel II, deel D, hoofdstuk 1)

Dit onderzoek is het gevolg van een klacht van een lid van de Belgische strijdkrachten dat meende dat hij het slachtoffer is geworden van misbruik door de Algemene Dienst inlichting en veiligheid van de Strijdkrachten (ADIV), ter gelegenheid van een controle van de veiligheid van het informaticasysteem bij de dienst waar hij was gedetacheerd.

Vragen van de leden

Een lid drukt zijn verwondering uit over de besluiten en aanbevelingen van het Vast Comité I in dit verslag.

In de eerste plaats maakt hij zich ongerust over het feit dat een dossier klaarblijkelijk zomaar uit de archieven van de ADIV blijkt te kunnen verdwijnen.

Hij wijst er op dat de periode waarin dit onderzoek gevoerd werd samenviel met deze waarin de regering een aantal belangrijke beslissingen met betrekking tot de Krijgsmacht diende te nemen, zoals bijvoorbeeld de eventuele deelname van België aan het Helios II-project. Men kan op geen enkele manier nagaan of de generale staf niet mogelijk de bedoeling had om met dit dossier de minister onder druk te zetten inzake de deelname van België aan bovengenoemd project.

Voorts zou de eventuele verdwijning van het bewuste dossier een ernstige schending van de rechten van de verdediging kunnen betekenen aangezien de klager zijn dossier niet kan inzien.

Ten slotte wenst hij een verduidelijking over de bevoegdheden van het Vast Comité I terzake.

Een ander lid informeert naar een eventuele band tussen het door de ADIV uitgelokte onderzoek en de persoonlijke situatie van de toenmalige minister van Landsverdediging.

Een derde spreker wijst op de risico's indien blijkt dat «derde instanties», zoals de generale staf van de Krijgsmacht, in het bezit zou blijken te zijn van het bewuste dossier.

Een laatste spreker tenslotte, wenst meer informatie over de klaarblijkelijke verdwijning van een ADIV-dossier, over de huidige bestemming ervan en

Ce faisant et en contrepartie, on évoluera aussi vers une meilleure prise de conscience de la part des citoyens du rôle important des services de renseignements et de sécurité dans le fonctionnement démocratique de l'État.

2. Discussion des rapports de contrôle

2.1. Rapport sur l'enquête relative au SGR à la suite d'une plainte d'un particulier (titre II, partie D, chapitre 1er)

Cette enquête résulte d'une plainte d'un membre des Forces armées belges qui estime avoir été la victime d'abus de la part du Service général de renseignements et de sécurité des Forces armées (SGR), à l'occasion d'un contrôle de la sécurité du système informatique au service où l'intéressé avait été détaché.

Questions des membres

Un membre fait part de son étonnement au sujet des conclusions et des recommandations du Comité permanent R dans ce rapport.

En premier lieu, il s'inquiète de constater qu'un dossier peut manifestement disparaître tout simplement des archives du SGR.

Il signale que l'époque à laquelle cette enquête a été menée correspond à une période pendant laquelle le gouvernement devait prendre une série de décisions importantes concernant les Forces armées, comme par exemple la participation éventuelle de la Belgique au projet Helios II. Il est impossible de déterminer si l'état-major général n'avait pas éventuellement l'intention d'utiliser ce dossier pour mettre le ministre sous pression au sujet de la participation de la Belgique au projet susvisé.

De plus, la disparition éventuelle du dossier concerné pourrait constituer une atteinte grave aux droits de la défense étant donné que le plaignant n'a pas la possibilité de consulter son dossier.

Enfin, il souhaite obtenir des précisions sur les compétences du Comité R en la matière.

Un autre membre s'enquiert de l'existence d'un lien éventuel entre l'enquête ouverte par le SGR et la situation personnelle du ministre de la Défense de l'époque.

Un troisième intervenant souligne les risques dans le cas où il s'avérerait que des «instances tierces», telles que l'état-major général des Forces armées, seraient en possession du dossier en question.

Enfin, un dernier intervenant désire obtenir davantage d'informations sur la disparition manifeste d'un dossier du SGR, sur l'endroit où se trouve ce dossier

— in het algemeen — over de regels die gelden binnen de ADIV voor de archivering van dossiers.

Antwoorden van het Comité I

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, schetst de manier waarop het toezichtsonderzoek is verlopen.

Omdat de gegevens, die de klager in eerste instantie aan het Vast Comité I bezorgde, mogelijk strafbare feiten bevatten werd het dossier in eerste instantie aan de procureur-generaal overgezonden die — zeer tot ongenoegen van de klager — beslist heeft het dossier zonder gevolg te seponeren.

De klager heeft zich vervolgens een tweede maal tot het Vast Comité I gewend.

In dit stadium heeft het Vast Comité I inzage gevraagd — en gekregen — in het dossier van de auditeur-generaal.

Een toezichtonderzoek werd geopend en de volgende vaststellingen werden gedaan:

• de toenmalige minister van Landsverdediging heeft de ADIV behoorlijk gemandateerd om een onderzoek in te stellen naar de beveiliging van het informaticanetwerk op zijn kabinet;

• de klager heeft gedurende een zekere periode loyaal aan dit onderzoek meegewerkt;

• het bestaan van een dossier werd niet betwist aangezien er in de loop van het onderzoek onder meer verschillende verhoren werden afgenomen;

• het desbetreffende dossier werd persoonlijk door de toenmalige chef van de ADIV behandeld;

• de huidige chef van de ADIV werd door zijn voorganger niet gebriefd over dit onderzoek;

• op het ogenblik van de tussenkomst van het Vast Comité I bevond er zich op de ADIV geen geïnventariseerd dossier aangaande dit onderzoek;

• het dossier werd meegenomen door de voorganger van de huidige chef van de ADIV bij zijn vertrek uit de dienst.

Het is daarentegen niet duidelijk of de door de ADIV uitgevoerde aanpassingen aan de beveiliging van het informatiecasysteem van het kabinet ook onder het mandaat van de minister ressorteren.

Tenslotte wijst de spreker op het feit dat het Vast Comité I reeds talloze malen heeft aangedrongen op de inventarisering van de dossiers van de ADIV.

Met betrekking tot de bevoegdheden van de Vast Comité I benadrukt de heer Delepière dat het Vast Comité I uitsluitend bevoegd is om op te treden jegens

actuellement et — en général — sur les règles applicables au sein du SGR en ce qui concerne l'archivage des dossiers.

Réponses du Comité R

M. Jean-Claude Delepière, président du Comité permanent R, décrit la manière dont l'enquête de contrôle s'est déroulée.

Étant donné que les informations que le plaignant avait fournies en premier lieu au Comité R pouvaient contenir des faits punissables, le dossier a d'abord été transmis au procureur général. Celui-ci a, à son tour, transmis le dossier à l'auditeur général, qui — au grand déplaisir du plaignant — a décidé de classer le dossier sans suite.

Le plaignant s'est alors adressé une deuxième fois au Comité permanent R.

À ce stade, le Comité permanent R a demandé et obtenu de consulter le dossier de l'auditeur général.

Une enquête de contrôle a été ouverte et les constatations suivantes ont été faites:

• le ministre de la Défense nationale de l'époque avait dûment mandaté le SGR pour ouvrir une enquête sur la protection du réseau informatique de son cabinet;

• pendant une certaine période, le plaignant a loyalement collaboré à cette enquête;

• l'existence d'un dossier n'a pas été contestée, étant donné qu'au cours de l'enquête, on a entre autres effectué plusieurs auditions;

• le dossier en question a été traité personnellement par l'ancien chef du SGR;

• le chef actuel du SGR n'a pas été informé de cette enquête par son prédécesseur;

• lors de l'intervention du Comité permanent R, il n'existait pas au SGR de dossier inventorié relatif à cette enquête;

• le dossier a été emporté par le prédécesseur du chef actuel du SGR lorsqu'il a quitté le service.

Par contre, on ne voit pas bien si les adaptations effectuées par le SGR à la protection du système informatique du cabinet relevaient également du mandat qui lui avait été donné par le ministre.

Enfin, l'intervenant signale que le Comité permanent R a déjà insisté à de nombreuses reprises pour que l'on fasse l'inventaire des dossiers du SGR.

S'agissant des compétences du Comité permanent R, M. Delepière souligne que ce dernier est exclusivement habilité à intervenir à l'égard des deux services

de beide veiligheidsdiensten. Het kan bijvoorbeeld niet stellen dat de privacy van de klager geschonden werd als de bevoegde gerechtelijke instanties reeds tot een andere conclusie zijn gekomen.

Vragen van de leden (tweede deel)

Een lid vraagt een reflexie over het toezicht op het vernietigen van archieven. In deze context verwijst hij naar Nederland waar een commissie, waarin onder meer parlementsleden zetelen, deze problematiek stuurt. Tevens vestigt hij de aandacht op het historische aspect van de eventueel voor vernietiging in aanmerking komende documenten.

Een ander lid is van oordeel dat deze problematiek gezien dient te worden in het licht van de wet op de bescherming van de persoonlijke levenssfeer. In deze context heeft hij geen bezwaar tegen de vernietiging van strikt persoonlijke gegevens zonder historische waarde. Hij wenst er wel op te wijzen dat documenten die vandaag historisch waardeloos lijken, in de toekomst uiterst belangrijk kunnen worden.

Een derde lid stelt voor om het Vast Comité I de opdracht te geven een nota op te stellen over de politieke verantwoordelijkheid voor het beheer van de archieven in het algemeen en voor deze van de inlichtingendiensten in het bijzonder en daarna met de betrokkene(n) een hoorzitting te organiseren.

Een laatste spreker, tenslotte, vraagt meer uitleg over de evolutie van het onderzoek inzake de gevallen waarin elementen uit een gerechtelijk onderzoek aan de inlichtingendiensten worden doorgegeven en *vice versa* zonder dat daarvan in het initieel dossier een spoor van terug te vinden is.

Antwoorden van het Comité I (tweede deel)

De heer Gérald Vande Walle, raadsheer bij het Vast Comité I, verduidelijkt dat er met de Veiligheid van de Staat een procedure overeengekomen werd die stipuleert dat er geen archieven vernietigd worden zonder dat het Vast Comité I geraadpleegd wordt en zonder dat het kan nazien wat er voor vernietiging in aanmerking komt. In deze overeenkomst wordt rekening gehouden met het eventueel historisch aspect van de betrokken documenten. Een medewerker van de Veiligheid van de Staat staat in voor de historische evaluatie. Wegens personeelsgebrek kunnen er voor het ogenblik echter geen archieven vernietigd worden.

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, stelt dat het verdwenen ADIV-dossier nog steeds niet terecht blijkt te zijn. Wel werden er in dit kader twee nieuwe vertrouwelijke documenten aan het Vast Comité bezorgd betreffende het door de ADIV uitgevoerde informaticaonderzoek. Deze worden voor het ogenblik bestudeerd. Het Comité is

de sécurité. Il ne peut par exemple pas dire que la vie privée du plaignant a été violée si les instances judiciaires compétentes sont déjà arrivées à une autre conclusion.

Questions des membres (deuxième partie)

Un commissaire invite à réfléchir sur le contrôle de la destruction d'archives. Dans ce contexte, il fait référence aux Pays-Bas, où une commission au sein de laquelle siègent notamment des parlementaires gère cette problématique. Il attire également l'attention sur l'aspect historique des documents éventuellement susceptibles d'être détruits.

Un autre commissaire estime que cette problématique doit être vue à la lumière de la loi sur la protection de la vie privée. Dans ce contexte, il ne s'oppose pas à la destruction de données strictement personnelles sans valeur historique. Il tient toutefois à souligner que des documents qui paraissent aujourd'hui dépourvus de valeur historique peuvent devenir extrêmement importants dans l'avenir.

Un troisième intervenant propose de charger le Comité permanent R de rédiger une note relative à la responsabilité politique de la gestion des archives en général et de celles des services de renseignements en particulier, puis d'organiser une audition de l'intéressé (des intéressés).

Enfin, un dernier intervenant demande des explications supplémentaires sur l'évolution de l'enquête sur les cas où des éléments d'une enquête judiciaire sont transmis aux services de renseignements et *vice versa* sans que l'on puisse en retrouver trace dans le dossier initial.

Réponses du Comité R (deuxième partie)

M. Gerald Vande Walle, conseiller au Comité permanent R, explique que l'on est convenu avec la Sûreté de l'État d'une procédure prévoyant qu'aucun document d'archives ne sera détruit sans que le Comité permanent R soit consulté et sans qu'il puisse examiner ce qui est susceptible d'être détruit. Cet accord tient compte de l'éventuel aspect historique des documents en question. Un collaborateur de la Sûreté de l'État est responsable de l'évaluation historique. Aucun document d'archives ne peut toutefois être détruit pour l'instant en raison d'une pénurie de personnel.

M. Jean-Claude Delepière, président du Comité permanent R, affirme que le dossier SGR disparu ne semble toujours pas avoir été retrouvé. Dans ce cadre, deux nouveaux documents confidentiels ont toutefois été remis au Comité permanent R concernant l'enquête sur l'informatique effectuée par le SGR. Ils sont actuellement à l'étude. Le Comité a l'intention de

voornemens om de voormalige bevelhebber van de ADIV uit te nodigen maar heeft geen verweer tegen zijn eventuele weigering. Het is evenmin bevoegd om het dossier, dat zich in een kluis bij de Generale Staf zou bevinden, op te vragen.

Besluit van de commissie

De beide begeleidingscommissies beslissen de minister van Landsverdediging om uitleg te vragen aangaande de wijze waarop de ADIV zijn dossier klasseert in het algemeen en de plaats van het hoger besproken dossier in het bijzonder, en om het Vast Comité I op te dragen een aanvullend onderzoek dienaangaande op te starten. Tevens zullen zij de minister van Landsverdediging vragen om het hoofd van de ADIV verdere uitleg te verschaffen aan de begeleidingscommissie.

2.2. Verslag van het onderzoek naar de manier waarop de inlichtingendiensten hebben gereageerd op mogelijke feiten van spionage of poging tot indringing in het computersysteem van een Belgisch onderzoekscentrum (titel II, hoofdstuk 2)

Vragen van de leden

Een lid informeert naar de aard van het door de ADIV uitgevoerde toezicht op de ondernemingen die tot de zogenaamde « gevoelige sectoren » behoren. *In concreto* informeert hij naar de juistheid van het gerucht als zou de verantwoordelijke veiligheidsofficier-informaticus na het bedoelde incident ontslag genomen hebben en vervolgens bij de NAVO in dienst zou zijn getreden.

Antwoorden van het Vast Comité I

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, bevestigt dat de betrokken veiligheidsofficier-informaticus, na de gebeurtenissen waarvan sprake, bij de NAVO in dienst getreden is. In deze context kondigt hij een vervolg aan op het reeds bestaande dossier dat in de nabije toekomst aan de begeleidingscomissies zal bezorgd worden.

2.3. De werking van onze inlichtingendiensten in een zaak van wapenhandel waarvan het Comité I kennis heeft gekregen via een open bron (titel II, hoofdstuk 2)

De voorzitter deelt mee dat het Comité I beslist heeft om — op expliciete vraag van de minister van Justitie — dit hoofdstuk niet in de eindversie van het activiteitenverslag op te nemen.

convoquer l'ancien commandant du SGR, mais il n'a pas de défense contre son éventuel refus. Il n'est pas non plus habilité à réclamer le dossier, qui se trouverait dans un coffre de l'état-major général.

Décision de la commission

Les deux commissions de suivi décident de demander au ministre de la Défense nationale des explications concernant la façon dont le SGR classe ses dossiers en général et la place du dossier discuté ci-dessus en particulier, et de charger le Comité permanent R d'ouvrir une enquête complémentaire à ce sujet. Elles demanderont également au ministre de la Défense nationale que le chef du SGR fournisse des explications supplémentaires à la commission de suivi.

2.2. Rapport sur l'enquête portant sur la manière dont les services de renseignements ont réagi à l'éventualité de faits d'espionnage ou de tentative d'effraction dans le système informatique d'un centre belge (titre II, chapitre 2)

Questions des membres

Un membre demande quelle est la nature du contrôle effectué par le SGR sur les entreprises qui appartiennent aux secteurs dits « sensibles ». Concrètement, il s'informe sur la véracité des rumeurs selon lesquelles l'officier de sécurité informaticien responsable aurait donné sa démission après l'incident en question, puis serait entré au service de l'OTAN.

Réponses du Comité permanent R

M. Jean-Claude Delepière, président du Comité permanent R, confirme que l'officier de sécurité informaticien concerné est entré en fonction à l'OTAN après les événements dont il a été question. Dans ce contexte, il annonce une suite au dossier déjà existant, qui sera transmise aux commissions de suivi dans un proche avenir.

2.3. L'action de nos services de renseignements dans une affaire de trafic d'armes dont le Comité R a eu connaissance par le biais d'une source ouverte (titre II, chapitre 2)

Le président annonce que le Comité R a décidé — à la demande expresse du ministre de la Justice — de ne pas insérer ce chapitre dans la version définitive du rapport d'activités.

2.4. Degeschillen inzake de veiligheidsmachtigingen (titel I, hoofdstuk 3)

Vragen van de leden

Een lid wenst in het kader van het hoofdstuk over de geschillen inzake de veiligheidsmachtigingen te vernemen op welke wijze de transparantie en de selectiviteit van het verlenen van een dergelijke machtiging kunnen verhoogd worden. Hij wenst concreet te vernemen hoever het staat met het verlenen van dergelijke machtigingen aan rechtspersonen. In deze context wijst hij op het mogelijk loyaliteitsprobleem waarmee de Belgische veiligheidsofficieren in dienst van een buitenlandse onderneming geconfronteerd zullen worden.

Een ander lid vraagt zich af welk economisch nut een onderneming uit een veiligheidsmachtiging kan puren.

Een derde spreker wijst op het feit dat een rechtspersoon bestaat door zijn organen en zijn aangestelden. Een rechtspersoon kan dus wel als dusdanig gestraft worden maar er een veiligheidsmachtiging aan verlenen lijkt de spreker minder evident.

Antwoorden van het Comité I

De voorzitter van het Comité I wijst er op dat de cel, die bij de ADIV instaat voor het toezicht op de ca. 300 betrokken ondernemingen en voor het beheer van de daarmee gepaard gaande veiligheidsmachtigingen, uit slechts drie personen bestaat.

Daarnaast blijken steeds meer ondernemingen, inzonderheid uit de technologiesector, een veiligheidsmachtiging aan te vragen omdat zij er van uitgaan dat dit hun in de internationale concurrentiestrijd een bonus oplevert.

Daarenboven wordt bij de aanvraag voor een veiligheidsmachtiging van een onderneming eerst nagegaan of de betrokken firma wel betrouwbaar is vooraleer het eigenlijke onderzoek naar de veiligheidsmachtiging kan worden opgestart. Men is er immers ten zeerste voor beducht dat ondernemingen met banden in de georganiseerde misdaad een veiligheidsmachtiging zouden krijgen.

Dit heeft als gevolg dat de betrokken cel er nog slechts kan naar streven de veiligheidsmachtigingen binnen de vereiste termijn af te leveren, enerzijds, en elke betrokken firma eenmaal per jaar te inspecteren, anderzijds.

De voorzitter van het Comité I benadrukt eveneens dat de huidige criteria voor het verlenen van een veiligheidsmachtiging aan een rechtspersoon (*cf.* artikel 27 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheids-

2.4. Les litiges relatifs aux habilitations de sécurité (titre I^er^, chapitre 3)

Questions des membres

Dans le cadre du chapitre consacré aux litiges relatifs aux habilitations de sécurité, un commissaire demande comment il est possible d'accroître la transparence et la sélectivité de l'octroi d'une telle habilitation. Il souhaite savoir concrètement où en est l'octroi de pareilles habilitations à des personnes morales. Dans ce contexte, il met l'accent sur l'éventuel problème de loyauté auquel les officiers de sécurité belges au service d'une entreprise étrangère seront confrontés.

Un autre commissaire demande quel avantage économique une entreprise peut tirer d'une habilitation de sécurité.

Un troisième intervenant signale qu'une personne morale existe par ses organes et ses préposés. Une personne morale peut donc être pénalisée en tant que telle, mais lui octroyer une habilitation de sécurité paraît moins évident à l'intervenant.

Réponses du Comité R

Le président du Comité R signale que la cellule responsable, au sein du SGR, de la surveillance des quelque 300 entreprises concernées et de la gestion des habilitations de sécurité qui vont de pair ne compte que trois personnes.

Il s'avère en outre que de plus en plus d'entreprises, surtout dans le secteur de la technologie, demandent une habilitation de sécurité parce qu'elles partent du principe que cela leur donne un bonus dans la compétition internationale à laquelle elles se livrent.

De plus, lorsqu'une entreprise demande une habilitation de sécurité, on vérifie d'abord si la firme en question est digne de confiance, et ce n'est qu'ensuite que l'enquête proprement dite sur l'habilitation de sécurité peut débuter. L'on craint en effet au plus haut point que des entreprises ayant des liens avec la criminalité organisée n'obtiennent une habilitation de sécurité.

La conséquence en est que la cellule en question ne peut plus s'efforcer que de délivrer les habilitations de sécurité dans le délai requis, d'une part, et d'inspecter chaque firme concernée une fois par an, d'autre part.

Le président du Comité R souligne également que les critères actuels d'octroi d'une habilitation de sécurité à une personne morale (*cf.* l'article 27 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité) ne sont plus suffisants.

machtigingen) niet meer toereikend zijn. De Nationale Veiligheidsautoriteit werkt ten andere aan de aanpassing van deze criteria.

Het probleem inzake het loyaliteitsconflict van de veiligheidsofficieren was een element in de besprekingen met de Nationale Veiligheidsoverheid in het kader van de nieuwe opdracht van het Vast Comité I als beroepsorgaan bij het verlenen van de veiligheidsmachtigingen.

Een lid vraagt zich af of de begeleidingscommissies de minister van Landsverdediging niet moeten vragen om de hogergenoemde ADIV-cel te versterken zodat zij haar taken naar behoren kan vervullen.

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, herinnert aan het hangende toezichtsonderzoek naar de aard en de aanwending door de beide inlichtingendiensten van de hen ter beschikking gestelde menselijke middelen. Daarom lijkt het hem opportuun de resultaten van dit onderzoek af te wachten vooraleer eventueel aan te dringen op een eventuele versterking van de betrokken cel.

2.5. Verslag van het onderzoek naar de manier waarop de Veiligheid van de Staat haar nieuwe opdracht inzake de bescherming van het wetenschappelijk of economisch potentieel van het land vervult (titel II, hoofdstuk 8)

Vragen van de leden

Een lid wijst er op dat nog nauwelijks 10 % van de in België gevestigde ondernemingen daadwerkelijk in Belgische handen blijkt te zijn. Hij vreest dan ook dat de zowel *qua* personeel als *qua* investeringen gevraagde inspanningen zullen leiden tot een afname van de middelen die worden ingezet in de strijd tegen de georganiseerde misdaad.

Een ander lid wenst de *status questionis* te horen betreffende de opvolging van de — zowel officiële als officieuze — aan sommige landen opgelegde economische sancties. Meer bepaald wenst hij te vernemen of het Vast Comité I tevreden is met de in het jaarverslag opgenomen antwoorden van de beide inlichtingendiensten.

Een lid vraagt zich af op welke wijze kan worden tegemoetgekomen aan de opmerking van het Vast Comité I dat het niet bevoegd is om de door het Ministerieel Comité voor Inlichting en Veiligheid verspreide inlichtingen op te vragen alhoewel precies dit comité de prioriteiten van de beide inlichtingendiensten bepaalt, de werking ervan coördineert en daartoe de nodige richtlijnen vaststelt.

Dezelfde spreker polst naar de mogelijke stappen die kunnen gezet worden in het raam van een toezicht

L'autorité nationale de sécurité œuvre par ailleurs à l'adaptation de ces critères.

Le problème du conflit de loyauté auquel sont confrontés les officiers de sécurité a été un élément des discussions avec l'autorité nationale de sécurité dans le cadre de la nouvelle mission du Comité permanent R en tant qu'organe d'appel lors de l'octroi des habilitations de sécurité.

Un membre se demande si les commissions de suivi ne doivent pas demander au ministre de la Défense nationale de renforcer la cellule SGR susvisée pour lui permettre de s'acquitter de sa mission comme il se doit.

M. Jean-Claude Delepière, président du Comité permanent R, rappelle l'enquête de contrôle en cours sur la nature et l'affectation, par les deux services de renseignements, des effectifs mis à leur disposition. C'est pourquoi il lui paraît opportun d'attendre les résultats de cette enquête avant d'éventuellement insister sur un renforcement de la cellule en question.

2.5. Rapport sur l'enquête portant sur la manière dont la Sûreté de l'État s'acquitte de sa nouvelle mission en matière de protection du potentiel scientifique ou économique du pays (titre II, chapitre 8)

Questions des membres

Un membre signale qu'à peine 10 % des entreprises établies en Belgique s'avèrent être encore réellement entre des mains belges. Il craint dès lors que les efforts demandés tant en personnel qu'en investissements n'entraînent une diminution des moyens affectés à la lutte contre la criminalité organisée.

Un autre membre souhaite connaître l'état de la question en ce qui concerne le suivi des sanctions économiques — tant officielles qu'officieuses — infligées à certains pays. Il désire savoir plus précisément si le Comité permanent R est satisfait des réponses des deux services de renseignements reproduites dans le rapport annuel.

Un commissaire se demande comment on peut répondre à l'observation du Comité permanent R selon laquelle celui-ci n'est pas habilité à demander les renseignements diffusés par le Comité ministériel du renseignement et de la sécurité, alors que c'est précisément ce comité qui détermine les priorités des deux services de renseignements, qui en coordonne le fonctionnement et qui fixe les directives requises à cet effet.

Le même intervenant s'interroge sur les démarches éventuelles qui peuvent être faites dans le cadre d'un

op de private inlichtingenondernemingen die vooral op het juridisch-economisch vlak actief blijken te zijn.

Een ander lid waarschuwt voor de privatisering van de inlichtingendiensten. Daarnaast vraagt hij de nodige aandacht voor het fenomeen van de belangenneming door leden van de inlichtingendiensten in private inlichtingenondernemingen in afwachting van hun overstap. Hij stelt dan ook voor om het Vast Comité I met een onderzoek in deze zin te gelasten.

Antwoorden van het Comité I

De heer Gérard Vande Walle, raadsheer bij het Vast Comité I, licht toe dat het comité schriftelijk bij de beide inlichtingendiensten geïnformeerd heeft naar de opvolging van de embargo's maar geen toezichtsonderzoek als dusdanig heeft opgestart. Wel kan het comité desgevallend rekening houden met de teneur van het antwoord van de beide inlichtingendiensten indien er in de toekomst een toezichtsonderzoek naar deze materie zou moeten ingeleid worden.

De heer Jean-Claude Delepière, voorzitter van het Vast Comité I, meent dat vooreerst moet worden nagegaan of het gaat om een systeem. Daarom dient de huidige toestand aan een onderzoek te worden onderworpen.

Hij wijst erop dat de inspanningen om via de inlichtingendiensten de door het Ministerieel Comité voor inlichting en veiligheid uitgevaardigde instructies te verkrijgen tot op heden niet erg succesvol zijn gebleken. Hij suggereert dan ook dat de begeleidingscommissies in eerste instantie bij de eerste minister zouden tussenkomen om de weg te effenen. Daarna zou er eventueel gedacht kunnen worden aan een wetswijziging.

De voorzitter van het comité stelt vast dat de problematiek van de privé-inlichtingenondernemingen niet alleen reëel is maar zelfs aan belang wint. De klassieke inlichtingendiensten blijken als dusdanig niet klaar te zijn om er een adequaat antwoord op te formuleren alhoewel een aantal individuele medewerkers wel bereid is om in deze materie te investeren.

2.6. De benoeming van een adjunct-administrateur-generaal

Een lid informeert naar de stand van zaken inzake de benoeming van een adjunct-administrateur-generaal van de Veiligheid van de Staat.

De heer Delepierre zal de meest recente ontwikkelingen inzake de benoeming van de adjunct-administrateur-generaal bij de Veiligheid van de Staat aan de begeleidingscommissies meedelen.

contrôle des entreprises de renseignements privées qui se révèlent surtout actives dans le domaine juridico-économique.

Un autre commissaire met en garde contre la privatisation des services de renseignements. Il attire en outre l'attention sur le phénomène de la prise d'intérêts par des membres des services de renseignements, dans des entreprises de renseignements privées dans l'attente d'y passer. Il propose dès lors de charger le Comité permanent R d'une enquête en ce sens.

Réponses du Comité R

M. Gérard Vande Walle, conseiller au Comité permanent R, explique que le comité s'est informé par écrit auprès des deux services de renseignements du suivi des embargos, mais n'a pas entamé d'enquête de contrôle proprement dite. Le cas échéant, le comité peut toutefois tenir compte de la teneur de la réponse des deux services de renseignements s'il fallait ouvrir une enquête de contrôle sur cette matière dans l'avenir.

M. Jean-Claude Delepière, président du Comité permanent R, estime qu'il faut d'abord examiner s'il s'agit d'un système. C'est pourquoi la situation actuelle doit faire l'objet d'une enquête.

Il signale que jusqu'à présent, les efforts pour obtenir les instructions par le Comité ministériel du renseignement et de la sécurité par l'intermédiaire des services de renseignements ne se sont pas révélés très fructueux. Il suggère donc que les commissions de suivi interviennent d'abord auprès du premier ministre pour préparer la voie. Ensuite, on pourrait éventuellement envisager une modification de la loi.

Le président du comité constate non seulement que la problématique des entreprises de renseignements privées est réelle, mais même qu'elle croît en importance. Les services de renseignements classiques ne s'avèrent pas prêts en tant que tels à y formuler une réponse appropriée, bien qu'un certain nombre de collaborateurs individuels soient malgré tout disposés à s'investir en la matière.

2.6. La nomination d'un administrateur général adjoint

Un commissaire s'informe de l'état d'avancement de la nomination d'un administrateur général adjoint de la Sûreté de l'État.

M. Delepière communiquera aux commissions de suivi les développements les plus récents en ce qui concerne la nomination de l'administrateur général adjoint à la Sûreté de l'État.

3. Beslissingen van de begeleidingscommissies

Er wordt overeegekomen om het Vast Comité I te belasten met de opdracht om:

— de begeleidingscommissies een document te bezorgen dat als basis kan dienen om de minister van Landsverdediging te ondervragen over de eventuele onderbezetting van de ADIV-cel die zich met de veiligheidsmachtigingen bezighoudt;

— een vergelijkende studie uit te voeren inzake het verlenen van een veiligheidsmachtiging aan een rechtspersoon;

— na te gaan hoe de archivering van documenten en de vernietiging ervan geregeld is, rekening houdende met de wet op de privé-sfeer. Daarna kunnen desgevallend — met het oog op het formuleren van een aanbeveling aan de bevoegde ministers — hoorzittingen georganiseerd worden;

— de commissies vóór het uitbrengen van het activiteitenverslag 2001 een tussenverslag te bezorgen over de opvolging door de beide inlichtingendiensten van de uitgevaardigde embargo's;

— na te gaan in hoeverre het niet-vermelden in gerechtelijke dossiers dat elementen eruit aan de inlichtingendiensten worden doorgegeven en *vice versa* op een systeem berust;

— een toezichtsonderzoek te openen naar de problematiek van de privé-inlichtingenondernemingen en de reactie van de inlichtingendiensten;

Er wordt eveneens overeengekomen om de eerste minister te contacteren om een oplossing te zoeken voor het bevoegdheidsprobleem van het Vast Comité I ten aanzien van het Ministerieel Comité voor inlichting en veiligheid.

Ten slotte stemmen de commissies ermee in om — zoals gevraagd door de minister van Justitie — het hoofdstuk over de werking van onze inlichtingendiensten in een zaak van wapenhandel waarvan het Comité I kennis heeft gekregen via een open bron uit de definitieve versie van het activiteitenverslag 2000 te lichten.

Dit verslag wordt eenparig goedgekeurd.

De rapporteurs, *De voorzitters,*

Hugo VANDENBERGHE. Armand DE DECKER.

Hugo COVELIERS. Herman DE CROO.

3. Décisions des commissions de suivi

Il est convenu de charger le Comité permanent R des missions suivantes:

— fournir aux commissions de suivi un document qui pourra servir de base pour interroger le ministre de la Défense nationale sur le manque de personnel de la cellule du SGR qui s'occupe des habilitations de sécurité;

— procéder à une étude comparative en matière d'octroi d'une habilitation de sécurité à une personne morale;

— examiner comment l'archivage des documents et leur destruction sont réglés, compte tenu de la loi sur la protection de la vie privée. Ensuite, des auditions — en vue de formuler une recommandation à l'intention des ministres compétents — pourront éventuellement être organisées;

— fournir aux commissions, avant la diffusion du rapport d'activités 2001, un rapport provisoire sur le suivi, par les deux services de renseignements, des embargos décrétés;

— examiner dans quelle mesure le fait de ne pas mentionner dans des dossiers judiciaires que des éléments en faisant partie sont communiqués aux services de renseignements et *vice versa* constitue un système;

— ouvrir une enquête de contrôle sur la problématique des entreprises de renseignements privées et la réaction des services de renseignements.

Il est également convenu de contacter le premier ministre en vue de trouver une solution au problème de compétence du Comité permanent R à l'égard du Comité ministériel du renseignement et de la sécurité.

Enfin, les commissions acceptent de retirer de la version définitive du rapport d'activité 2000 — à la demande du ministre de la Justice — le chapitre consacré à l'action de nos services de renseignements dans une affaire de vente d'armes dont le Comité R a eu connaissance par le biais d'une source ouverte.

Le présent rapport a été approuvé à l'unanimité.

Les rapporteurs, *Les présidents,*

Hugo VANDENBERGHE. Armand DE DECKER.

Hugo COVELIERS. Herman DE CROO.

2 - 867/1 - 2001/2002
DOC 50 **1434/001**

BIJLAGE

ANNEXE

ACTIVITEITENVERSLAG 2000

RAPPORT D'ACTIVITÉ 2000

INHOUD

SOMMAIRE

TITEL I

INLEIDING

HOOFDSTUK 1

ALGEMEEN

1. Toezichtsonderzoeken

1.1. Algemene toezichtsbevoegdheden van het Comité I

Het toezicht, dat krachtens de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten werd ingevoerd, heeft betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, alsook op de coördinatie en de efficientie van de inlichtingen- en veiligheidsdiensten (1).

De bovengenoemde organieke wet van 18 juli 1991 noemt in artikel 3 de twee inlichtingendiensten die onderworpen zijn aan het democratisch toezicht van het parlement. Het parlement oefent dit toezicht uit via het Comité I, dat krachtens dezelfde wettekst werd opgericht. Deze twee diensten zijn de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (ADIV).

Om het Comité I in de gelegenheid te stellen toezicht uit te oefenen, heeft de wetgever aan dit Comité de bevoegdheid verleend onderzoek te voeren naar de activiteiten en de werkwijzen van de voornoemde inlichtingendiensten, naar hun interne reglementen en richtlijnen, alsook naar alle documenten die de handelwijze van de leden van deze diensten regelen. Overigens zijn deze diensten verplicht hun interne reglementen en richtlijnen en de documenten tot regeling van het gedrag van hun leden, uit eigen beweging aan het Comité I te bezorgen (*cf.* artikel 33 van de wet van 18 juli tot regeling van het toezicht op de politie- en inlichtingendiensten).

Voorts vermelden we dat het Ministerieel Comité voor Inlichting en Veiligheid (2) (voorgezeten door de eerste minister, en bestaande uit de ministers van Buitenlandse Zaken, Binnenlandse Zaken, Landsverdediging, Justitie en de Staatssecretaris voor Energie en Ontwikkeling) het algemeen beleid inzake inlichtingen uitstippelt. Dit Comité bepaalt ook de priori-

(1) Artikel 1 van de wet van 18 juli 1991 zoals gewijzigd door de wet van 1 april 1999 (*Belgische Staatsblad* van 3 april 1999, blz. 11161).

(2) *Cf.* met name de artikelen 4, 7, 1º, 10, § 1, 11, § 1-4º, 20, § 3 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (*Belgische Staatsblad* van 18 december 1998).

TITRE Ier

INTRODUCTION

CHAPITRE 1er

GÉNÉRALITÉS

1. Les enquêtes de contrôle

1.1. Les compétences générales de contrôle du Comité R

Le contrôle institué par la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement porte sur la protection des droits que la Constitution et la loi confèrent aux personnes ainsi que sur la coordination et l'efficacité des services de renseignement et de sécurité (1).

La loi organique du 18 juillet 1991, précitée, répertorie en son article 3 les deux services de renseignement auxquels s'applique le contrôle démocratique du parlement, via le Comité R institué par le même texte légal. Il s'agit de la Sûreté de l'État et du Service général de renseignement et de sécurité des forces armées (SGR).

Pour exercer son contrôle, le Comité R a reçu du législateur la compétence d'enquêter sur les activités et sur les méthodes de ces services de renseignement, sur leurs règlements et directives internes, ainsi que sur tous les documents réglant le comportement des membres de ces services. Ces services sont d'ailleurs tenus de transmettre d'initiative au Comité ces règlements, directives internes et documents qui règlent le comportement de leurs membres (*cf.* article 33 de la loi du 18 juillet organique du contrôle des services de police et de renseignement).

Il faut préciser également que le Comité ministériel du renseignement (2) (présidé par le premier ministre et composé des ministres des Affaires étrangères, de l'Intérieur, de la Défense nationale, de la Justice et du secrétaire d'État à l'Énergie et au Développement) établit la politique générale du renseignement. Il détermine également les priorités de la Sûreté de l'État

(1) Article 1er de la loi du 18 juillet 1991 tel qu'il a été modifié par la loi du 1er avril 1999 (*Moniteur belge* du 3 avril 1999, p. 11161).

(2) *Cf.* notamment les articles 4, 7, 1º, 10, 1er, 11, § 4º , 20, § 3, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*Moniteur belge* du 18 décembre 1998).

teiten van de Veiligheid van de Staat en van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht. Het coördineert tevens de activiteiten van deze diensten. Bovendien bepaalt het Ministerieel Comité het beleid inzake het beschermen van gevoelige informatie. Hiertoe stelt het richtlijnen vast.

In verband hiermee vestigt het Comité I de aandacht op het feit dat het bovengenoemde artikel 33 van de wet van 18 juli 1991 tot regeling van het toezicht, niet bepaalt dat de richtlijnen van het Ministerieel Comité voor inlichting en veiligheid, of de richtlijnen van het College voor inlichting en veiligheid(1) moeten worden opgenomen in de interne documenten die de inlichtingendiensten uit eigen beweging aan het Comité I moeten bezorgen.

Niettemin is het Comité I van mening dat het toegang tot die richtlijnen zou moeten hebben, teneinde zijn controleopdracht met kennis van zaken te kunnen uitvoeren, alsook zijn nieuwe opdracht als beroepsorgaan inzake de veiligheidsmachtigingen (zie verder — Titel I, hoofdstuk 3: «De geschillen inzake de veiligheidsmachtigingen» blz. 18).

Met betrekking tot de wijze waarop administratieve toezichtsonderzoeken kunnen worden geopend, moet men een onderscheid maken tussen onderzoeken die worden geopend op verzoek van het parlement, onderzoeken die het Comité I -of zijn Dienst Enquêtes — uit eigen beweging opent, en de onderzoeken die worden geopend naar aanleiding van een klacht van een particulier betrokken bij de activiteiten van een inlichtingendienst of van een lid van deze diensten. Bovendien bepaalt de wet dat, ook al is het Comité I een uitvloeisel van de wetgevende macht, een toezichtsonderzoek ook aan het Comité I kan worden toevertrouwd op verzoek van een van de bevoegde ministers, zijnde de minister van Justitie en de minister van Landsverdediging(2).

Benevens dit parlementair toezicht dat *a posteriori* wordt uitgeoefend, zijn de activiteiten van beide inlichtingendiensten sinds 1 februari 1999 ook onderworpen aan de bepalingen van de wet van 30 november 1998 houdende regeling van de Inlichtingen- en veiligheidsdiensten.

Het probleem waartoe dit toezicht leidt in geval van materies die tegelijk de politie- en de inlichtingendiensten kunnen aanbelangen, wordt behandeld in artikel 53 van de wet van 18 juli 1991. Dit artikel bepaalt dat wat betreft de taakverdeling en de coördinatie van de werking tussen enerzijds de politiediensten en anderzijds de inlichtingendiensten, de Vaste Comités P en I gezamenlijke toezichtsonderzoeken

(1) Opgericht bij koninklijk besluit van 21 juni 1996.

(2) Van deze laatste mogelijkheid, om het Comité I te belasten met een onderzoek, werd (zo goed als) geen gebruik gemaakt sinds dit Comité zijn activiteiten heeft aangevat op 26 mei 1993.

et du Service général du renseignement et de la sécurité des Forces armées. Il coordonne aussi les activités de ces différents services. Le Comité ministériel définit, en outre, la politique en matière de protection des informations sensibles. Il établit pour ce faire des directives.

Le Comité R attire à ce sujet l'attention sur le fait que l'article 33 précité de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991 n'inclut pas les directives du Comité ministériel du renseignement et de la sécurité, ni celles du Collège du renseignement et de la sécurité(1), dans les documents internes que les services de renseignement doivent transmettre d'initiative au Comité R.

Celui-ci pense néanmoins qu'il serait indispensable qu'il puisse y avoir accès de manière à pouvoir exercer en connaissance de cause sa mission de contrôle ainsi d'ailleurs que sa nouvelle mission d'organe de recours en matière d'habilitations de sécurité (voir à ce sujet le chapitre 3 ci-après: «Le contentieux des habilitations de sécurité» p. 18).

En ce qui concerne la manière dont les enquêtes administratives de contrôle peuvent être initiées, il faut distinguer celles suscitées par le parlement, celles ouvertes d'initiative par le Comité R ou par son Service d'enquêtes et celles résultant d'une plainte d'un particulier concerné par les activités d'un service de renseignement ou d'un membre de ces services. En outre, bien que le Comité R soit une émanation du pouvoir législatif, la loi prévoit encore qu'une enquête de contrôle peut être confiée au Comité R à la demande d'un des ministres compétents, à savoir celui de la Justice et celui de la Défense nationale(2).

Outre ce contrôle parlementaire *a posteriori*, les activités des deux services de renseignement sont depuis le 1er février 1999 désormais encadrées par les dispositions de la loi du 30 novembre 1998 organique des Services de renseignement et de sécurité.

La problématique de ce contrôle pour des matières susceptibles de concerner à la fois les services de police et de renseignement est rencontrée par l'article 53 de la loi du 18 juillet 1991 qui prévoit que «pour ce qui concerne la répartition des missions et la coordination du fonctionnement entre d'une part les services de police et d'autre part les services de renseignement, les Comités permanent P et R peuvent réali-

(1) Créé par l'arrêté royal du 21 juin 1996.

(2) Cette dernière possibilité de saisir le Comité permanent R n'a pratiquement pas été utilisée depuis que celui-ci a débuté ses activités le 26 mai 1993.

kunnen verrichten. (Zie Titel II, «Eindverslag over het gezamenlijk onderzoek naar de veiligheidsmaatregelen die binnen de algemene politiesteundienst (APSD) werden genomen om het welslagen van de gerechtelijke onderzoeken te waarborgen en meer in het algemeen naar de doelmatigheid van deze dienst» (blz. 187).

1.2. Staat van de onderzoeken

Ook al bestaat de gewoonte om in een jaarlijks activiteitenverslag statistieken op te nemen, willen we eerst en vooral benadrukken dat, in de specifieke, heel bijzondere(1) -en al bij al recente- materie van het bestendig parlementair toezicht op de activiteiten van de inlichtingendiensten(2), dergelijke gegevens wellicht slechts van ondergeschikt belang zijn om inzicht te krijgen in de resultaten van de controleopdracht, zoals ze wordt beschreven in punt 1.1 hierboven.

Benevens de toezichtsonderzoeken, een bij wet ingevoerde procedure die toelaat *a posteriori* de doeltreffende werking van de diensten te controleren en na te gaan of de fundamentele rechten en vrijheden van de burgers worden gerespecteerd, beschikt het Comité I over andere middelen waarmee het probeert zijn opdracht concreet te vervullen in een klimaat van grotere transparantie vanwege de inlichtingendiensten(3).

Op het gebied van een betere kwantitatieve en kwalitatieve kennisgeving aan het controleorgaan door deze diensten, moeten inderdaad nog inspanningen worden gedaan en is er nog heel wat ruimte voor verbetering. Het Comité I vraagt de diensten regelmatig informatie over sommige actuele thema's of

(1) Zie activiteitenverslag Comité I, 1999, Titel III, hoofdstuk 4, blz. 131: Het beknopt rapport betreffende de deelname van het Comité I aan de Conferentie van de organen die toezicht houden op de activiteiten inzake inlichtingen (Ottawa, 28 en 29 juni 1999), gewijd aan het thema *«Onderzoek en toezicht in het nieuwe millennium: de uitdagingen van een multipolaire wereld»*.

(2) Bij wijze van voorbeeld: er bestaan systemen van parlementaire controle in de Verenigde Staten, in Groot-Brittannië, Duitsland, Italië. Het Comité I toont vooral belangstelling voor de evolutie van het probleem van het parlementair toezicht in Frankrijk, waar de diensten zich lijken te verzetten tegen het beginsel van dit toezicht. Een eerste wetsvoorstel werd ingediend in 1997, maar werd nadien weer ingetrokken. Op 23 november 1999 legde de heer Paecht, volksvertegenwoordiger, in naam van de Commissie Landsverdediging en Krijgsmacht, voorgezeten door de heer Paul Quilès, aan de Assemblée Nationale een rapport voor met het oog op de oprichting van een parlementaire delegatie voor inlichtingen.

(3) Terloops en bij wijze van voorbeeld onderstreept het Comité I, met betrekking tot de openstelling naar een betere kennis van de activiteiten van de inlichtingendiensten, dat in sommige landen de inlichtingendiensten — zoals de Bvf in Duitsland — jaarverslagen opmaken die informatie bevatten. Deze handelwijze contrasteert met de gebruikelijke nevelen waarin de activiteiten van deze diensten gewoonlijk gehuld zijn.

ser des enquêtes communes de contrôle». (Voir le rapport d'enquête commune concernant «les mesures de sécurité prises au sein du SGAP en vue d'assurer le succès des enquêtes judiciaires et de manière plus générale sur l'efficacité de ce service» p. 173 du présent rapport).

1.2. La situation des enquêtes

S'il est de tradition dans un rapport annuel d'activités d'aligner des statistiques, il convient de souligner d'emblée que dans la matière spécifique, très particulière(1), et somme toute récente du contrôle parlementaire permanent des activités des services de renseignement(2), ces données n'ont sans doute qu'une importance secondaire pour appréhender les résultats de la mission de contrôle, telle qu'elle est décrite au point 1.1. ci-dessus.

Au-delà d'ailleurs des enquêtes de contrôle, le Comité R a recours à d'autres démarches pour tenter d'accomplir concrètement sa tâche dans un climat de plus grande transparence de la part des services de renseignement(3).

C'est en effet dans le domaine d'une meilleure information, tant quantitative que qualitative, de l'organe de contrôle par ces services que des efforts doivent encore être développés et des progrès accomplis. C'est ainsi que le Comité R adresse régulièrement des demandes d'information aux services sur certains

(1) Voir à ces sujets «Le rapport succinct relatif à la participation du Comité R à la Conférence des organismes de surveillance des activités de renseignement (Ottawa 28 et 29 juin 1999) tenue sur le thème *«Examen et surveillance dans le nouveau millénaire: les défis d'un monde multipolaire»*. Rapport général d'activités du Comité R 1999, pp. 116 et 117.

(2) À titre d'exemples des systèmes de contrôle parlementaire existent aux États-Unis, en Grande-Bretagne, en Allemagne, en Italie. Le Comité R marque un intérêt particulier à suivre l'évolution de la problématique du contrôle parlementaire en France, où le principe de ce dernier semble avoir soulevé l'opposition des services. Une première proposition de loi déposée en 1997 a été retirée. Un rapport tendant à la création d'une délégation parlementaire pour les affaires de renseignement a été présenté à l'Assemblée nationale, le 23 novembre 1999 par M. le député Paecht, au nom de la commission de la Défense nationale et des Forces armées présidée par M. Paul Quilès.

(3) Incidemment et à titre d'exemple dans le domaine de l'ouverture vers une meilleure connaissance de l'activité des services de renseignement, le Comité permanent R souligne que dans certains pays des services comme le Bvf en Allemagne établissent des rapports annuels contenant des informations, ce qui contraste avec l'habituelle opacité générale qui entoure généralement les activités de tels services.

vraagstukken (zie verder blz. 10 «Vragen gesteld door het Comité I aan de inlichtingendiensten»). Geleidelijk wordt ook een systeem van periodieke vergaderingen of briefings ingevoerd, teneinde de activiteiten van de diensten beter te kunnen volgen.

We komen even terug op de eigenlijke onderzoeken: tussen 1 januari en 31 december 2000 hebben het Vast Comité van Toezicht op de inlichtingendiensten en zijn Dienst Enquêtes in totaal 29 dossiers behandeld. Daarvan werden er 15 geopend in diezelfde periode. Van deze 15 onderzoeken werden er 10 geopend op initiatief van het Comité I, 4 naar aanleiding van een klacht van particulieren en 1 op verzoek van de begeleidingscommissie van het Comité I. Van deze 15 onderzoeken hebben er 8 uitsluitend betrekking op de Veiligheid van de Staat en 4 uitsluitend op de Algemene Dienst inlichting en veiligheid van de Krijgsmacht. De overige 3 onderzoeken hebben betrekking op materies die tot de bevoegdheid van beide diensten behoren.

Op de datum waarop we dit verslag sluiten, zijn 14 toezichtsonderzoeken, waarvan sommige van groot belang, nog in behandeling. Voor sommige onderzoeken moet de Dienst Enquêtes van het Comité I nog een aantal opdrachten uitvoeren, in andere heeft deze Dienst de resultaten van zijn onderzoeksactiviteiten aan het Comité I bezorgd en stelt dit Comité een rapport op dat krachtens artikel 33, lid 3 van de organieke wet inzake toezicht bestemd is voor de betrokken ministers en voor de begeleidingsscommissie van de Senaat.

De onderzoeken, waarvan een rapport reeds werd verzonden naar de ministers van Justitie en Landsverdediging, evenals naar de Senaat, zijn het voorwerp van Titel II van dit algemeen activiteitenverslag 2000.

In de praktijk hebben de toezichtsonderzoeken betrekking op specifieke feiten (in het geval van klachten), op gevoelige actuele thema's waarvan het Comité I kennis krijgt door het raadplegen van open bronnen (bijvoorbeeld: het bestaan van een interceptiesysteem van het type «Echelon»), of op meer algemene thema's waarvoor de diensten belangstelling hebben, in het bijzonder indien deze thema's verband houden met de wettelijke opdrachten waarmee deze diensten zijn belast krachtens de organieke wet van 30 november 1998 (bijvoobeeld: verdedigen van het economisch potentieel van het land.)

Bij het voeren van deze onderzoeken hoeden het Comité I en zijn Dienst Enquêtes zich ervoor de werking van de Veiligheid van de Staat en de ADIV niet te hinderen. Daarvoor maken ze gebruik van een aantal praktische maatregelen die hen toelaten rekening te houden met de beschikbaarheid van de leden van deze diensten die bij de toezichtsonderzoeken betrokken zijn.

sujets ou questions d'actualité (voir plus loin p. 11: «Les questions posées aux services de renseignement par le Comité R.») Un système de réunions périodiques ou des briefings permettant de mieux suivre les activités des services est également mis progressivement en place.

Pour en revenir aux enquêtes proprement dites, le Comité permanent de contrôle des services de renseignement et son Service d'enquêtes ont eu en traitement, du 1er janvier au 31 décembre 2000, un total de 29 dossiers, dont 15 ont été ouverts au cours de la même période. Parmi ces dernières enquêtes, 10 ont été ouvertes sur initiative du Comité R, 4 à la suite de plaintes de particuliers et 1 à la demande de la commission de suivi du Comité R. Ces enquêtes concernent pour 8 d'entre elles uniquement la Sûreté de l'État et pour 4 d'entre elles uniquement le Service général du renseignement et de la sécurité des Forces armées. Les 3 enquêtes restantes sont relatives à des matières qui relèvent de la compétence des deux services.

À la date de clôture du présent rapport, 14 enquêtes de contrôle, dont certaines d'envergure, sont toujours ouvertes et en traitement, soit que des devoirs sont encore à exécuter par le Service d'enquêtes du Comité R, soit que celui-ci ait transmis les résultats de ses investigations au Comité R qui prépare un rapport destiné, comme l'article 33, 3e alinéa de la loi organique de contrôle le prévoit, aux ministres concernés ainsi qu'à la commission sénatoriale de suivi.

Les rapports d'enquêtes déjà transmis aux ministres de la Justice et de la Défense nationale, ainsi qu'au Sénat sont repris sous le Titre II du présent rapport général d'activités 2000.

Pratiquement les enquêtes de contrôle concernent des faits ponctuels (c'est le cas des plaintes) ou des sujets d'actualité sensibles révélés au Comité R par le suivi des sources ouvertes (comme l'existence d'un système d'interception de type «Échelon») ou encore des thèmes plus généraux intéressant les services et en particulier ceux qui se rapportent aux missions légales qui leur ont été conférées par la loi organique du 30 novembre 1998 (comme la défense du potentiel économique du pays.)

Dans l'exécution de ces enquêtes, le Comité R ainsi que son Service d'enquêtes veillent à ne pas perturber le fonctionnement de la Sûreté de l'État et du SGR en ayant recours à une série de mesures pratiques permettant de tenir compte des disponibilités des membres de ces services concernés par les contrôles.

Voorts wint het Comité I, voor zover zijn middelen dit toelaten, zoveel mogelijk inlichtingen in over de behandelde thema's. Daarvoor doet het eventueel een beroep op externe deskundigen, overeenkomstig artikel 48, § 3 van de bovengenoemde wet van 18 juli 1991.

Tot slot wijzen we erop dat in het kader van sommige toezichtsonderzoeken, de Veiligheid van de Staat tegen het Comité I en tegen zijn Dienst Enquêtes, het geheim van een lopend gerechtelijk onderzoek heeft aangevoerd, ter rechtvaardiging van zijn beslissing geen informatie aan het controleorgaan te bezorgen.

Hierbij beriep de Veiligheid van de Staat zich op artikel 48, § 2 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, dat bepaalt: «De leden van de inlichtingendiensten zijn verplicht geheimen waarvan zij kennis dragen aan het Vast Comité I bekend te maken, behalve indien ze betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek.»

In verband hiermee is het Comité I van mening dat een extensieve interpretatie van een bepaling die slechts een uitzondering wil zijn, die overigens volledig gegrond is, natuurlijk tot gevolg heeft dat het verloop van een toezichtsonderzoek in de praktijk voor onbepaalde tijd wordt belet. Bijgevolg is zulk een interpretatie onverzoenbaar met de filosofie van het controlesysteem dat werd ingevoerd krachtens de bovengenoemde wet tot regeling van het toezicht van 18 juli 1991.

Voorts willen we er op wijzen dat de kennisname door het Comité I en door zijn onderzoekers van precieze feiten die van belang zijn voor een gerechtelijk dossier niet noodzakelijkerwijze onmisbaar is in het kader van een controle *a posteriori* van de doeltreffendheid van de diensten en van de wijze waarop hun onderlinge samenwerking wordt gecoördineerd.

In dit opzicht beveelt het Comité I de inlichtingendiensten aan het geheim van het onderzoek zo nauwkeurig mogelijk te evalueren en in geval van twijfel een beroep te doen op de met het onderzoek belaste magistraat.

Het Comité I behoudt zich hetzelfde recht voor.

2. Gerechtelijke onderzoeken

In tegenstelling tot zijn Dienst Enquêtes geniet het Comité I niet de minste gerechtelijke bevoegdheid.

Artikel 40, lid 3 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten bepaalt dat wanneer de Dienst Enquêtes van het Comité I in deze hoedanigheid handelt, hij niet langer onder het toezicht staat van het Comité I, maar onder het directe toezicht van een parketmagistraat of een onderzoeksrechter.

Pour ce faire également le Comité R s'informe, dans la mesure de ses moyens, de la façon la plus complète possible sur les sujets abordés, en recourant éventuellement à des experts extérieurs, ainsi que l'article 48, § 3 de loi du 18 juillet précitée lui en donne la possibilité.

Il faut signaler enfin qu'à l'occasion de quelques enquêtes de contrôle, la Sûreté de l'État a opposé au Comité R, ainsi qu'à son Service d'enquêtes, le secret d'une instruction judiciaire en cours pour justifier de ne communiquer aucune information à l'organe de contrôle.

Ce faisant, la Sûreté de l'État invoque le § 2 de l'article 48 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement qui indique notamment: «Les membres des services de renseignements sont tenus de révéler au Comité R les secrets dont ils sont dépositaires, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours.»

Le Comité R estime néanmoins que si le principe est totalement fondé, son interprétation extensive est de nature à empêcher dans la pratique et pour un temps indéterminé le déroulement d'une enquête de contrôle et est, dans ce sens, incompatible avec la philosophie du système mis en place par la loi organique du contrôle du 18 juillet 1991 précitée.

Il convient d'ailleurs de souligner que la connaissance par le Comité R, ainsi que par ses enquêteurs, de faits précis intéressant un dossier judiciaire n'est pas nécessairement indispensable dans le cadre d'un contrôle *a posteriori* de l'efficacité des services et de la manière dont la coopération entre ceux-ci s'est coordonnée.

Dans cette optique, le Comité R recommande aux services de renseignement d'évaluer aussi précisément que possible le secret de l'instruction et, en cas de doute, de s'en référer au magistrat titulaire.

Le Comité R se réserve également la même possibilité.

2. Les enquêtes judiciaires

À la différence de son Service d'enquêtes, le Comité R n'a aucune compétence judiciaire.

L'article 40, 3e alinéa de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement prévoit que lorsque le Service d'enquêtes du Comité R agit en cette qualité, il est non plus sous le contrôle du Comité R, mais sous le contrôle direct d'un magistrat du parquet ou d'un juge d'instruction.

Tijdens het voorbije jaar werd de Dienst Enquêtes van het Comité I belast met drie nieuwe gerechtelijke onderzoeken, waarvan er één uitzonderlijk belangrijk.

In het kader van dit onderzoek, geopend in de context van een gerechtelijk onderzoek dat reeds was geopend om een andere reden, werd voor het eerst sinds de inwerkingtreding van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de procedure toegepast die wordt beschreven in artikel 38, § 2 van deze wet.

Krachtens deze procedure kan het hoofd van een inlichtingendienst zich verzetten tegen de gerechtelijke inbeslagneming van geclassificeerde documenten (1).

In het bewuste geval zijn de redenen van dit verzet, genoemd in de kennisgeving die het hoofd van de betrokken dienst krachtens de wet aan de voorzitter van het Comité I bezorgt, de volgende: « de mogelijke inbreuk op de internationale betrekkingen en het mogelijk gevaar voor een natuurlijk persoon (2) ».

Het Comité I zal de evolutie van dit geval (3) blijven volgen in de context van zijn controlebevoegdheden en zal daarover verslag uitbrengen aan het Parlement. Daarnaast stelt zich meer in het algemeen het probleem van de circulatie van de informatie, in het bijzonder van de informatie die wordt geclassificeerd

Au cours de l'année qui vient de s'écouler, le Service d'enquêtes du Comité R a été chargé d'une nouvelle enquête judiciaire particulièrement importante.

Dans le cadre de cette enquête, ouverte dans le contexte d'une instruction judiciaire déjà en cours pour une autre cause, il a été fait, pour la première fois depuis l'entrée en vigueur de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, application de la procédure prévue à l'article 38, § 2 de cette loi.

Cette procédure prévoit pour le chef d'un service de renseignement la possibilité de faire opposition à la saisie judiciaire de documents classifiés (1).

En l'espèce, les raisons de cette opposition mentionnées dans la notification pour information faite en vertu de la loi au président du Comité R par le chef du service concerné, sont les suivantes: « l'atteinte qui pourrait être portée aux relations internationales et le danger pour une personne physique (2) ».

Au-delà du cas d'espèce (3), dont le Comité R ne manquera ni de suivre l'évolution dans le contexte de ses compétences de contrôle ni de faire rapport à ce sujet au Parlement, se pose également de manière plus générale le problème de la circulation des informations, et plus particulièrement de celles qui sont classi-

---

(1) Artikel 38, § 1: De gerechtelijke huiszoekingen en inbeslagnemingen die uitgevoerd worden op de plaatsen waar de leden van inlichtingen- en veiligheidsdiensten hun functie uitoefenen, worden verricht in aanwezigheid van hun korpschef of zijn plaatsvervanger. De korpschef of zijn plaatsvervanger waarschuwt onmiddellijk de bevoegde minister over de uitgevoerde gerechtelijke huiszoekingen en inbeslagnemingen.
§ 2. Indien de korpschef of zijn plaatsvervanger van oordeel is dat de inbeslagneming van de geclassificeerde gegevens en voorwerpen van die aard is dat zij een bedreiging vormt voor de uitoefening van de opdrachten bedoeld in de artikelen 7, 8 en 11, §§ 1 en 2, of dat zij een gevaar meebrengt voor een natuurlijk persoon, waarschuwt hij onmiddellijk de voorzitter van het Vast Comité I en de bevoegde minister. Deze geclassificeerde inbeslaggenomen stukken worden in een verzegelde omslag geplaatst, ondertekend door de korpschef of zijn plaatsvervanger en op een veilige plaats bewaard door de onderzoeksmagistraat. »

(2) We herinneren eraan dat de Dienst Enquêtes van het Comité I in gerechtelijke zaken alleen bevoegd is voor « onderzoeken naar de misdaden en wanbedrijven ten laste van de leden van de inlichtingendiensten (artikel 40, lid 3 van de wet van 18 juli 1991).

(3) In dit stadium is het Comité I echter van mening dat, vóór men zijn toevlucht neemt tot dergelijke geschilprocedures die volgens dit Comité de uitzondering moeten blijven, de samenwerking tussen de diensten, waarvan de wetgever wilde dat ze zo doeltreffend mogelijk zou zijn, onvermijdelijk verloopt, benevens de formele akkoorden die ook onmisbaar zijn, via het op gang brengen van een eerlijke en constructieve dialoog. Zie Titel II, B, hoofdstukken 1 en 3 van dit verslag pagina's 68-86 en volgende.

(1) Article 38, § 1er. Les perquisitions et saisies judiciaires opérées dans les lieux où les membres des services de renseignement et de sécurité exercent leur fonction, s'effectuent en présence de leur chef de corps ou de son remplaçant. Le chef de corps ou son remplaçant avertit sans délai le ministre compétent des perquisitions et saisies judiciaires opérées.
§ 2. Si le chef de corps ou son remplaçant estime que la saisie de données ou matériels classifiés est de nature à constituer une menace pour l'exercice des missions visées aux articles 7, 8 et 11, §§ 1er et 2, ou qu'elle présente un danger pour une personne physique, il en informe immédiatement le président du Comité R et le ministre compétent. Ces pièces classifiées saisies sont mises sous pli scellé, signé par le chef de corps ou son remplaçant et conservé en lieu sûr par le magistrat instructeur... »

(2) Pour rappel, le Service d'enquêtes du Comité R n'est compétent en matière judiciaire que pour « les enquêtes sur les crimes et délits à charge des membres des services de renseignements (article 40, 3e alinéa de la loi du 18 juillet 1991) ».

(3) À ce stade, le Comité R pense toutefois qu'avant d'en arriver à de telles procédures contentieuses, qui doivent lui semble-t-il rester l'exception, la coopération entre les services, que le législateur a voulu aussi efficace que possible, passe nécessairement, au-delà des accords formels indispensables d'autre part, par l'initiation d'un dialogue franc et constructif.

krachtens de wet van 11 december 1998 inzake de classificatie- en de veiligheidsmachtigingen.

In het kader van een ander toezichtsonderzoek waarvan elders sprake in dit algemeen activiteitenverslag heeft het Comité I met betrekking tot het meedelen van informatie aan de gerechtelijke overheden vastgesteld dat, in weerwil van de principes inzake samenwerking en communicatie van de gegevens die de wetgever heeft bekrachtigd in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten(1), er op dit gebied in de praktijk soms nog steeds obstakels bestaan die in de bewuste gevallen verband zouden hebben met de bescherming van de bronnen en vooral met de toepassing door onze inlichtingendiensten van «de regel van de derde of van de derde dienst(2)».

De reële gevoeligheid van de materie en het behoud van de grootst mogelijke efficiëntie van de Belgische inlichtingendiensten, nopen het Comité I tot voorzichtigheid, vóór het uit deze vaststellingen algemene conclusies trekt.

Niettemin is het Comité I de mening toegedaan dat principiële vragen moeten worden gesteld, i.h.b. betreffende de toepassing van «de regel van de derde» door de inlichtingendiensten ten overstaan van de politieke of gerechtelijke nationale overheden.

Meer in het algemeen meent het Comité I dat de bovengenoemde recente wetteksten, die niet alleen de organisatie en de werking van de inlichtingen- en veiligheidsdiensten regelen, maar ook materies zoals de classificatie en de veiligheidsmachtigingen, in de praktijk oplossingen kunnen aanbrengen met het oog op meer en wellicht ook een betere communicatie tussen de inlichtingendiensten en de andere nationale overheden en diensten.

De natuurlijke bestemmelingen van geclassificeerde informatie moeten echter een noodzakelijke basisvoorwaarde naleven. Zij moeten de passende maatregelen nemen om gevolg te geven aan de vereisten van de wet. Vervolgens kunnen ze toegang krijgen tot deze gegevens, teneinde met kennis van zaken de beslissingen te nemen die tot hun domein van bevoegdheid en soevereiniteit behoren. Tegelijk garanderen ze de doeltreffende bescherming die het wettelijk gevolg is van het niveau van classificatie van deze gegevens.

In verband hiermee past het erop te wijzen, in het bijzonder met betrekking tot de gerechtelijke overhefiées en application de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

En ce qui concerne leur communication aux autorités judiciaires, le Comité R a constaté à ce sujet dans deux autres enquêtes de contrôle, dont l'une est publiée dans le présent rapport, que malgré les principes de coopération et de communication des données, affirmés par le législateur dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité(1), des obstacles subsistent parfois en pratique dans ce domaine, qui relèveraient dans les cas d'espèces de la protection des sources et notamment de l'application par nos services de renseignement de «la règle du tiers ou du service tiers(2)».

La réelle sensibilité de la matière et le maintien de la plus grande efficacité possible des services de renseignement belges imposent certes la prudence au Comité R avant de tirer de ces constatations des conclusions générales.

Il considère toutefois que des questions de principe devraient être posées, notamment quant à l'application de «la règle du tiers» par les services de renseignement à l'égard des autorités nationales, qu'elles soient politiques ou judiciaires.

Le Comité R pense d'une manière plus générale que les textes législatifs récents précités, réglant à la fois l'organisation et le fonctionnement des services de renseignement et de sécurité, ainsi que les matières de la classification et des habilitations de sécurité, sont de nature à apporter dans la pratique des solutions à une plus grande et, sans doute, à une meilleure communication entre les services de renseignement et les autres autorités et services nationaux.

Un préalable indispensable consiste cependant pour les destinataires naturels d'informations classifiées que ceux-ci prennent les mesures appropriées pour répondre aux exigences de la loi, et puissent ainsi avoir accès à ces données pour prendre en toute connaissance de cause les décisions propres à leur domaine de compétence et de souveraineté tout en continuant à assurer la protection effective qu'implique légalement le degré de classification de ces données.

Il convient de rappeler à ce propos qu'en ce qui concerne plus précisément les autorités judiciaires, la

---

(1) Artikelen 19 en 20 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

(2) Deze regel beschermt de informatie bezorgd door een derde inlichtingendienst, door te beletten dat deze informatie, zonder de voorafgaande toestemming van de dienst die de informatie heeft bezorgd, wordt doorgespeeld aan andere bestemmelingen.

(1) Articles 19 et 20 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998.

(2) Cette règle protège les informations transmises par un service de renseignement tiers, en empêchant qu'elles soient transmises à d'autres destinataires sans l'autorisation préalable du service qui les a fournies.

den, dat de beperking van toegang tot de diverse geclassificeerde elementen bepaald in artikel 8 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, niet van toepassing is wanneer deze overheden handelen in het kader van hun eigen bevoegdheden.

3. Private inlichtingenondernemingen

Het toezicht van het Comité I strekt zich niet uit over dit type activiteiten, ook al kunnen ze in bepaalde gevallen de activiteiten van de officiële inlichtingendiensten overlappen.

Bijgevolg kan men zich afvragen hoe het staat met het toezicht op de activiteiten van deze private inlichtingenondernemingen, onder de specifieke invalshoek van «de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen», bedoeld in artikel 1 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en de inlichtingendiensten.

Op algemene wijze is het Comité I van mening dat het nodig is rekening te houden met de huidige dimensie van de private inlichtingensector. Aan de activiteiten van deze sector wordt steeds meer belang toegekend, vooral op internationaal niveau en in de economische, industriële en financiële wereld. Ook al zijn deze activiteiten op zich niet onwettelijk(1), de maatschappij en haar verantwoordelijken zijn zich niet steeds even zeer bewust van de risico's en de bedreigingen die ze kunnen vormen.

Er bestaan inderdaad wettelijke bepalingen die het toezicht regelen op sommige van deze sectoren, zoals de wet van 19 juli 1991 tot regeling van het beroep van privé-detective en de wet van 10 april 1990 op de bewakingsondernemingen, de beveiligingsondernemingen en de interne bewakingsdiensten.

Krachtens deze bepalingen moet de minister van Binnenlandse Zaken jaarlijks een schriftelijk verslag overleggen aan de Kamer en de Senaat. Voorts bevat ons intern recht een aantal strafbepalingen om te reageren op mogelijke disfuncties, misbruiken en inbreuken van eender welke aard die op dit gebied zouden worden vastgesteld of onthuld. Bij wijze van voorbeeld, dat representatief is voor de bijzondere

(1) Jérôme Dupré, auteur van een thesis met als titel *«Pour un droit de la sécurité privée de l'entreprise»*, die hij op 3 november 2000 verdedigde aan de Faculteit Rechten van Nice Sophia Antipolis, wijst vooral op de wettelijkheid van de praktijken inzake economische inlichtingen. Hij stelt: *«In tegenstelling tot wat mensen uit de sector denken of wat algemeen wordt aangenomen, sluit de exploitatie van zogenaamde open inlichtingen, d.i. beoefend op grond van toegankelijke informatie, niet uit dat bepaalde rechtsregels worden nageleefd. Anderzijds is de beoefening van «gesloten» inlichtingen niet noodzakelijk onwettelijk.»*

limitation d'accès aux divers éléments classifiés, prévue par l'article 8 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, ne s'applique pas lorsque ces autorités agissent dans le cadre de leurs compétences propres.

3. Les entreprises de renseignement privé (SRP)

Le contrôle du Comité R ne porte pas sur ce type d'activités, bien qu'elles puissent sans doute chevaucher, dans certains cas, celles des services officiels de renseignement.

La question peut dès lors notamment se poser du contrôle des activités de ces entreprises de renseignement privé, sous l'angle spécifique de «la protection des droits que la Constitution et la loi confèrent aux personnes» visée par l'article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

D'une manière générale, le Comité R estime que la dimension actuelle du renseignement privé doit être prise en considération. Les activités de ce secteur, particulièrement au niveau international et dans la sphère économique, industrielle et financière, sont reconnues comme de plus en plus importantes. Bien qu'elles ne soient pas illégales en tant que telles(1), la conscience que l'on peut en avoir au niveau de la société civile et de ses responsables dans les risques et les menaces qu'elles peuvent représenter, n'est pas toujours des plus aiguës.

Il existe certes des dispositions légales qui organisent le contrôle de certains secteurs dans ce domaine comme la loi du 19 juillet 1991 organisant la profession de détective privé et la loi du 10 avril 1990 sur les entreprises de gardiennage, de sécurité et sur les services internes de gardiennage.

Ces dispositions prévoient notamment que le ministre de l'Intérieur fait annuellement un rapport écrit devant les Chambres. Des dispositions pénales existent également dans notre droit interne pour répondre aux éventuels dysfonctionnements, abus et infractions de toute nature qui seraient constatés ou dénoncés dans ce domaine. Ne citons qu'à titre exemplatif et représentatif du domaine particulier qui nous occupe,

(1) Jérôme Dupré, auteur d'une thèse intitulée *«Pour un droit de la sécurité privée de l'entreprise»* soutenue le 3 novembre 2000 à la Faculté de droit de Nice Sophia Antipolis pointe surtout la légalité des pratiques d'intelligence économique. Selon lui: *«contrairement à l'avis des praticiens ou à l'opinion commune, l'exploitation du renseignement dit ouvert, c'est-à-dire pratiqué à partir d'informations accessibles, n'exclut pas le respect de certaines règles de droit. Quant au renseignement fermé, il n'est pas nécessairement illégal»*.

materie die ons bezighoudt, noemen we de wet van 28 november 2000 inzake informaticacriminaliteit.

Door op dit feit de nadruk te leggen meent het Comité I dat het probleem een bijzondere en volgehouden aandacht verdient, niet alleen vanuit de invalshoek van de beperkte middelen waarover onze nationale diensten beschikken in vergelijking met de «concurrentie» van private ondernemingen, die binnen deze sector meestal zijn georganiseerd op een niveau dat de landsgrenzen overschrijdt en die over aanzienlijke financiële middelen beschikken, maar ook en vooral vanuit de invalshoek van de bedreigingen die onze nationale diensten moeten identificeren en die dit type activiteiten zonder betwisting kunnen vormen voor andere actoren van het economisch en wetenschappelijk potentieel van het land.

Nog andere aspecten, zoals het rekruteren of weghalen van leden van de officiële inlichtingendiensten door private inlichtingenondernemingen en de eventuele samenwerking van deze ondernemingen met de officiële diensten, moeten volgens het Comité I eveneens deel uitmaken van een evaluatie en een bezinning (1).

Ter illustratie van deze thema's is het interessant erop te wijzen dat tijdens de conferentie *«Intelligence in the 21st Century»*, die in februari laatstleden in Italië plaatsvond en waaraan Europese en Amerikaanse verantwoordelijken op het gebied van inlichtingen deelnamen, bijzondere aandacht werd besteed aan het probleem van de private inlichtingen. Dit blijkt althans uit het verslag daarover in *«Le Monde du Renseignement»* van 22 februari 2001. Met betrekking tot de samenwerking tussen de officiële en private diensten lezen we onder meer: *«De publieke beslissingnemers erkennen dat deze samenwerking stilvalt wanneer de opdrachten betrekking hebben op heel gevoelige en globale zaken, in het kader waarvan alleen die agenten kunnen optreden die een band hebben met hun regering. Anderzijds staan de private ondernemingen die wereldwijd onderzoeken voeren, aan het hoofd van een geheel van netwerken van lokale inspecteurs, die meestal uit de inlichtingendiensten van de betrokken landen afkomstig zijn.»* Met betrekking tot economische inlichtingen schaart het Comité I zich achter de conclusie van de analyse van de Canadese onderzoeker Gregory Treverton, die in hetzelfde artikel wordt geciteerd: *«De cultuur van de geheime diensten blijkt voorgoed niet langer te zijn*

(1) Artikel 16, § 2, lid één van de wet van 19 juli 1991 tot regeling van het beroep van privé-detective regelt al een vorm van samenwerking met bepaalde overheden, aangezien de privé-detective zonder verwijl gevolg moet geven aan het verzoek om inlichtingen van de minister van Binnenlandse Zaken, van de minister van Justitie of van de gerechtelijke overheden over een uitgevoerde of lopende opdracht, wanneer deze inlichtingen nodig zijn voor de nationale veiligheid, de handhaving van de openbare orde en voor het voorkomen of opsporen van strafbare feiten.

la loi du 28 novembre 2000 relative à la criminalité informatique.

En soulignant ce fait, le Comité R estime que sous cet éclairage, le problème mérite une attention et une réflexion particulières et soutenues non seulement sous l'angle des moyens limités dont nos services nationaux disposent face à la «concurrence» d'entreprises privées, organisées le plus souvent dans ce secteur au niveau transnational et disposant de moyens financiers considérables, mais également et surtout sous l'angle des menaces qu'ils sont chargés d'identifier et que peut sans conteste représenter ce type d'activités pour d'autres acteurs du potentiel économique et scientifique du pays.

D'autres aspects comme celui du recrutement voire du débauchage par des entreprises privées de renseignement de membres des services de renseignement officiels et de la collaboration éventuelle de ces entreprises avec ces mêmes services doivent pour le Comité R faire également partie d'une évaluation et d'une réflexion (1).

Pour illustrer ces thèmes, il est intéressant de signaler que lors de la conférence *«Intelligence in the 21st Century»* qui s'est tenue en Italie en février dernier, et qui rassemblait des responsables européens et américains du renseignement, le problème de l'intelligence privée a particulièrement retenu l'attention, du moins aux termes du compte rendu qu'en fait le périodique *«Le Monde du Renseignement»* dans sa livraison du 22 février 2001. On peut y lire notamment en ce qui concerne la collaboration entre les services officiels et privés: *«Les décideurs publics reconnaissent que ces collaborations cessent dès lors que les missions portent sur des sujets très sensibles et globaux: ceux sur lesquels seuls les agents tenus par des liens avec leur gouvernement peuvent intervenir. À l'inverse, les sociétés privées qui mènent des investigations à l'échelle de la planète se trouvent à la tête d'une imbrication de réseaux d'enquêteurs locaux, issus le plus souvent des services de renseignement des pays concernés.»* En ce qui concerne d'autre part le renseignement économique, le Comité R retient également la conclusion de l'analyse faite par le chercheur canadien Gregory Treverton, qui est citée dans le même article: *«La culture des services secrets se révèle définitivement inadaptée aux événements qui marquent*

(1) L'article 16, § 2, premier alinéa, de la loi du 19 juillet 1991 organisant la profession de détective privé prévoit déjà une forme de collaboration avec certaines autorités puisque le détective privé est tenu de répondre sans délai à la demande de renseignements du ministre de l'Intérieur, du ministre de la Justice ou des autorités judiciaires concernant une mission en cours ou exécutée, lorsque ces renseignements sont nécessaires à la sûreté nationale, au maintien de l'ordre public et à la prévention ou la recherche de faits punissables.

aangepast aan de belangrijke gebeurtenissen in het zakenleven. Gevoelige economische informatie vereist geen buitensporige clandestiniteit, maar veeleer adresboekjes van hoog niveau, behandeld door vakmensen met gevoel voor tempo. Als gevolg hiervan zou er een afscheiding komen tussen het economische inlichtingenwezen en het door de staat georganiseerde inlichtingenwezen.» (Zie Titel II — Hoofdstuk 7, blz. 116: «Verslag van het onderzoek naar de manier waarop de veiligheid van de staat zich kwijt van haar nieuwe opdracht inzake de bescherming van het wetenschappelijk of economisch potentieel van het land» en hoofdstuk 2, blz. 61 «Verslag van het onderzoek naar de wijze waarop de inlichtingendiensten gereageerd hebben op eventuele spionagefeiten of pogingen tot binnendringen in het informaticacentrum van een Belgisch onderzoekscentrum.»)

4. Het toezicht op het informatiebeheer

Op verzoek van het kabinet van de minister van Justitie heeft de subwerkgroep III «Beheer & Toezicht van de Informatie» op 13 oktober 2000 de voorzitter van het Comité I gehoord. Dit gebeurde in het kader van de politiehervorming.

De voorzitter van het Comité I heeft van de gelegenheid gebruik gemaakt om het standpunt van dit Comité naar voren te brengen. Dit standpunt luidt als volgt:

«Het Vast Comité I is van mening dat het als controleorgaan van de inlichtingendiensten bevoegd is om zijn bevoegdheden in de praktijk uit te oefenen op het gebied van het beheer van de informatie door deze diensten.»

«Het past echter te benadrukken dat dit toezicht extern is en dat het slechts *a posteriori* kan plaatsvinden, op bepaalde momenten en ter gelegenheid van een administratief onderzoek.»

«De Dienst Enquêtes van het Vast Comité zou in het kader van zijn gerechtelijke bevoegdheid en onder het toezicht van een magistraat en niet van het Comité, kunnen tussenkomen indien strafrechtelijke inbreuken worden begaan inzake het beheer van de informatie door leden van de inlichtingendiensten.»

«De onderstaande beschouwingen illustreren de praktische domeinen waarop het beheer van de informatie tegelijk betrekking heeft op de inlichtingendiensten, de politiediensten en de gerechtelijke overheden.»

«De opdrachten die de wet van 30 november 1998 houdende regeling van de inlichtingen- en de veiligheidsdiensten (*Belgisch Staatsblad* van 18 december 1998) aan de Veiligheid van de Staat toekent, hebben betrekking op domeinen zoals criminele organisaties, het terrorisme, schadelijke sektarische organisaties, het extremisme. De Algemene Dienst Inlichting en

la vie des affaires. Les informations économiques sensibles ne nécessitent pas des débauches de clandestinité, mais plutôt des carnets d'adresse de haut niveau, manipulés par des professionnels qui ont le sens du tempo. Un tel état des lieux conduirait donc à isoler le renseignement économique du renseignement étatique.» (voir Titre II — chapitre 7 du présent rapport: «Rapport de l'enquête sur la manière dont la Sûreté de l'État s'acquitte de sa nouvelle mission de protection du potentiel scientifique et économique» p. 109 et le chapitre 2: «Rapport de l'enquête sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge» p. 58).

4. Le contrôle de la gestion de l'information

Le président du Comité R a été entendu à la demande du cabinet du ministre de la Justice, le 13 octobre 2000, par le sous-groupe de travail III — Gestion & Contrôle de l'information, dans le cadre de la réforme des polices.

Il a fait valoir à cette occasion le point de vue du Comité R qui est reproduit ci-après.

«Le Comité permanent R estime qu'en sa qualité d'organe de contrôle des services de renseignement, il est bien habilité à exercer en pratique ses compétences dans le domaine de la gestion de l'information par ces services.»

«Il convient de souligner toutefois que ce contrôle est externe et qu'il ne peut s'exercer qu'*a posteriori*, de manière ponctuelle et à l'occasion d'une enquête de nature administrative.»

«Le Service d'enquêtes du Comité permanent pourrait, dans le cadre de sa compétence judiciaire et sous le contrôle non plus du comité mais d'un magistrat, intervenir si des infractions pénales étaient commises en matière de gestion de l'information par des membres des services de renseignement.»

«Les considérations qui suivent illustrent les domaines pratiques dans lesquels la gestion de l'information concerne à la fois les services de renseignement, les services de police et les autorités judiciaires.»

«Les missions attribuées par la loi du 30 novembre 1998, organique des services de renseignement et de sécurité (*Moniteur belge* du 18 décembre 1998) à la Sûreté de l'État visent des domaines comme les organisations criminelles, le terrorisme, les organisations sectaires nuisibles, l'extrémisme. Le Service général du renseignement et de la sécurité a également en

Veiligheid is eveneens belast, in het kader van zijn wettelijke opdrachten, met opdrachten die betrekking kunnen hebben op de strijd tegen deze verschillende ernstige vormen van criminaliteit.»

«In deze sectoren impliceert de samenwerking met de politiediensten en de gerechtelijke overheden, die overigens wordt opgelegd door artikel 20 van de bovengenoemde wet, natuurlijk dat er informatie wordt uitgewisseld, hetgeen dan weer wordt beoogd in artikel 44/1 van de wet op het politieambt(1).»

«Voorts wijzen we erop dat de inlichtingendiensten overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen de opdracht hebben veiligheidsonderzoeken uit te voeren. Ook in dit kader is de toegang tot inlichtingen van de politiediensten van toepassing.»

«Binnen de beperkingen die voor het overige hierboven worden beschreven, wordt de rol van het Comité I in het kader van de toepassing van artikel 44 pas duidelijk wanneer een inlichtingendienst betrokken is bij het beheer van de informatie en indien er «redenen zijn om te geloven dat de bevoegdheden inzake toezicht van het Comité I toepassing vinden.»

«Ook al is dit extern toezicht marginaal, toch bekleedt het een belangrijk aanvullend karakter in de mate waarin er op het niveau van de inlichtingendiensten geen intern toezicht bestaat van dezelfde aard als het toezicht voorzien door artikel 44/7 van de wet op het politieambt(2).»

«Terloops is er reden om op te merken dat in toepassing van artikel 53 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, de Comités P en I gezamenlijke toezichtsonderzoeken kunnen verrichten, i.h.b. met betrekking tot de taakverdeling en de coördinatie van de werking tussen de politiediensten enerzijds en de inlichtingendiensten anderzijds.»

«Concreet en in de mate waarin het betrokken is, schaart het Comité I zich achter de standpunten van het Comité P in dezelfde context, te weten:

(1) Artikel 44/1. Bij het vervullen van de opdrachten die hun zijn toevertrouwd, kunnen de politiediensten gegevens van persoonlijke aard en inlichtingen inwinnen en verwerken, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een concreet belang vertonen voor de uitoefening van hun opdrachten van bestuurlijke politie en voor de uitoefening van hun opdrachten van gerechtelijke politie overeenkomstig de artikelen 28*bis*, 28*ter*, 55 en 56 van het Wetboek van strafvordering.

(2) Artikel 44/7, lid 1: «Er wordt een controleorgaan opgericht onder het gezag van de minister van Binnenlandse Zaken en van de minister van Justitie, belast met de controle van het beheer van de algemene nationale gegevensbank bedoeld in artikel 44/4, eerste lid. Dit controleorgaan heeft een onbeperkt recht op toegang tot alle inlichtingen en gegevens bewaard in deze gegevensbank.»

charge pour sa part, dans le cadre de ses missions légales, des missions qui peuvent intéresser la lutte contre ces différentes formes graves de criminalité.»

«Dans ces secteurs, la coopération avec les services de police et les autorités judiciaires, coopération imposée d'ailleurs par l'article 20 de la loi précitée, implique bien évidemment l'échange d'informations, qui est d'autre part visé par l'article 44/1 de la loi sur la fonction de police(1).»

«Il faut également mentionner que les services de renseignement se voient conférer par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, la mission de réaliser les enquêtes de sécurité. Dans ce cadre également l'accès aux renseignements policiers est d'application.»

«Dans les limites qui pour le surplus ont été précisées ci-dessus, le rôle du Comité R dans le cadre de l'application de l'article 44 ne se conçoit que lorsqu'un service de renseignement est concerné par la gestion de l'information et qu'il y a des raisons de penser que les compétences de contrôle du Comité R trouvent à s'appliquer.»

«Bien que marginal, ce contrôle externe revêt toutefois un caractère complémentaire important dans la mesure où il n'existe pas au niveau des services de renseignement un contrôle interne de la même nature que celui prévu par l'article 44/7 de la loi sur la fonction de police(2).»

«Il y a lieu de rappeler incidemment qu'en application de l'article 53 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, les Comités P et R peuvent réaliser des enquêtes communes de contrôle notamment pour ce qui concerne la répartition des missions et la coordination du fonctionnement entre, d'une part, les services de police et, d'autre part, les services de renseignement.»

«Concrètement et dans la mesure où il est concerné, le Comité R rencontre les points de vue exprimés par le Comité P dans le même contexte, à savoir:

(1) Article 44/1. Dans l'exercice des missions qui leur sont confiées, les services de police peuvent recueillir et traiter des données à caractère personnel et des informations relatives notamment à des événements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative et pour l'exécution de leurs missions de police judiciaire conformément aux articles 28*bis*, 28*ter*, 55 et 56 du Code d'instruction criminelle.

(2) Article 44/7 , 1er alinéa: «Il est créé un organe de contrôle sous l'autorité du ministre de l'Intérieur et de la Justice, chargé du contrôle de la gestion de la banque de données nationale générale visée à l'article 44/4, alinéa 1er. Cet organe de contrôle a un accès illimité à toutes les informations et les données conservées dans cette banque de données.»

1. de vraag naar een uitwisseling van informatie tussen het intern controleorgaan en het Vast Comité I in zijn hoedanigheid van extern orgaan van toezicht, zowel met betrekking tot de mogelijke klachten als de vastgestelde disfuncties waarbij de inlichtingen- en veiligheidsdiensten betrokken zijn;

2. het concretiseren van deze samenwerking en deze uitwisseling van informatie met het intern controleorgaan door middel van een protocolakkoord.»

1. la demande d'un échange d'informations entre l'organe de contrôle interne et le Comité permanent R en sa qualité de contrôleur externe, visant aussi bien les plaintes éventuelles que les dysfonctionnements constatés impliquant les services de renseignement et de sécurité;

2. la concrétisation de cette collaboration et de cet échange de renseignements avec l'organe de contrôle interne au moyen d'un protocole d'accord.»

HOOFDSTUK 2

VRAGEN GESTELD DOOR HET COMITE I AAN DE INLICHTINGENDIENSTEN

Benevens de onderzoeken die het voert op verzoek van het Parlement of van een van de bevoegde ministers of uit eigen beweging, meende het Comité I dat zijn wettelijke bevoegdheden dit Comité ook toelieten regelmatig de verantwoordelijken van de inlichtingendiensten te ondervragen over het een of andere thema dat deze diensten behandelen.

Het betreft een soepeler en informeler manier van toezicht houden, die geen aanleiding geeft tot een onderzoeksopdracht noch tot enige controle ter plaatse. Dergelijke uitwisselingen laten het Comité I echter toe zonder veel formaliteiten op de hoogte te blijven van de prioriteiten op een welbepaald ogenblik en over de manier waarop de inlichtingendiensten een welbepaalde materie behandelen.

De vragen worden per post verzonden of worden mondeling gesteld tijdens ontmoetingen en gedachtewisselingen die van tijd tot tijd worden georganiseerd met de verantwoordelijken van de inlichtingendiensten.

Aan sommige vragen en aan sommige antwoorden die het Comité I ontving, werd een classificatieniveau «vertrouwelijk» of zelfs «geheim» toegekend in de zin van de wet d.d. 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen. Dit betekent dat het Comité I daarvan niet integraal kennis mag geven in een rapport dat voor publicatie is bestemd.

Het Comité I biedt hier een samenvatting van vragen die het in het jaar 2000 heeft gesteld en van de niet-geclassificeerde antwoorden daarop die het van de inlichtingendiensten heeft ontvangen.

Sommige van de vragen en antwoorden die het Comité I in 2000 behandelde, komen niet voor in dit rapport, omdat het onderzoek nog niet volledig is afgerond. Deze hangende zaken worden besproken in een volgend activiteitenverslag.

CHAPITRE 2

QUESTIONS POSÉES AUX SERVICES DE RENSEIGNEMENT PAR LE COMITÉ R

Outre les enquêtes qu'il mène à la demande du Parlement, d'un des ministres compétents ou de sa propre initiative, le Comité R a estimé que ses compétences légales l'autorisaient à questionner régulièrement les responsables des services de renseignement sur l'un ou l'autre sujet traité par ces services.

Il s'agit d'un mode de contrôle plus souple et informel, qui ne donne lieu à aucun devoir d'enquête ni à aucune vérification sur place. Ces échanges permettent toutefois au Comité R de se tenir sommairement informé sur les priorités du moment et sur la manière dont les services de renseignement traitent une matière déterminée.

Les questions sont posées, soit par courrier, soit oralement au cours de rencontres et d'échanges de vues organisés périodiquement avec les responsables des services de renseignement.

Un niveau de classification « confidentiel « ou même « secret « au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a été attribué à certaines questions ainsi qu'à certaines réponses données au Comité R, ce qui ne lui permet donc pas d'en donner connaissance intégrale dans un rapport destiné à être publié.

Le Comité R présente donc ici un résumé de questions qu'il a posées et auxquelles des réponses non classifiées ont été données par les services de renseignement au cours de l'année 2000.

Certaines questions et réponses traitées en 2000 ne sont pas reprises dans le présent rapport à défaut pour le Comité R d'avoir complètement vidé le sujet. Ces problèmes en suspens seront exposés dans un prochain rapport d'activités.

1. Voetbalkampioenschap «Euro2000» — Evaluatie door de Veiligheid van de Staat van de bedreigingen die sommige extremistische supporters van voetbalclubs kunnen vormen tijdens hun verblijf in België

Een artikel met als titel *«L'ombre d'Arkan plane sur l'Euro 2000»* («De geest van Arkan hangt boven Euro 2000»), dat verscheen in het tijdschrift *Courrier International* nr. 483 van 3 tot 9 februari 2000, heeft de aandacht van het Comité I getrokken.

Het is bekend dat ook in België extreem-rechtse elementen infiltreren in clubs van voetbalsupporters.

Op 15 februari 2000 stelde het Comité I de volgende vragen aan de Veiligheid van de Staat:

— Is het in het artikel beschreven gevaar reëel?

— Heeft de Veiligheid van de Staat dit probleem onderzocht?

— Heeft ze verslagen over het probleem opgesteld?

— Aan wie zou ze deze verslagen hebben bezorgd?

— Houdt de Veiligheid van de Staat bepaalde Belgische supportersclubs in het oog?

Antwoord van de Veiligheid van de Staat
(brief van 28 februari 2000)

Samengevat:

In het kader van haar opdrachten beschreven in de artikelen 7 en 8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, i.h.b. op het vlak van extremisme of terrorisme, besteedt de Veiligheid van de Staat aandacht aan sommige Belgische supportersclubs (hooligans *lato sensu*) van voetbalploegen.

Er werden inderdaad al extremistische uitspattingen vastgesteld bij personen die tot bepaalde clubs behoren en die niet veraf staan van bewegingen van nationalistisch-revolutionaire strekking.

Met uitzondering van verbale beledigingen door toeschouwers aan het adres van sommige voetballers met een andere huidskleur en het opduiken van nationalistische symbolen zoals Keltische kruisen, werd België tot op heden nog niet geconfronteerd met een golf van extremisme vergelijkbaar met wat men in Italië heeft meegemaakt, waar georganiseerde groepen enorme spandoeken ontrolden ter verheerlijking van een of andere figuur van extreem-rechtse strekking (Arkan, Mussolini).

In februari 2000 onderzocht de Veiligheid van de Staat echter de mogelijkheid dat georganiseerde groe-

1. Tournoi de football «Euro 2000» — Évaluation par la Sûreté de l'État des menaces que certains supporters extrémistes de clubs de football peuvent faire courir lors de leur séjour en Belgique

Un article intitulé «L'ombre d'Arkan plane sur l'Euro 2000» paru dans la revue *Courrier International* nº 483 du 3 au 9 février 2000 a attiré l'attention du Comité R.

Il est bien connu que, même en Belgique, des éléments d'extrême droite infiltrent des clubs de supporters de football.

Le 15 février 2000, le Comité R a posé les questions suivantes à la Sûreté de l'État:

— le danger évoqué par l'article est-il réel?

— la Sûreté de l'État a-t-elle examiné ce problème?

— a-t-elle produit des rapports sur la question?

— à qui les aurait-elle transmis?

— la Sûreté de l'État surveille-t-elle certains clubs belges de supporters?

Réponse de la Sûreté de l'État
(lettre du 28 février 2000)

Résumé:

Dans le cadre de ses missions énumérées aux articles 7 et 8 de la loi organique du 30 novembre 1998 relative aux services de renseignement et de sécurité et liées notamment à l'extrémisme ou au terrorisme, la Sûreté de l'État s'intéresse à certains clubs belges de supporters (hooligans *lato sensu*) d'équipes de football.

En effet des dérives extrémistes ont pu être mises en évidence parmi des personnes appartenant à certains clubs et qui sont proches de mouvements de tendance nationaliste-révolutionnaire.

Si l'on excepte les injures verbales par des spectateurs à l'encontre de certains joueurs de football en raison de la couleur de leur peau et l'apparition de symboles nationalistes, comme des croix celtiques, la Belgique ne connaît pas, jusqu'à présent, un déferlement extrémiste comparable à celui qu'a connu l'Italie, où des groupes organisés ont déroulé des banderoles géantes à la gloire de l'un ou l'autre personnage lié à la mouvance extrémiste de droite (Arkan, Mussolini).

Au mois de février 2000, la Sûreté de l'État examinait cependant l'éventualité que des groupements

peringen extreem-rechtse of Joegoslavische hooligans van Euro 2000 wilden profiteren om actie te voeren.

De Veiligheid van de Staat stelde echter vast dat in België afwijkend gedrag ter zake veeleer het werk was van individuen, ten hoogste van kleine groepjes.

In voorbereiding op Euro 2000 is er een samenwerking tot stand gekomen tussen de Veiligheid van de Staat en de rijkswacht. Deze laatste bezorgde regelmatig gegevens over de extremistische aard van de hooligans in de voetbalstadions aan de Veiligheid van de Staat.

Een specifieke nota over dit probleem werd tegelijk gericht aan de ministers van Justitie en van Binnenlandse Zaken, aan de Nationale Magistraat en aan de Algemene Rijkspolitie (ARP).

2. De mogelijke rol van de inlichtingendiensten bij de evaluatie van economische sancties opgelegd aan sommige landen

Zoals blijkt uit twee parlementaire interpellaties op 7 juni 2000 in de Commissie Buitenlandse Betrekkingen van de Kamer van Volksvertegenwoordigers (1), stellen NGO's regelmatig vragen naar de doeltreffendheid van de internationale sancties die tegen sommige landen worden uitgesproken (Irak, Joegoslavië, enz.).

Het Comité I vroeg zich af of de inlichtingendiensten, in het kader van hun opdrachten, nuttige informatie hierover bezorgen of kunnen bezorgen aan de regering.

Op 23 juni 2000 stuurde het Comité I een brief in deze zin naar de verantwoordelijken van de Veiligheid van de Staat en van de ADIV:

«Houdt uw dienst in het kader van zijn opdrachten toezicht op de toepassing van de economische sancties die de internationale gemeenschap tegen een land uitspreekt?

Verzamelt en analyseert uw dienst informatie betreffende de gevolgen van een dergelijk embargo (militaire gevolgen, gevolgen op het vlak van de Veiligheid, voor de burgerbevolking, voor de economie, voor de internationale betrekkingen, enz.)?

Zo ja, over welke landen in het bijzonder? Aan wie worden deze eventuele verslagen bezorgd? Bent u van mening dat uw dienst al dan niet bevoegd is om dit soort gegevens te verzamelen, te analyseren en aan de politieke beslissingnemers te bezorgen?».

(1) *Cf.* Commissie buitenlandse betrekkingen, 7 juni 2000 — COM 224.

organisés d'hooligans d'extrême droite ou yougoslaves cherchent à profiter du tournoi Euro 2000 pour mener des actions.

Elle notait toutefois qu'en Belgique, les comportements déviants en la matière semblaient davantage le faits d'individus, tout au plus de groupuscules.

En préparation de l'Euro 2000, une coopération s'est établie entre la Sûreté de l'État et la gendarmerie, celle-ci transmettant régulièrement à la première des données sur le caractère extrémiste des hooligans dans les stades de football.

Une note spécifique sur cette question a été adressée à la fois aux ministres de la Justice et de l'Intérieur, au Magistrat national et à la Police générale du Royaume (PGR).

2. Le rôle éventuel des services de renseignement dans l'évaluation des sanctions économiques appliquées à certains pays

Comme en témoignent deux interpellations parlementaires posées le 7 juin 2000 en commission des relations extérieures de la Chambre des représentants (1), la question de l'efficacité des sanctions internationales prononcées à l'encontre de certains pays (Irak, Yougoslavie, etc.) est régulièrement posée par des ONG.

Le Comité R s'est demandé si, dans le cadre de leurs missions, les services de renseignement apportaient ou étaient susceptibles d'apporter des informations utiles au gouvernement sur ce sujet.

Il a adressé une lettre en ce sens aux responsables de la Sûreté de l'État et du SGR le 23 juin 2000:

«Dans le cadre de ses missions, votre service surveille-t-il l'application des sanctions économiques prononcées par la communauté internationale contre un pays?

Recueille-t-il et analyse-t-il des informations en rapport avec les effets d'un tel embargo (du point de vue militaire, sur la sécurité, sur la population civile, sur l'économie, sur les relations internationales, etc.)?

Si oui, à propos de quels pays en particulier? A qui ces rapports éventuels ont-ils été transmis? Estimez-vous que votre service est compétent, ou non, pour recueillir ce type d'information, l'analyser et la transmettre aux décideurs politiques?»

(1) *Cf.* Commission des relations extérieures, 7 juin 2000 — COM 224.

Antwoord van de ADIV (brief van 10 juli 2000)

Samengevat:

De organieke wet van november 1998 stelt de opdrachten van de militaire inlichtingendienst vast. De doeltreffendheid van de internationale sancties behoort op zich niet tot de zaken die deze dienst opvolgt.

De militaire situatie, de Veiligheid, de binnenlandse en buitenlandse politiek van sommige landen worden gevolgd voor zover dit wordt voorzien in het richtplan Inlichtingen van de Strijdkrachten.

Dit document stelt de prioriteiten van de ADIV vast. Gelet op zijn opdrachten en zijn beperkte middelen is het voor de ADIV niet mogelijk de doeltreffendheid van internationale sancties van nabij te volgen.

Indien de informatie waarover de dienst in verband hiermee beschikt ook betrekking heeft op de Veiligheid van de Belgische militairen, brengt de ADIV de overheden daarvan op de hoogte (de Eerste minister, de minister van Buitenlandse Zaken, de minister van Landsverdediging en de Veiligheid van de Staat).

Réponse du SGR (lettre du 10 juillet 2000)

Résumé:

La loi organique de novembre 1998 prévoit les missions du service militaire de renseignement. L'efficacité des sanctions internationales n'est pas en soi un sujet suivi par ce service.

La situation militaire, la sécurité, la politique intérieure et extérieure de certains pays sont suivies pour autant qu'ils soient repris dans le plan directeur du renseignement des Forces Armées.

Ce document définit les priorités du SGR. Vu ses missions et ses moyens limités, le SGR n'a cependant pas la possibilité de suivre l'efficacité des sanctions internationales de près.

Si les informations dont le service dispose à ce sujet concernent aussi la sécurité des troupes militaires belges, le SGR en fait part aux autorités (Premier ministre, ministre des Affaires étrangères, ministre de la Défense nationale et la Sûreté de l'État).

Antwoord van de Veiligheid van de Staat (brief van 27 juli 2000)

Samengevat:

Het opvolgen van de toepassing van internationale sancties die tegen sommige landen worden getroffen, maakt geen deel uit van de opdrachten waarmee de wetgever de Veiligheid van de Staat heeft belast.

Hoewel deze dienst dus niet op algemene en systematische wijze inlichtingen in verband hiermee verzamelt, kan het gebeuren dat hij in het kader van zijn wettelijke opdrachten relevante informatie produceert.

Zo neemt de Veiligheid van de Staat deel aan de interministeriële werkgroep *«Task Force Diamant»*, sinds de Verenigde Naties hun embargo hebben uitgebreid tot de diamanthandel waarvan de opbrengsten worden gebruikt om de UNITA in Angola te financieren.

De Veiligheid van de Staat stelt ook verslagen op over luchtvervoermaatschappijen die ervan worden verdacht het luchtembargo van de Verenigde Naties en de Europese Unie tegen ex-Joegoslavië niet te respecteren.

Op het vlak van proliferatie besteedt de Veiligheid van de Staat aandacht aan de uitvoer van materieel, producten, goederen en knowhow die een land dat onder een embargo gebukt gaat kan gebruiken om niet-conventionele of heel gesofisticeerde wapens te vervaardigen. Deze inlichtingen worden aan de bevoegde overheden bezorgd.

Réponse de la Sûreté de l'État (lettre du 27 juillet 2000)

Résumé:

Le suivi de l'application des sanctions internationales imposées à certains pays ne fait pas partie des missions que le législateur a attribuées à la Sûreté de l'État.

Bien que ce service ne recueille donc pas de manière globale et systématique de renseignements à ce sujet, il se peut néanmoins que dans le cadre de ses missions légales, il génère de l'information pertinente.

Ainsi par exemple, la Sûreté de l'État participe au groupe de travail interministériel *«Task Force Diamant»* depuis que les Nations Unies ont étendu leur embargo au commerce des diamants destiné à financer l'UNITA en Angola.

La Sûreté de l'État rédige aussi des rapports concernant des firmes de transport aérien suspectées de ne pas respecter l'embargo aérien décrété par les Nations Unies et l'Union européenne à l'encontre de l'ex-Yougoslavie.

En matière de prolifération, la Sûreté de l'État est attentive aux exportations de matériel, de produits, de marchandises et de savoir-faire qui peuvent aider un pays soumis à embargo à produire de l'armement non-conventionnel ou très sophistiqué. Ces renseignements sont transmis aux autorités compétentes.

3. Vragen gesteld in het kader van een opvolging van het onderzoek naar de deelname van de Belgische inlichtingendienstenaansatellietprogramma'sop het vlak van inlichtingen

3.1. Toegang van de ADIV tot de satellietbeelden

Bij het afsluiten van zijn onderzoek in 1998 naar het deelnemen van de Belgische inlichtingendiensten aan satellietprogramma's op het vlak van inlichtingen(1), was het Comité I van mening dat de ADIV rechtstreeks en autonoom toegang moest kunnen hebben tot satellietbeelden als aanvullende informatiebron, vooral met het oog op het ondersteunen van operaties waarbij België alleen optreedt en beslissingen neemt in een nationaal kader.

Het Comité I keurde dan ook goed dat de toenmalige minister van Landsverdediging onderhandelingen had aangeknoopt met de Franse regering met het oog op een Belgische deelname aan het Europese Helios II-programma.

In oktober 1998 echter besliste de beperkte ministerraad daar niet mee voort te gaan, rekening houdend met de te hoge kosten voor het budget van Landsverdediging. Deze beslissing kon echter worden herzien bij het voltooien van het nieuwe investeringsplan van Landsverdediging.

Op diezelfde ministerraad werd beslist een nationaal centrum voor de interpretatie van satellietbeelden op te richten, dat zou afhangen van de generale staf van het leger. Voorts kreeg een comité, met vertegenwoordigers van de vier betrokken ministeries — d.i. Landsverdediging, Wetenschapsbeleid, Economie en Buitenlandse Zaken —, de opdracht de ontwikkelingen te volgen op het gebied van observatiesatellieten, teneinde aan de regering alternatieve oplossingen te kunnen voorstellen.

Het Comité I heeft de nieuwe minister van Landsverdediging de vraag gesteld om te weten of de werkzaamheden van het voornoemd Interministerieel Comité werden voortgezet en te vernemen hoe ver men gevorderd is.

Het Comité I heeft ook de ADIV ondervraagd om te weten te komen hoe ver de strijdkrachten staan met het oprichten van de cel voor het analyseren van satellietbeelden.

(1) *Cf.* Activiteitenverslag Comité 1998, Hfd. 5, p. 140.

3. Questions posées dans le cadre d'un suivi de l'enquêtesurlaparticipationdesservicesderenseignement belges à des programmes satellitaires de renseignement

3.1. L'accès du SGR aux images satellitaires

A l'issue de son rapport d'enquête menée en 1998 sur la participation des services de renseignement belges à des programmes satellitaires de renseignement(1), le Comité R était d'avis que le SGR devait pouvoir disposer d'un accès direct et autonome à des images satellitaires comme source complémentaire d'informations, surtout pour le soutien à des opérations où la Belgique agit et prend ses décisions seule dans un cadre national.

Le Comité R avait dès lors approuvé les négociations que l'ancien ministre de la Défense nationale avait entreprises auprès du gouvernement français en vue de faire participer la Belgique au programme européen Hélios II.

Cependant, en octobre 1998, le Conseil des ministres restreint a pris la décision de ne pas poursuivre ces démarches vu le coût trop élevé qui en résulterait pour le budget de la Défense nationale.

Cette décision était toutefois susceptible d'être revue lors de la finalisation du nouveau plan des investissements de la Défense nationale. Ce même Conseil des ministres a aussi décidé la création d'un centre national d'interprétation d'images satellitaires qui devra dépendre de l'État-major général de l'armée. Par ailleurs, un comité, réunissant des représentants des quatre départements concernés, à savoir la Défense nationale, la Politique scientifique, l'Economie et les Affaires étrangères, a été chargé de suivre l'évolution dans le domaine des satellites d'observation afin de pouvoir présenter des solutions alternatives au gouvernement.

Le Comité R a questionné le nouveau ministre de la Défense nationale pour savoir si les travaux du comité interdépartemental en charge de cette affaire se poursuivaient et pour en connaître l'état d'avancement.

Le Comité R a aussi questionné le SGR pour savoir à quel stade en était l'installation de la cellule d'analyse d'images satellitaires auprès des forces armées.

(1) *Cf.* Rapport d'activités Comité R — 1998, Chapitre 5, p. 130.

Antwoord van de ADIV
(uitvoerige briefing van 11 februari 2000)

Samengevat:

Na de beslissing van de regering in oktober 1998, is er toch nog informeel contact geweest tussen vertegenwoordigers van Landsverdediging en de Franse overheden, om te onderzoeken of er voor België alternatieve mogelijkheden bestonden om deel te nemen aan het programma Helios II.

Zes formules van partnership werden bestudeerd, gaande van de volledige deelname aan het programma voor een bedrag van 2,8 miljard frank tot de aankoop van beelden volgens de specifieke behoeften van de Belgische strijdkrachten (± 1,2 miljoen frank per foto).

Ook de verschillende mogelijkheden om beelden te verkrijgen bij andere, eventueel commerciële leveranciers, werden onderzocht.

Na de voor- en nadelen van de verschillende mogelijkheden tegen elkaar te hebben afgewogen, meende de ADIV dat de beste oplossing erin bestond operationeel deel te nemen aan het programma Helios II. Dit was echter ook de duurste oplossing.

Daarnaast werd het Belgisch centrum voor de interpretatie van satellietbeelden vanaf december 1999 geleidelijk geïnstalleerd. Het ressorteert onder de ADIV en zou in september 2001 volledig operationeel moeten zijn.

Commentaar van het Comité I:

In november 2000 heeft de regering een nieuw investeringsplan van het ministerie van Landsverdediging voor de jaren 2000 en 2001 goedgekeurd.

Dit investeringsprogramma plant militaire aankopen voor meer dan 80 miljard, waaronder 2,923 miljard voor deelname aan de satelliet Helios II.

3.2. De weerslag van een storing van de Amerikaanse transmissiesystemen op de bevoorrading van de ADIV in satellietbeelden

Volgens een artikel van de Amerikaanse journalist James Risen, verschenen in de «New York Times» van 11 april 2000, deed zich in augustus 1999 een storing voor van de Amerikaanse Veiligheidstransmissiesystemen.

Als gevolg van deze storing zou de transmissie van satellietbeelden naar analisten en naar de politieke en militaire overheden gedurende meerdere dagen onderbroken zijn geweest. De beelden konden zelfs niet meer worden afgedrukt.

Réponse du SGR
(briefing circonstancié du 11 février 2000)

Résumé:

Après la décision du gouvernement en octobre 1998, des contacts informels se sont néanmoins poursuivis entre des représentants de la Défense nationale et les autorités françaises en vue d'examiner des possibilités alternatives de participation de la Belgique au programme Hélios II.

Six formules de partenariat ont été examinées, allant de la participation à part entière au programme pour un montant de 2,8 milliards de francs, à l'achat d'images selon les besoins ponctuels (± 1,2 millions de francs la photo) des Forces armées belges.

Les différentes possibilités de se fournir en images auprès d'autres fournisseurs, éventuellement commerciaux, ont également été examinées.

Après comparaison des avantages et inconvénients des diverses possibilités, le SGR estimait que la meilleure solution était la participation opérationnelle au programme Hélios II, mais c'était aussi la plus coûteuse.

Par ailleurs, le centre belge d'interprétation d'images satellitaires s'est progressivement mis en place à partir du mois de décembre 1999. Il dépend du SGR et il devrait être pleinement opérationnel en septembre 2001.

Commentaires du Comité R:

En novembre 2000, le gouvernement a marqué son accord pour un nouveau plan d'investissement du ministère de la Défense nationale pour les années 2000 et 2001.

Plus de 80 milliards d'achats militaires figurent dans ce programme d'investissement parmi lesquels 2,923 milliards seront consacrés à la participation au satellite Hélios II.

3.2. L'incidence d'une panne des systèmes américains de transmissions sur l'approvisionnement du SGR en images satellitaires

Selon un article du journaliste américain James Risen, paru dans le « New York Times « du 11 avril 2000, une panne des systèmes américains de transmissions de sécurité est survenue en août 1999.

Cette panne aurait eu pour conséquence d'interrompre pendant plusieurs jours la transmission des images satellitaires aux analystes ainsi qu'aux autorités politiques et militaires. Les images ne pouvaient même plus être imprimées.

De Amerikaanse inlichtingendiensten konden hun archiefbeelden dus niet vergelijken met de nieuwe beelden, wat betekent dat ze niet meer in staat waren toezicht te houden op de militaire activiteiten van sommige vijandige staten.

Het Comité I heeft de ADIV ondervraagd over de realiteit van dit incident en over de eventuele gevolgen voor de werking van de dienst.

Het Comité I heeft gevraagd of de ADIV op de hoogte was van dit veiligheidincident en als gevolg daarvan niet kon beschikken over informatie die nuttig kan zijn in het kader van zijn opdrachten.

Antwoord van de ADIV (brief van 21 juni 2000)

Samengevat:

De ADIV heeft geen kennis gekregen van het bewuste incident, wat volgens deze dienst normaal is. Aangezien de ADIV in die tijd nog niet beschikte over een operationele analysecel, heeft deze dienst geen nadeel ondervonden van het incident.

Indien een dergelijk incident opnieuw zou voorvallen, zou dit volgens de ADIV geen gevolgen hebben voor de werking van de dienst. Immers, de ADIV krijgt van zijn geallieerden alleen beelden die ten minste 14 dagen oud zijn.

De ADIV herhaalde dat de enige manier om toegang te hebben tot heel recente beelden, erin bestaat deel te nemen aan het Helios II-programma.

Commentaar van het Comité I:

In het jaarverslag 2000 van het «Intelligence and Security Committee»(1) wordt toegegeven dat het NSA inderdaad te maken heeft gehad met een storing van de informatica.

Tegelijk wordt de nadruk gelegd op de kwaliteit van de samenwerking tussen de Britse en Amerikaanse inlichtingendiensten in het kader van het UKUSA-verdrag.

HOOFDSTUK 3

De geschillen inzake veiligheidsmachtigingen

1. Inleiding

Tot voor kort bestond er in België geen gestructureerde wetgeving tot regeling van de procedure voor

(1) *Cf.* Het Britse toezichtsorgaan op de inlichtingendiensten.

Les services de renseignement américains se seraient ainsi trouvés dans l'impossibilité de comparer leurs images d'archives avec les nouvelles, et par conséquent ils n'auraient plus été en mesure de surveiller les activités militaires de certains états hostiles.

Le Comité R a interrogé le SGR sur la réalité de cet incident et sur ses conséquences éventuelles sur le fonctionnement du service.

Le Comité a demandé si le SGR était au courant de cet incident de sécurité et s'était ainsi trouvé privé d'informations utiles à ses missions.

Réponse du SGR (lettre du 21 juin 2000)

Résumé:

Le SGR n'a pas été informé de l'incident en question, ce qui à ses yeux est normal. Etant donné qu'à cette époque, le SGR ne disposait pas encore d'une cellule d'analyse d'images opérationnelle, il n'en a subi aucun inconvénient.

Si un tel incident devait à nouveau se produire, le SGR estime qu'il n'aurait aucune conséquence sur le fonctionnement du service puisque celui-ci n'acquiert auprès de ses alliés que des images datant d'au moins 14 jours.

Et le SGR de répéter que la seule manière pour lui d'avoir accès à des images tout à fait récentes est de participer au programme Hélios II.

Commentaires du Comité R:

Le rapport de l'année 2000 rédigé par l'*«Intelligence and security committee»*(1) a reconnu la survenance de cette panne informatique de la NSA.

En soulignant au passage la qualité de la coopération existant entre les services de renseignement britanniques et américains dans le cadre du traité UKUSA.

CHAPITRE 3

Le contentieux des habilitations de sécurité

1. Préambule

Jusqu'il y a peu la Belgique ne disposait pas d'une législation structurée réglant la procédure de déli-

(1) *Cf.* L'organe britannique de contrôle des services de renseignement.

het uitreiken van een «veiligheidsmachtiging». Niettemin werden jaarlijks duizenden «veiligheidscertificaten» uitgereikt.

Met de wet van 11 december 1998, die op 1 juni 2000 in werking is getreden, had de wetgever tot doel de diverse onderzoeksprocedures te uniformiseren die voorafgaan aan het uitreiken van een veiligheidsmachtiging. Voordien vonden al die procedures hun bron, naargelang het geval, in diverse internationale verordeningen, in richtlijnen van een minister of van de regering, in een koninklijk besluit van 19 december 1989 houdende organisatie van de generale staf en in een wet van 4 augustus 1955 betreffende de veiligheid van de staat op het gebied van de kernenergie ..., maar we willen geenszins beweren dat deze opsomming volledig is.

Nog meer dan voor de noodzaak om de soms tegenstrijdige bepalingen te harmoniseren, had de wetgever vooral aandacht voor het probleem van de onderzoeken die voorafgaan aan het uitreiken van deze officiële machtigingen, die de houders ervan toegang verlenen tot geclassificeerde gegevens.

Het beginsel van de wettigheid van veiligheidsonderzoeken wordt niet betwist, ook niet door het Europees Hof. Dit neemt echter niet weg dat deze onderzoeken een reële inmenging vormen in het privé-leven van de betrokkene en, bijgevolg, slechts kunnen bestaan onder de voorwaarden (arrest-Silver van 25 maart 1983) bepaald in een wet — die toegankelijk en duidelijk is (arrest-Leander van 26 maart 1987) — of in een verwante norm (artikel 8/2º van het Verdrag tot bescherming van de rechten van de mens en van de fundamentele vrijheden).

Ook de Belgische Grondwet (artikel 22) laat de inmenging in het privé-leven van de burgers alleen toe wanneer dit krachtens een wet gebeurt.

Dit was wellicht niet de voornaamste zorg van de bovengenoemde verspreide wetsbepalingen tot regeling van de voorwaarden betreffende de voorafgaande onderzoeken.

2. Verwittiging met betrekking tot de methodologie

Teneinde deze synthese niet te verzwaren, heeft het Comité I niet de bedoeling commentaar te leveren op de wet, die «duidelijk, volledig, toegankelijk en precies» wilde zijn (zie «memorie van toelichting», Kamer van volksvertegenwoordigers van België, 1193/1, 1996-1997 en 1194/1, 1996/1997, blz. 5), in antwoord op de gezamenlijke verwachtingen van het Europees Verdrag, de rechtspraak van het Hof te Straatsburg en de herhaalde adviezen van de Raad van State.

Niettemin heeft het Comité I, *qualitate qua*, de wet geanalyseerd voor intern gebruik. Dit was voor het

vrance d'une habilitation de sécurité. Plusieurs milliers de certificats de sécurité étaient cependant annuellement délivrés.

La loi du 11 décembre 1998, en application depuis le 1er juin 2000, a entendu uniformiser les différentes procédures d'enquêtes conduisant à la délivrance d'une habilitation de sécurité, lesquelles trouvaient antérieurement leur source, selon l'espèce, dans divers règlements internationaux, des directives ministérielles ou gouvernementales, un arrêté royal du 19 décembre 1989 portant organisation de l'état-major général et une loi du 4 août 1955 relative à la sûreté de l'État dans le domaine de l'énergie nucléaire, ... sans prétendre ici à l'exhaustivité.

Plus encore que la nécessité d'harmonisation de dispositions parfois dissonantes, c'est la problématique des enquêtes préalables à la délivrance de ces autorisations officielles d'accès à des données classifiées qui a retenu l'attention du législateur.

Si le principe de la légitimité des enquêtes de sécurité n'est en effet pas contesté, en ce compris par la Cour européenne, il n'en reste pas moins vrai que ces enquêtes représentent une réelle ingérence dans la vie privée et, à ce titre, ne peuvent exister qu'aux conditions prévues (arrêt Silver du 25 mars 1983) par une loi — accessible et précise (arrêt Leander du 26 mars 1987) — ou une norme apparentée (article 8/2º de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Dans le même ordre d'idées la Constitution belge, en son article 22, n'autorise — quant à elle — l'ingérence dans la vie privée des citoyens qu'en vertu d'une loi.

Ce n'était sans doute pas exactement la préoccupation principale dont à créditer les dispositions éparses précitées organisant les modalités des enquêtes préalables.

2. Avertissement méthodologique

Dans le but de ne pas alourdir la présente synthèse, il n'entre pas dans les intentions du Comité R de se livrer au commentaire de cette loi qui a été voulue «claire, complète, accessible et précise» (voir «exposé des motifs», Chambre des représentants de Belgique, 1193/1, 1996-1997 et 1194/1, 1996/1997, p. 5) en réponse aux attentes conjointes de la Convention européenne, de la jurisprudence de Strasbourg et des avis répétés du Conseil d'État.

Le Comité R en a cependant effectué, *qualitate qua*, l'analyse à usage interne qui lui était indispensable,

Comité absoluut noodzakelijk, aangezien het gaat om het positief recht toepasbaar op concrete gevallen die ter beoordeling aan het Comité worden voorgelegd. Het Comité neemt zich voor deze analyse te publiceren ter gelegenheid van haar volgend rapport, na die analyse te hebben verfijnd aan de hand van de activiteiten die het Comité I, in zijn hoedanigheid van beroepsorgaan, gedurende een volledig jaar heeft uitgeoefend.

Vandaag zullen we dus uitsluitend aandacht hebben voor de wet die uit de eerste wet voortvloeit en die voortaan in het middelpunt staat van de gewone bekommernissen van het Comité I. Het gaat om de wet tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen. Het is natuurlijk geen toeval dat deze laatste wet op dezelfde datum is verschenen (op 11 december 1998) en op dezelfde dag in werking is getreden (op 1 juni 2000) als die andere wet. Het praktisch bestaan van beide wetten is immers onlosmakelijk met elkaar verbonden.

3. Huidige analyse van het Comité I

Hoewel de wetgeving terzake nog niet zo lang bestaat, gaat er geen week voorbij zonder dat een eiser bij het Comité, in zijn hoedanigheid van beroepsorgaan, een betwisting indient met betrekking tot een beslissing van weigering, intrekking of diskwalificatie van de veiligheidsmachtiging van het gewenste niveau, genomen sinds de datum van inwerkingtreding van de wet betreffende de veiligheidsmachtigingen.

We herinneren er hier even aan dat in de oude procedure geen specifieke mogelijkheid van beroep was opgenomen. Dit leidde tot een graad van ontevredenheid — al dan niet terecht — waarvan we pas vandaag een duidelijk beeld beginnen te krijgen.

Natuurlijk kon een burger die vond dat hij werd benadeeld door een beslissing van weigering of van intrekking, aangenomen dat de bewuste beslissing ongegrond was, of zelfs door het uitblijven van een beslissing, de zaak aanhangig maken bij de rechtbank van eerste aanleg en aanvoeren dat er een fout was begaan als gevolg waarvan hij schade had geleden. Op die manier kon hij, indien het gerecht vaststelde dat de vermeende fout werkelijk was begaan, de uitspraak van een veroordeling tot het betalen van een materiële schadeloosstelling verkrijgen.

Ook al leidt het geschil inzake de schadeloosstelling in deze jurisdictionele logica tot een vermogensrechtelijke compensatie, een veiligheidsmachtiging wordt nog steeds niet uitgereikt. Bijgevolg krijgt de kandidaat geen toegang tot de functie waarvoor een veiligheidsmachtiging is vereist. Het Comité I heeft echter geen kennis gekregen van een geval dat definitief ten gronde werd beslecht op de datum van het afsluiten van dit verslag, zijnde op 4 januari 2001.

s'agissant du droit positif applicable aux cas concrets lui soumis, et se propose de la publier à l'occasion du prochain rapport, affinée à la lumière d'une année complète d'exercice de son rôle d'organe de recours.

Nous nous pencherons donc exclusivement aujourd'hui sur la loi-corollaire, désormais au centre des préoccupations courantes du Comité R, soit celle qui organise un organe de recours en matière d'habilitations de sécurité. Et ce n'est évidemment pas un hasard si cette dernière porte la même date de publication du 11 décembre 1998 ainsi que la même date d'entrée en vigueur du 1er juin 2000, tant leurs existences pratiques respectives sont indissociables.

3. L'analyse actuelle du Comité R

Malgré le caractère récent de la législation il ne se passe désormais plus de semaine sans qu'un(e) requérant(e) saisisse le Comité-organe de recours d'une contestation relative, selon le cas, au refus, au retrait ou à la disqualification de l'habilitation de sécurité du degré convoité, intervenus depuis la date d'application de la loi sur les habilitations de sécurité.

Faut-il rappeler, à ce stade, que le système antérieur n'organisait aucun recours spécifique, ce qui engendrait un taux d'insatisfaction — justifiée ou non — que l'on commence seulement à mesurer aujourd'hui.

Bien sûr, un citoyen s'estimant lésé par une décision de refus ou de retrait, voire même par une absence de décision, pouvait, dans l'hypothèse où celle-ci aurait été injustifiée, s'adresser au tribunal de première instance, alléguant une faute ayant provoqué un dommage dans son chef, dans le but d'obtenir de la juridiction constatant la réalité de la faute prétendue le prononcé d'une condamnation à un dédommagement matériel.

Mais dans cette logique judiciaire, si le contentieux de l'indemnité conduit à compensation patrimoniale, il n'y a pour autant pas délivrance d'une habilitation de sécurité et, partant, la fonction nécessitant l'habilitation de sécurité restait inaccessible au candidat. Le Comité R n'a cependant pas eu connaissance d'un cas d'espèce définitivement tranché au fond à la date de rédaction du présent rapport, soit le 4 janvier 2001.

Het resultaat was nagenoeg hetzelfde indien dezelfde burger zich wendde tot het Comité I, toen dit Comité nog geen jurisdictionele bevoegdheid genoot. In dit geval werd de betwisting neergelegd op grond van een administratieve klacht en verrichtte het Comité I, in zijn hoedanigheid van controleorgaan, een controleonderzoek teneinde een eventuele disfunctie aan het licht te brengen.

Toch kon de burger, aangenomen dat de redenen van zijn klacht relevant waren, van het Comité I als controleorgaan niet meer verwachten dan een vertrouwelijk rapport waarvan de inhoud strikt was voorbehouden voor de toezichthoudende minister en de parlementaire opvolgingscommissie.

Bovendien is het Comité I niet de natuurlijke bestemmeling van de informatie betreffende eventueel genomen maatregelen, en was het dat wel geweest, dan nog zou het niet bevoegd zijn om die informatie bekend te maken.

Deze handelwijze leidde voor de klager dus evenmin tot de beoogde oplossing, dat is een nieuw onderzoek van zijn dossier met het oog op de uiteindelijke uitreiking van de gewenste veiligheidsmachtiging.

Met betrekking tot de rechtspraak van de Raad van State verwijst het Comité I naar de analyse die het al heeft gepubliceerd (Jaarverslag 1995, blz. 114 tot 139).

De bovengenoemde wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, en haar uitvoeringsbesluit van 24 maart 2000 hebben de procedure voor het regelen van de betwistingen geregeld op jurisdictionele wijze (1).

Nog andere concrete voorwaarden illustreren deze formele aard, maar het heeft geen zin ze hier in detail te beschrijven. Indien nog niet iedereen overtuigd is, volstaat het te verwijzen naar de commentaren op de artikelen van het wetsontwerp (nr. 1194/1), en in het bijzonder artikel 3, § 2, die duidelijk blijk geven van de wil op die manier een jurisdictioneel orgaan onaf-

(1) Het Comité I/beroepsorgaan wordt voorgezeten door een magistraat; het verzoekschrift wordt ingediend per aangetekend schrijven; termijn van verval van één maand vanaf de schriftelijke kennisgeving van de weigering of de intrekking door de veiligheidsofficier; de onmisbare formele stukken en, eventueel, eender welk document dat voor de zaak nuttig wordt geacht, als bijlage bij het verzoek, worden aan het beroepsorgaan bezorgd; het beroepsorgaan ontvangt het volledige onderzoeksdossier op initiatief van de veiligheidsoverheid binnen de vijftien dagen na de kennisgeving aan deze overheid, door de griffier, van het ingediende beroep; neerlegging van het genoemde dossier op de griffie; inzage van het dossier door de eiser en/of zijn advocaat gedurende vijf werkdagen; bepaling van een rechtsdag; eventueel verhoor of verhoren; verplichting uitspraak te doen binnen een termijn van zestig dagen vanaf het indienen van de vordering, betekening, alomtegenwoordige regel van de motivering (vanaf het verzoek tot de definitieve beslissing van het beroepsorgaan, gaande via de akte van weigering of intrekking, de «tussenbeslissingen» ...) enz.

L'aboutissement était quasiment identique si ce même citoyen s'adressait au Comité R, non encore investi de sa compétence juridictionnelle. Dans cet autre cas de figure, la contestation était introduite sur base d'une plainte de type administratif et le Comité R/organe de contrôle procédait à une enquête de contrôle ciblant un éventuel dysfonctionnement.

Toutefois, à supposer pertinents les motifs de la plainte, ce citoyen ne pouvait attendre du Comité R/organe de contrôle qu'un rapport confidentiel dont le contenu était strictement réservé au ministre de tutelle et à la commission parlementaire de suivi.

Le Comité R n'est en outre pas le destinataire naturel de l'information relative aux mesures éventuellement prises et, l'eût-il été, il n'est pas organiquement habilité à la divulguer.

Cette voie n'offrait donc pas non plus au plaignant la solution recherchée, soit le réexamen de son dossier en vue de la délivrance à terme de l'habilitation de sécurité convoitée.

Quant à la jurisprudence du Conseil d'État, le Comité R renvoie à l'analyse déjà publiée (rapport 1995, pp. 129 à 133).

La loi précitée du 11 décembre 1998, instaurant un organe de recours en matière d'habilitations de sécurité, et son arrêté d'exécution du 24 mars 2000 ont organisé la procédure de règlement des contestations sur un mode juridictionnel (1).

D'autres modalités concrètes illustrent ce caractère formel, qu'il serait superflu de détailler ici. S'il fallait cependant en convaincre encore, il suffirait alors de renvoyer aux commentaires des articles du projet de loi (n° 1194/1), et notamment de l'article 3, § 2, qui expriment clairement la volonté de créer de la sorte un organe juridictionnel indépendant du pouvoir législa-

(1) Présidence du Comité R/organe de recours par un magistrat; introduction de la requête par courrier recommandé; délai de forclusion d'un mois à compter de la notification écrite du refus ou du retrait par l'officier de sécurité; communication à l'organe de recours des pièces formelles indispensables et, le cas échéant, de tout document jugé utile à l'espèce, en annexe à la requête; transmis à l'organe de recours du dossier d'enquête complet à l'initiative de l'autorité de sécurité dans les quinze jours de la notification à celle-ci par le greffier du recours introduit; dépôt dudit dossier au greffe; consultation de celui-ci par le requérant et /ou son avocat durant cinq jours ouvrables; fixation d'un jour d'audience; audition(s) éventuelle(s); obligation de statuer dans un délai de soixante jours à compter de l'introduction de la demande, signification, règle omniprésente de la motivation (depuis la requête jusqu'à la décision finale de l'organe de recours en passant par l'acte de refus ou de retrait, les décisions «interlocutoires» ...) etc.

hankelijk van de wetgevende macht te creëren, aan dewelke het Comité I normaal is onderworpen in zijn hoedanigheid van controleorgaan.

Als beroepsorgaan is het Comité I duidelijk zijn beslissing verschuldigd aan een geïndividualiseerd burger.

Het conflict wordt dus wel degelijk op jurisdictionele wijze geregeld, maar daar stopt elke vergelijking met het klassieke juridisch systeem. Het toepassingsgebied van het beroep wordt immers strikt afgebakend door specifieke bepalingen die ondenkbaar zijn in het gemeen recht.

Bijvoorbeeld: het beroep staat niet open wanneer de eiser zich bevindt in het geval beschreven in artikel 16, § 1, lid 3, van de bovengenoemde wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, namelijk indien hij — op eender welk ogenblik — zijn instemming om een veiligheidsonderzoek te ondergaan of houder te zijn van een veiligheidsmachtiging heeft ingetrokken.

Of nog: artikel 5, § 2, lid 4, van de bovengenoemde wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen bepaalt dat informatie ingewonnen binnen het kader van het veiligheidsonderzoek, op het initiatief van een lid van de inlichtingendienst die het onderzoek heeft uitgevoerd, niet aan de eiser wordt meegedeeld, en evenmin aan het (collegiaal) beroepsorgaan indien de voorzitter van dit orgaan daarmee instemt na het diensthoofd te hebben gehoord, gelet op de noodzaak de bronnen of de persoonlijke levenssfeer van derden te beschermen of rekening houdend met de uitvoering van de opdrachten van de dienst.

In verband hiermee, ter uitvoering van de bepalingen van artikel 5, § 3, van de bovengenoemde wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, kan het beroepsorgaan intern beslissen, op initiatief van een inlichtingendienst, dat bepaalde informatie ontoegankelijk zal blijven voor de eiser en voor zijn advocaat, wegens dezelfde criteria inzake bescherming als beschreven in de vorige paragraaf.

Bovendien, indien de informatie afkomstig is van een buitenlandse inlichtingendienst, beslist de nationale inlichtingendienst die het veiligheidsonderzoek heeft verricht — alleen — over de niet-inzage.

Tot slot bepaalt artikel 5, § 2, lid 3, dat, geconfronteerd met een verzoek tot aanvullende inlichtingen uitgaand van het beroepsorgaan op grond van artikel 5, § 2, lid één, van de bovengenoemde wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, dat de leden van de inlichtingendienst die het onderzoek heeft verricht zich mogen beroepen op het geheim van het onderzoek om vrijgesteld te worden van de vertif auquel le Comité R est normalement soumis sous sa casquette d'organe de contrôle ...

C'est très clairement à l'égard d'un citoyen individualisé que le Comité «R»/organe de recours est redevable de sa décision.

Si le mode de règlement du conflit est bel et bien juridictionnel, la comparaison avec un système judiciaire classique s'arrête là. Le champ d'application du recours est en effet strictement contenu par des dispositions spécifiques inimaginables en droit commun.

Par exemple le recours n'est-il pas ouvert lorsque le requérant se situe dans le cas de figure prévu à l'article 16, § 1er, alinéa 3, de la loi précitée du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, soit s'il a — à un moment quelconque — retiré son accord de faire l'objet d'une enquête de sécurité ou de détenir une habilitation de sécurité.

Ou encore: l'article 5, § 2, alinéa 4, de la loi précitée du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité dispose qu'une information recueillie dans le cadre de l'enquête de sécurité peut, à l'initiative d'un membre du service de renseignement qui a procédé à l'enquête, rester hors d'atteinte du requérant, et même de l'organe (collégial) de recours si le président de ce dernier y consent après avoir entendu le chef de service, eu égard à la nécessité de protection de sources, de la vie privée de tiers ou à l'accomplissement des missions du service.

Dans le même ordre d'idées, en exécution des dispositions de l'article 5, § 3, de la loi précitée du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, l'organe de recours peut décider en son sein, sur initiative d'un service de renseignement, que certaines informations seront, sous les mêmes critères de protection que visés au paragraphe ci-dessus, inaccessibles tant au requérant qu'à son avocat.

En outre, si l'information provient d'un service de renseignement étranger, c'est le service de renseignement national qui a procédé à l'enquête de sécurité qui décide — seul — de la non-consultation.

Enfin, l'article 5, § 2, alinéa 3, stipule que, face à une demande d'informations complémentaires adressée par l'organe de recours sur pied de l'article 5, § 2, alinéa premier, de la loi précitée du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, les membres du service de renseignement qui a procédé à l'enquête puissent exciper du secret de l'instruction pour se dispenser de révéler à l'organe de recours lui-même le contenu de

plichting aan het beroepsorgaan zelf de inhoud te onthullen van «geheime informatie die betrekking heeft op een nog lopend opsporings- of gerechtelijk onderzoek(1)».

Al deze beslissingen «alvorens recht te doen», die respectievelijk worden genomen door het beroepsorgaan, zijn voorzitter alleen of de diensten zelf en die betrekking hebben op het verstrekken van informatie (die daadwerkelijk in het bezit is van de inlichtingendiensten), zijn voor geen enkel beroep vatbaar, of ze nu gericht zijn tot de eiser alleen of tot de eiser en het beroepsorgaan samen, of nog tot de dienst die het onderzoek heeft gevoerd. Beroep is evenmin mogelijk tegen de definitieve beslissing van het Comité I als beroepsorgaan.

We stellen vast dat we hier ver verwijderd zijn van de beginselen van het gerechtelijk recht. Zonder de hierboven genoemde wetsbepalingen alle afzonderlijk en systematisch te gaan analyseren, kunnen we in het algemeen onthouden dat de wetgever op dit domein de bedoeling had de onthulling te voorkomen van informatie die schadelijk kan zijn voor de behoorlijke bescherming van de bronnen, voor de persoonlijke levenssfeer van derden en voor de uitvoering van de opdrachten van de inlichtingendiensten. Daartoe creëerde de wetgever een procedure die in principe uitsluitend tot doel had een individueel verhaalmiddel aan te reiken.

«De door de regering gekozen oplossing wil een evenwicht tot stand brengen tussen de rechten van de verdediging en de vereisten inzake de bescherming van de bronnen en van de nationale veiligheid.» (1193/1-1996/1997 en 1194/1-1996/1997, artikel 5, blz. 23.)

Door de procedure om te keren heeft men duidelijk voorrang gegeven aan het mogelijke risico van de onwettige toegang tot de geclassificeerde informatie, die bijzonder schadelijk kan zijn voor de natie.

Het lijkt wel of dat bewust werd gedaan, aangezien het beroepsorgaan vandaag de dag, in strikte toepassing van de wet, en met een gecontroleerd veiligheidsniveau, een dossier met geclassificeerde informatie ter beschikking stelt van eisers en/of hun raadsman, die hypothetisch gesproken niet bewijzen dat ze een veisecrets qui concernent une information ou une instruction judiciaire en cours(1)».

Toutes ces décisions avant dire droit respectivement prises par l'organe de recours, son président seul ou les services eux-mêmes et relatives à la communication d'informations (effectivement détenues par les services de renseignement), qu'elles s'adressent au requérant seul ou conjointement au requérant et à l'organe de recours, ou encore au service qui a mené l'enquête ne sont susceptibles d'aucun recours. Il en va de même à l'égard de la décision finale du Comité R/organe de recours.

On le voit, nous sommes ici bien éloignés des principes du droit judiciaire. Sans entrer dans l'analyse individuelle et systématique des dispositions ci-dessus évoquées, on retiendra globalement que la motivation du législateur était, sur ce plan, de ne pas permettre la divulgation d'informations susceptibles de porter atteinte à la protection due aux sources, à la vie privée des tiers et à l'accomplissement des missions des services de renseignement, par le biais d'une procédure par principe uniquement destinée à offrir une voie de recours individuel.

«La solution adoptée par le gouvernement tend à réaliser un équilibre entre les droits de la défense et les exigences de la protection des sources et de la sécurité nationale.» (1193/1-1996/1997 et 1194/1-1996/1997, article 5, p. 23.)

À l'évidence c'est l'éventualité du risque d'accès illégitime, susceptible d'être hautement préjudiciable à la nation, à l'information classifiée, par le biais d'un détournement de procédure, qui a été privilégiée.

À bon escient semble-t-il, puisqu'à l'heure actuelle, et à un niveau de sécurité contrôlé, l'organe de recours met hebdomadairement, en rigoureuse application de la loi, à la disposition de requérants et/ou leurs conseils, qui ne justifient par hypothèse pas de l'habilitation de sécurité du degré correspondant, un

---

(1) Het principe van het geheim van het gerechtelijk onderzoek, dat zo op opportune wijze wordt aangevoerd, zorgt niet voor problemen, maar dit geldt niet noodzakelijk met betrekking tot de beoordeling van wat daadwerkelijk «betrekking heeft» op een geheim van een nog lopend gerechtelijk onderzoek. In verband hiermee heeft het Comité I de onderzoeksdiensten aanbevolen deze bepaling niet blind toe te passen en, in geval van twijfel (die natuurlijk ten goede komt aan het geheim van het onderzoek), de zaak voor te leggen aan de onderzoeksrechter die met het onderzoek is belast en die, volgens het Comité I althans, als eerste bevoegd is om een onderscheid te maken tussen informatie die door het geheim van het onderzoek wordt gedekt en informatie waarvoor dat niet het geval is.

(1) Si le principe du secret de l'instruction, opportunément rappelé de la sorte, ne fait pas problème, il n'en va pas nécessairement de même au niveau de l'évaluation de ce qui «concerne» effectivement un secret d'instruction en cours. En l'état, le Comité «R» a recommandé aux services d'enquêtes de ne pas faire application aveugle de cette disposition et, en cas de doute (qui profite naturellement au secret de l'instruction), d'en référer au juge d'instruction titulaire, premier habilité lui a-t-il semblé à distinguer les informations couvertes par le secret de l'instruction de celles qui ne le sont pas.

ligheidsmachtiging van het overeenstemmende niveau bezitten, waartoe ze onder andere omstandigheden dan het indienen van beroep nooit toegang zouden krijgen.

Deze paradox is het gevolg van de voorrang die tot op zekere hoogte aan de individuele rechten van de verdediging wordt gegeven. Daartegenover staat dat deze situatie kan worden gecorrigeerd door de hierboven beschreven mogelijkheden, voor diverse betrokkenen, om het dossier ten dele te censureren of slechts de gedeeltelijke inzage ervan toe te staan.

Het Comité I had voorheen nog nooit volledig toegang gekregen tot eender welk onderzoeksdossier van een inlichtingendienst. Bijgevolg heeft het deze dossiers pas voor het eerst gezien op het ogenblik van het eerste beroep en de eerste beslissing van weigering/intrekking door de veiligheidsoverheid.

Op de datum waarop dit rapport werd afgesloten, dat is op 4 januari 2001, waren twintig beroepen neergelegd, het eerste op 31 augustus 2000.

Onder de zaken waarin op 4 januari 2001 een beslissing was genomen, onderscheiden we: twee gevallen waarin werd beslist dat het beroepsorgaan niet bevoegd was, één waarin het beroep niet ontvankelijk was, acht waarin het beroep ontvankelijk was maar niet gegrond, één waarin het beroep ontvankelijk en gegrond was en waarin bijgevolg de beslissing van weigering/intrekking nietig werd verklaard en de uitreiking van de veiligheidsmachtiging werd uitgesproken, en tot slot nog vier gevallen waarin het dossier naar de veiligheidsoverheid werd verwezen voor aanvullend onderzoek en het nemen van een nieuwe beslissing door deze overheid.

In 9 van de bovengenoemde 20 dossiers werd de eiser bijgestaan door een advocaat. In één van die 20 dossiers is een vakbond tussengekomen.

Aangezien de referentieperiode te kort is, kunnen we nog geen statistische gevolgtrekkingen maken. We kunnen hoogstens opmerken dat de drempel van twintig beroepen per jaar, waarmee rekening werd gehouden bij de voorbereidende werkzaamheden en dit wellicht op grond van (moeilijke) ramingen van de diensten zelf, momenteel ruimschoots wordt overschreden.

De toekomst moet uitwijzen of deze tendens, na een proefperiode voor het beroepsorgaan, een dalende lijn zal vertonen of zich integendeel zal voortzetten. In dit laatste geval moet men nagaan of het Comité I over voldoende middelen beschikt om deze opdracht uit te voeren, naast zijn andere opdrachten.

Volledigheidshalve moeten we preciseren dat de meeste beroepen die tot op vandaag zijn ingediend betrekking hebben op een beslissing van de ADIV in zijn hoedanigheid van veiligheidsoverheid. In deze hoedanigheid is de ADIV bevoegd niet alleen «voor

dossier contenant des informations classifiées auquel ils n'auraient jamais accès en d'autres circonstances que le recours.

Ce paradoxe apparent s'explique en fait par une certaine prévalence accordée aux droits individuels de défense, et se voit — en contrepartie — corrigé par les possibilités ci-dessus exposées, offertes aux uns et aux autres, d'expurger en partie le dossier, soit de n'en permettre qu'une consultation partielle.

Le Comité R n'avait auparavant jamais eu un accès complet à un dossier d'enquête de sécurité réalisée par un service de renseignement. Il a donc découvert ceux-ci en même temps que le premier recours et la première décision de refus/retrait prise par l'autorité de sécurité.

À la date de clôture du présent rapport, soit le 4 janvier 2001, vingt recours avaient été introduits, dont le premier le 31 août 2000.

Parmi ceux qui avaient, à cette date du 4 janvier 2001, fait l'objet d'une décision, on en dénombre deux concluant à l'incompétence de l'organe de recours, un concluant à l'irrecevabilité du recours, huit concluant à la recevabilité du recours mais à son absence de fondement, un concluant à la recevabilité et au fondement du recours, infirmant la décision de refus/retrait et prononçant la délivrance de l'habilitation de sécurité, et enfin quatre concluant au renvoi du dossier à l'autorité de sécurité pour complément d'enquête et prise d'une nouvelle décision par elle.

Dans 9 dossiers sur les 20 de référence évoqués ci-dessus, les requérants étaient assistés d'un avocat, tandis qu'un syndicat s'est manifesté dans un dossier sur les 20 de référence.

Compte-tenu d'une période de référence insuffisante, aucune conclusion d'ordre statistique ne saurait être actuellement tirée. Tout au plus peut-on remarquer que le seuil de vingt recours annuels, envisagé lors des travaux préparatoires, vraisemblablement sur base d'estimations (malaisées) des services eux-mêmes, est actuellement largement dépassé.

L'avenir nous dira si, après une phase de test de l'organe de recours, le mouvement décroîtra ou se maintiendra. Dans cette dernière hypothèse se poserait alors la question des moyens, en regard des autres missions du Comité R.

Pour être tout à fait exact il convient de préciser que la grande majorité des recours réceptionnés à ce jour visent une décision rendue par le SGR en sa qualité d'autorité de sécurité compétente non seulement pour les personnes qui relèvent du ministre de la Défense

de personen die ressorteren onder de minister van Landsverdediging», maar ook «voor de kandidaten voor een betrekking binnen het ministerie van Landsverdediging» (artikel 15, 2º, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen). Dit is met grote voorsprong de grootste groep houders van een machtiging.

Deze eerste beschouwingen hebben dus vooral betrekking op dossiers opgesteld door de Algemene Dienst inlichting en veiligheid.

Een eerste vaststelling van het Comité I, in zijn hoedanigheid van beroepsorgaan, heeft betrekking op de manier waarop de beroepen worden neergelegd. Weinig eisers leven nauwgezet de vormen na die worden voorgeschreven in het bovengenoemd koninklijk uitvoeringsbesluit van 24 maart 2000 tot regeling van de rechtspleging voor het beroepsorgaan inzake veiligheidsmachtigingen. Bijgevolg betroffen de eerste beraadslagingen van het Comité I, in de bovengenoemde hoedanigheid, natuurlijk de ontvankelijkheid van de beroepen.

Bij gebrek aan duidelijke richtlijnen in die zin van de wetgever, kon het Comité I in de meeste gevallen niet anders dan besluiten dat het beroep ontvankelijk was op grond van een interpretatie conform de theorie van de nietigheden in het gerechtelijk recht. We kunnen natuurlijk niet uitsluiten dat deze theorie in de toekomst nog zal wijzigen, naar het voorbeeld van om het even welke doctrine of rechtspraak.

Een tweede vaststelling betreft de (vereiste) motivering van elke beslissing door de veiligheidsoverheid. In die motiveringen is er heel vaak sprake van integriteit, loyauteit, eerbaarheid en betrouwbaarheid. Voor het Comité I was het al gauw duidelijk dat de criteria van eerbaarheid, loyauteit en, tot op zekere hoogte, integriteit niet automatisch passend waren en dat hun systematisch gebruik de behoorlijke motivering van de beslissing eerder in de weg stond.

Wat is er immers meer vatbaar voor discussie dan het begrip eerbaarheid, dat evolueert met de tijd en volgens de cultuur? En wat te denken van de «loyauteit», bijvoorbeeld in een internationale geïntegreerde militaire context? Welk noodzakelijk verband zou er automatisch bestaan tussen een strafrechtelijke veroordeling, bijvoorbeeld, die iemand in het verleden heeft opgelopen en de integriteit die hij vandaag heeft teruggewonnen?

In deze omstandigheden, en aangezien het Comité I van tijd tot tijd geconfronteerd wordt met een beroep dat wellicht eerder wordt ingediend in een reactie van afwijzing van de meegedeelde motivering dan werkelijk krachtens een bezwaar ten gronde, heeft het er de voorkeur aan gegeven vooral aandacht te besteden aan het vierde criterium dat gewoonlijk wordt meegedeeld, namelijk dat van de betrouwbaarheid.

Is de beoordeling van dit criterium uiteindelijk niet het hoofddoel van deze veiligheidsonderzoeken:

nationale, mais aussi, pour les candidats à un emploi au sein du ministère de la Défense nationale (article 15, 2º, de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité). C'est de très loin le groupe de détenteurs d'habilitation le plus important.

C'est donc, en l'état, surtout au départ de dossiers constitués par le SGR que ces premières réflexions ont émergé.

Une première constatation du Comité R/organe de recours est relative à la manière dont les recours sont introduits. Peu de requérants respectent scrupuleusement les formes prescrites par l'arrêté royal d'exécution précité du 24 mars 2000 déterminant la procédure à suivre devant l'organe de recours en matière d'habilitations de sécurité. Les premières délibérations du Comité «R»/organe de recours ont donc naturellement porté sur la recevabilité.

À défaut d'indications péremptoires données en ce sens par le législateur, le Comité «R» a donc été, dans plusieurs cas, amené à admettre la recevabilité du recours sur base d'une interprétation conforme à la théorie des nullités en droit judiciaire. Il n'est évidemment pas exclu que celle-ci évolue encore dans le futur, à l'instar de toute doctrine ou jurisprudence.

Une seconde contestation concerne la motivation (indispensable) apportée par l'autorité de sécurité à chaque décision. Il y est abondamment question d'intégrité, de loyauté, d'honorabilité et de fiabilité. Il a rapidement paru au Comité «R» que les critères d'honorabilité, de loyauté et, dans une certaine mesure, d'intégrité n'étaient pas automatiquement adéquats et que leur usage systématique encombrait plutôt la motivation de la décision.

Quoi de plus discutable en effet que le concept d'honorabilité, évolutif dans le temps et selon les cultures? Quid de la «loyauté», par exemple dans un contexte militaire intégré international? Quelle nécessaire liaison existerait-il automatiquement entre une condamnation pénale antérieure, par exemple, et une intégrité actuellement restaurée?

Dans ces conditions, et face à l'un ou l'autre recours plus vraisemblablement introduits sur une réaction de rejet de la motivation exprimée qu'en vertu d'une véritable objection de fond, le Comité «R» a préféré privilégier la piste du quatrième critère généralement exprimé, soit celui de fiabilité.

N'est-ce en définitive pas ce, seul, à quoi tendent ces enquêtes de sécurité: évaluer la capacité d'une

nagaan in welke mate een persoon die toegang heeft tot geclassificeerde informatie bekwaam is om die informatie alleen te gebruiken in strikte uitvoering van de heersende veiligheidsregels.

Op deze manier bekeken zijn de eerste drie criteria geen (collaterale) criteria meer krachtens dewelke de veiligheidsmachtiging wordt toegekend of afgewezen, maar (ondergeschikte) instrumenten waarmee het criterium «betrouwbaarheid» wordt gemeten. Wat er ook van zij, de beschouwingen hierover zullen zeker nog wijzigen.

Een derde vaststelling heeft betrekking op de inhoud van bepaalde dossiers. Het beroepsorgaan heeft de indruk dat sommige dossiers onvolledig zijn en soms zelfs materiële fouten bevatten.

Dit is des te meer onaanvaardbaar indien de informatie in deze dossiers, soms onvermijdelijk, op het randje van het gerucht ligt. Het beroepsorgaan is dan ook de mening toegedaan dat in deze gevallen, wanneer er twijfel is over de inhoud van doorslaggevende elementen in het dossier — en meestal wordt dit al duidelijk bij lezing van de eerste bladzijden —, de veiligheidsdienst die het onderzoek voert, de kandidaat zou moeten uitnodigen om hem te verhoren, vóór een beslissing wordt genomen betreffende deze persoon.

Een vierde vaststelling betreft de foute benadering die meestal wordt gehanteerd door de personen met betrekking tot dewelke het Comité I in zijn hoedanigheid van beroepsorgaan een beslissing moet nemen. Het ligt blijkbaar niet voor de hand dat het beroepsorgaan zich niet laat leiden door een logica van repressie. Toegegeven, de — onvermijdelijke — verwijzing naar strafrechtelijke omstandigheden die een doorslaggevend deel van het dossier vormen, draagt er niet toe bij vlot aan te nemen dat repressie niet het doel is van het Comité I.

Omgekeerd is het voor de eisers niet evident toe te geven dat de wet van hen geen houders maakt van een subjectief recht om een veiligheidsmachtiging te verwerven. Dit valt echter gemakkelijk te begrijpen wanneer men weet dat de definitieve weigering van een veiligheidsmachtiging, waartegen geen beroep mogelijk is, bijzonder ernstige gevolgen kan hebben voor de eisers, zoals daar zijn: intern verlies van geloofwaardigheid, mogelijk uitstel van bevordering, verlies — soms aanzienlijk — van inkomsten, overplaatsing naar een militaire basis die verder van de woonplaats is verwijderd, met alle familiale gevolgen vandien ...

We kunnen dus nooit genoeg herhalen dat, krachtens de wet, het onvermijdelijk logisch gevolg van het recht op beroep voor een afgewezen kandidaat, dat is het individueel tegenwicht dat in het verle-

personne ayant accès à des informations classifiées à n'en faire usage qu'en exécution stricte des règles de sécurité prévalentes.

Dans cette optique, les trois premiers critères deviennent non plus des critères (collatéraux) commandant l'attribution ou le rejet de l'habilitation de sécurité, mais des instruments (subordonnés) de mesure du critère de fiabilité. Quoi qu'il en soit, la réflexion évoluera certainement encore sur ce plan.

Une troisième constatation réside dans le contenu de certains dossiers. Il paraît à l'organe de recours que certains dossiers se révèlent parcellaires, voire même dépositaires d'erreurs matérielles.

Ceci est d'autant plus inacceptable si les informations contenues dans ces dossiers se situent, parfois inévitablement, à la limite de la rumeur. L'organe de recours a donc été amené à considérer, dans ces cas d'espèce, qu'en cas de doute quant au contenu d'éléments déterminants du dossier, surgissant la plupart du temps dès lecture des premières pages, il devrait s'imposer au service de sécurité qui réalise l'enquête de convoquer le candidat pour audition, préalablement à toute prise de décision qui le concerne.

Une quatrième constatation n'est autre que l'erreur d'approche qu'ont tendance à faire les justiciables du Comité «R»/organe de recours. Il ne tombe apparemment pas sous le sens que l'organe de recours n'est pas mû par une logique de répression. Il est vrai que la référence — inévitable — à des circonstances d'ordre pénal constituant une part prépondérante du dossier n'est pas là pour favoriser la perception d'une finalité différente.

À l'inverse il n'est pas évident non plus pour les requérants d'admettre que la loi ne fait pas d'eux les titulaires d'un droit subjectif à acquérir une habilitation de sécurité. Cela se comprend toutefois aisément quand on sait que le refus définitif, sans appel, d'une habilitation de sécurité s'avère susceptible d'entraîner des conséquences majeures pour les requérants, et notamment: perte de crédibilité interne, retard potentiel d'avancement, perte — parfois substantielle — de revenus, mutation vers une implantation militaire plus éloignée du lieu de résidence, avec les complications familiales que cela induit parfois ...

On ne répétera donc jamais assez qu'en vertu de la loi, le corollaire obligé du droit au recours pour un candidat évincé, soit le contrepoids individuel qui faisait précédemment défaut, n'est autre que le droit

den ontbrak, niets anders is dan het collectief recht op de veiligheid van de geclassificeerde informatie en, achter dit geheim, van de collectiviteit die erdoor wordt beschermd.

Van zijn kant probeert het Comité I te doen inzien dat het, wanneer het bijvoorbeeld rekening houdt met betekenisvolle strafrechtelijke veroordelingen in het verleden, die verband houden met de algemene betrouwbaarheid van een individu, de betrokkene niet een tweede keer veroordeelt (*« non bis in idem »*) door hem de toegang tot de gewenste veiligheidsmachtiging te weigeren.

Het Comité I houdt zo goed als mogelijk rekening met alle pro's en contra's bij het beoordelen van de individuele rechten enerzijds en het recht van de collectiviteit anderzijds om te kunnen beschikken over houders van geclassificeerde informatie (waarvan de onthulling de natie ernstig nadeel kan berokkenen) en die kunnen bewijzen dat ze de grootst mogelijke beproefde betrouwbaarheid bezitten.

Nog in verband hiermee vindt het Comité I, in zijn hoedanigheid van beroepsorgaan, dat de *ratio legis* vereist dat de individuele materiële voordelen die eventueel het gevolg zijn van het bezitten van een veiligheidsmachtiging moeten wijken voor het collectief materieel nadeel dat kan voortvloeien uit de schadelijke onthulling door een houder, van wie de betrouwbaarheid niet voldoende op de proef is gesteld, van geclassificeerde informatie aan een persoon met kwade bedoelingen.

Een laatste vaststelling heeft betrekking op de wil waarvan de SGR onmiddellijk blijk heeft gegeven om de nieuwe verplichtingen ter zake waarmee de wet deze dienst belast, te goeder trouw en zo doeltreffend mogelijk uit te voeren. Het is niet overdreven te stellen dat de hoeveelheid werk in belangrijke mate is toegenomen en dat de huidige opvolging, dat wil zeggen conform de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, van het personeel bovendien een reële inspanning tot aanpassing vergt in vergelijking met de werkwijze in het verleden.

Op een voorbereidende vergadering werd gesteld dat de diensten vandaag de dag blijk moeten kunnen geven van overtuigingskracht, terwijl het vroeger voldoende was dat ze afdoende argumenten aanvoerden. De marge tussen beide houdingen is recht evenredig met de inspanning die van het personeel wordt verwacht.

In de rand van het eigenlijke probleem zou nog een andere vaststelling, waarover momenteel wordt nagedacht, zich op termijn kunnen opdringen: de typologie van de militaire activiteiten waarvoor momenteel een veiligheidsmachtiging is vereist, geldig in vredes- en in oorlogstijd, lijkt te moeten worden herzien en zou bovendien van tijd tot tijd herzienbaar moeten zijn, niet alleen met betrekking tot het veiligheidsnicollectif à la sécurité pour l'information classifiée, et derrière ce secret, pour la collectivité qu'il protège.

Le Comité « R », quant à lui, s'efforce de faire comprendre qu'en tenant compte, par exemple de condamnations pénales antérieures significatives, en rapport avec la fiabilité générale d'un individu, il ne condamne pas une seconde fois cette personne (« *non bis in idem* ») en lui refusant l'accès à l'habilitation de sécurité convoitée.

Il fait le plus exactement possible la part des choses entre les droits individuels et le droit de la collectivité à bénéficier de titulaires d'informations classifiées (dont la divulgation serait de nature à causer un préjudice grave à la nation) qui puissent justifier de la fiabilité la plus éprouvée possible.

Dans le même ordre d'idées, il semble au Comité « R »/organe de recours que la *ratio legis* exige que les avantages matériels individuels résultant éventuellement de la détention d'une habilitation de sécurité cèdent le pas devant le dommage matériel collectif qui résulterait de la délivrance préjudiciable par un titulaire, dont la fiabilité n'a pas été assez éprouvée, d'une information classifiée à une personne mal intentionnée.

Une dernière constatation concerne la volonté immédiatement manifestée par le SGR d'exécuter de bonne foi et le plus efficacement possible les obligations nouvelles lui imposées en la matière par la loi. Il n'est pas excessif de dire que le volume de travail a été multiplié et que le suivi actuel, c'est-à-dire conforme à la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, nécessite en outre de la part de son personnel, un réel effort d'adaptation par rapport à la pratique antérieure.

Ainsi qu'il a été exprimé lors d'une réunion préparatoire, si auparavant les services pouvaient se montrer péremptoires, ils doivent dorénavant se montrer convaincants. La marge entre les deux attitudes révèle l'ampleur de l'effort exigé d'eux.

En marge du contentieux proprement dit, enfin, une constatation d'un autre ordre actuellement sujette à réflexion, pourrait ultérieurement s'imposer: la typologie des activités militaires exigeant actuellement une habilitation de sécurité, valable aussi bien en temps de paix qu'en temps de guerre, paraît devoir être revue, et devrait même être périodiquement révisible, tant au plan du niveau de sécurité

veau dat volstaat voor de bewuste activiteit maar ook met betrekking tot het aantonen dat een veiligheidsmachtiging voor diezelfde activiteit vereist is.

Uit de huidige ervaring van het Comité I, die weliswaar heel beperkt is, blijkt immers dat voor sommige functies, door een gebrek aan herevaluatie, een te hoog niveau van veiligheid in stand wordt gehouden in vergelijking met de dagelijkse praktijk van die functies.

Het is dan ook niet uitgesloten dat het Comité I, deze keer in zijn hoedanigheid van controleorgaan van de ADIV, bijvoorbeeld aandacht besteedt aan de statistieken van de functies waarvoor een veiligheidsmachtiging is vereist en waarvoor men, binnen de strijdkrachten, geen houders vindt, in elk geval niet binnen de termijn gewenst met het oog op de inzetbaarheid van de strijdkrachten.

Men zou ook kunnen overwegen, voor zover dat mogelijk is, het probleem van de veiligheidsmachtigingen aan bod te laten komen in de rekruteringsfase, al was het maar in de vorm van een evaluatie, door een lid van de ADIV, van de risico's inzake de carrière die gepaard gaan met de mogelijkheid, die in deze fase reeds kan worden voorzien, dat de veiligheidsmachtiging, die bij sommige eenheden ambtshalve *quasi* onmisbaar is, in een latere fase wordt geweigerd.

Deze aan de rekrutering voorafgaande evaluatie zou op basis van het dossier kunnen plaatsvinden en ter kennis van de kandidaat kunnen worden gebracht.

Bij gebrek aan een dergelijke evaluatie zou op initiatief van een lid van de ADIV kunnen worden verwezen naar het risico voor de carrière, nadat tijdens het voorafgaand interview materiële elementen vrijwillig werden onthuld (na uitdrukkelijk verzoek daartoe, met toelichting, om te vermijden dat de ondervraagde persoon zich terughoudend opstelt of een valse verklaring aflegt, hetgeen eigen is aan de menselijke aard).

Welke procedure uiteindelijk ook wordt toegepast, en met betrekking tot dewelke het Comité I trouwens niet bevoegd is, de kandidaat zou dan tenminste in staat zijn rekening te houden met dit risico bij het uitstippelen van zijn carrière. Wellicht zou hij zich dan eerder kandidaat stellen voor andere functies dan voor de functies waartoe hij wel eens — al dan niet tijdelijk — geen toegang zou kunnen krijgen, gelet op het (tijdelijk) veiligheidsrisico dat zijn dossier, van in het begin en objectief gezien, inhoudt in het licht van de nieuwe wet.

Deze voorafgaande evaluatie zou natuurlijk extra inspanningen vergen van de ADIV, maar zou er wellicht toe bijdragen te voorkomen dat bepaalde zaken uit frustratie, wat zeer schadelijk is voor de kwaliteit van de latere dienst, bij het beroepsorgaan aanhangig worden gemaakt door eisers die gegriefd zijn omdat

suffisant pour l'activité considérée que celui même de la nécessité démontrée d'exigence d'une habilitation de sécurité pour cette même activité.

Il semble en effet ressortir de l'expérience actuelle, fort limitée il faut en convenir, du Comité «R» que certains postes seraient maintenus, faute de réévaluation, à un degré de sécurité surqualifié par rapport à la pratique quotidienne de la dite fonction.

Il n'est donc pas exclu que le Comité «R», agissant en qualité d'organe de contrôle du SGR cette fois, s'intéresse par exemple aux statistiques des emplois nécessitant une habilitation de sécurité qui, au sein des forces armées, ne trouvent pas de titulaires ou, du moins, pas dans les délais souhaitables pour l'opérationnalité des forces armées.

Une autre réflexion pourrait être que, dans la mesure du possible, la phase de recrutement intègre la problématique des habilitations de sécurité, ne serait-ce que par une évaluation par un membre du SGR des risques de carrière liés à une éventualité prévisible dès cet instant de refus ultérieur d'une habilitation de sécurité, *quasi*-indispensable d'office dans certaines unités.

Cette évaluation préliminaire à l'engagement pourrait se faire sur dossier et être portée à la connaissance du candidat.

À défaut, une évocation du risque de carrière, consécutive à des éléments matériels volontairement révélés (sur demande expresse en ce sens, démarche explicative à la clé afin d'éviter les réticences ou fausses déclarations liées à la nature humaine) au cours de l'interview préalable, pourrait avoir lieu à l'initiative d'un membre du SGR.

Quelle que soit, en définitive, la procédure mise en œuvre, qui n'entre d'ailleurs pas dans la sphère de compétence du Comité «R», le candidat serait alors en mesure d'intégrer ce risque dans son choix de carrière et orienterait sans doute plus volontiers sa candidature vers des fonctions autres que celles qui risquent de lui être inaccessibles, ou momentanément inaccessibles, en raison du risque ou du risque temporaire de sécurité que révèle, dès le départ et objectivement, son dossier en regard de la loi nouvelle.

Cette évaluation préliminaire nécessiterait évidemment un investissement supplémentaire de la part du SGR, mais elle éviterait vraisemblablement les frustrations, hautement préjudiciables à la qualité ultérieure du service, régulièrement exposées à l'organe de recours par des requérants navrés de devoir inter-

ze een activiteit moeten onderbreken waarin ze veel van zichzelf hadden gelegd en die, in sommige gevallen, precies geschikt leek om opnieuw voldoende betrouwbaarheid te herwinnen.

Dit zou kunnen helpen om te voorkomen dat bepaalde functies, waarvoor niet onmiddellijk een geschikte kandidaat wordt gevonden die de vereiste veiligheidsmachtiging kan bezitten, gedurende lange tijd vacant zijn, wat nadelig is voor de goede organisatie van de Belgische strijdkrachten, des te meer omdat het Comité I momenteel vaststelt, ter gelegenheid van zijn opeenvolgende verhoren, dat de periode tijdens dewelke een functie vacant is wordt verlengd met de tijd die de kandidaat nodig heeft om zijn beroep uit te oefenen (dat is dertig dagen), alsook met de tijd die het beroepsorgaan nodig heeft om een beslissing te nemen (dat is nog eens zestig dagen).

Anderzijds zou het aantal onderzoeken afnemen, aangezien aanvragen tot het verkrijgen van een veiligheidsmachtiging niet langer, zoals dat nu wel het geval is, zouden worden ingediend hoewel men van in het begin al geen enkele kans op slagen heeft, omdat men niet op de hoogte is van de tenietdoende materiële elementen die de uitreiking verhinderen. Tot mislukken gedoemde beroepen zouden verdwijnen, bij gebrek aan voorwerp vanwege mogelijke eisers, die tegelijk minder talrijk zullen zijn, maar tevens beter op de hoogte zullen zijn van alle risico's die het resultaat van het ingediende beroep kunnen beïnvloeden.

Een daling van het aantal veiligheidsonderzoeken, gepaard gaand met een vermindering van het aantal bijkomende opdrachten bevolen door het beroepsorgaan binnen het kader van het onderzoek van het beroep, zou misschien een compensatie kunnen zijn voor de hierboven genoemde extra investering in tijd, met als «bonus» een daling van het aantal gevallen van professionele demotivatie en een snellere rotatie van de beveiligde functies.

*
* *

Hoewel het in deze niet handelt om een onderzoek in strikte betekenis, werd deze analyse voorgelegd aan de ministers van Landsverdediging en Justitie op 19 maart 2001.

Op datum van 25 april 2001 zond eerstvermelde een brief aan het Comité I waarin hij de nieuwheid van de materie onderlijnde, hij vestigde ook de aandacht op de natuurlijke evolutie van de procedure, het verruimde debat binnen de Strijdkrachten bij het opstellen van een typologie en het vaststellen van een carrière-risico bij de aanwerving. Tot slot geeft hij blijk van tevredenheid bij de vaststelling van de goodwill waarvan de ADIV blijk geeft bij de uitoefening van zijn nieuwe verplichtingen.

De minister van Justitie heeft geen opmerkingen bekendgemaakt.

rompre une activité dans laquelle ils s'étaient investis et qui, dans certains cas, semblait justement de nature à les réintégrer plus rapidement dans un contexte de fiabilité suffisante.

Cela éviterait éventuellement la vacance prolongée, préjudiciable à la bonne organisation des forces armées belges, de postes ne trouvant pas tout de suite le candidat apte à détenir l'habilitation de sécurité nécessaire, et ce d'autant plus que le Comité «R» constate actuellement, à l'occasion de ses auditions successives, que la vacance du poste se prolonge le temps nécessaire au candidat pour exercer son recours, soit trente jours, plus le temps pour l'organe de recours de rendre sa décision, soit soixante jours supplémentaires.

En aval, le nombre des enquêtes diminuerait puisque des demandes d'habilitation de sécurité ne seraient pas, comme c'est le cas aujourd'hui, introduites en pure perte dès le départ parce qu'en méconnaissance de cause d'éléments matériels dirimants faisant obstacle à la délivrance, et des recours voués à l'échec disparaîtraient faute d'objet de la part de requérants potentiels, à la fois moins nombreux et mieux informés des aléas de leur recours.

Moins d'enquêtes de sécurité, conjugué à moins de devoirs complémentaires ordonnés par l'organe de recours dans le cadre de l'examen du recours pourrait peut-être compenser le surcroît d'investissement en temps pré-cité, avec la «prime» que constituerait moins de démotivation professionnelle globale et plus de rapidité dans la rotation des postes sécurisés.

*
* *

Bien que ne s'agissant pas d'une «enquête» *sensu stricto*, la présente analyse a été soumise pour observations aux ministres de la Défense nationale et de la Justice en date du 19 mars 2001.

En date du 25 avril 2001, le premier a fait parvenir au Comité R, organe de recours, un courrier soulignant la nouveauté de la matière, l'évolution naturelle ultérieure de la procédure, le débat élargi au sein des Forces armées que suppose l'aménagement d'une typologie et la détection d'un risque de carrière à l'engagement et enfin sa satisfaction de constater la bonne volonté manifestée par le SGR dans l'exécution de ses nouvelles obligations.

Le ministre de la Justice n'a, quant à lui, formulé aucune observation.

TITEL II

DE TOEZICHTSONDERZOEKEN

A. Onderzoeken op verzoek van het Parlement of van ministers

HOOFDSTUK 1

SYNTHESEVERSLAG VAN HET ONDERZOEK OVER DE MANIER WAAROP DE BELGISCHE INLICHTINGENDIENSTEN REAGEREN OP HET EVENTUEEL BESTAAN VAN EEN AMERIKAANS SYSTEEM, ECHELON GENAAMD, VOOR HET ONDERSCHEPPEN VAN TELECOMMUNICATIES IN BELGIË

1. Inleiding

In de hele Europese Unie heeft de pers veel aandacht besteed aan een tussentijds rapport van september 1998 met de titel «Une évaluation des techniques de contrôle politique». Dit rapport is opgesteld door de «Omega Foundation» uit Manchester (UK). en werd voorgesteld aan de groep «STOA» (Scientific and Technological Assessment) van het Europees Parlement.

Uit dit door de Britse journalist, Duncan Campbell, opgestelde rapport, bleek dat de Verenigde Staten, Groot-Brittannië, Canada, Australië en Nieuw-Zeeland een netwerk «Echelon» zouden hebben opgezet.

Deze studie bracht aan het licht dat: «Alle elektronisch, telefoon- en faxverkeer in Europa wordt dagelijks onderschept door de *National Security Agency* van de Verenigde Staten, dat alle informatie afkomstig van het Europese continent via het strategisch centrum in Londen en vervolgens via satelliet naar Fort Meade in Maryland doorstuurt, via het cruciale centrum Menwith Hill in het gebied van de North York Moors in het Verenigd Koninkrijk.»

De verspreiding van dit rapport in de pers heeft de aandacht gewekt van een aantal regeringen — met name de Franse —, en van sommige Belgische parlementsleden.

Het onderzoek dat het Comité I voerde over dit onderwerp, werd geopend op verzoek van de leden van het Federaal Parlement en de Bijzondere Commissie belast met de parlementaire begeleiding van de Vaste Comités P en I.

Het verzoek tot opening van onderzoek, toegezonden op 10 november 1998, werd als volgt geformuleerd:

«Hoe reageren de Belgische inlichtingendiensten op het eventueel bestaan van een Amerikaans sys-

TITRE II

LES ENQUÊTES DE CONTRÔLE

A. Enquêtes à la requête du Parlement ou des ministres

CHAPITRE 1er

RAPPORT DE SYNTHÈSE SUR LA MANIÈRE DONT LES SERVICES BELGES DE RENSEIGNEMENT RÉAGISSENT FACE A L'ÉVENTUALITÉ D'UN RÉSEAU «ECHELON» D'INTERCEPTION DES COMMUNICATIONS EN BELGIQUE

1. Introduction

Une étude de septembre 1998, intitulée «Une évaluation des techniques de contrôle politique» rédigée par la Fondation Omega de Manchester, et présentée au groupe STOA (Scientific and Technological Assessment) du Parlement Européen a éveillé un grand intérêt dans la presse de toute l'Union européenne.

Cette étude menée par le journaliste britannique Duncan Campbell révélait l'existence d'un réseau «Echelon», qui aurait été mis en place par les États-Unis, la Grande Bretagne, le Canada, l'Australie et la Nouvelle-Zélande.

Selon cette étude, «toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la «National Security Agency» des États-Unis, qui transfère toutes les informations provenant du continent européen via le centre stratégique de Londres, puis par satellite vers Fort Meade au Maryland via le centre crucial de Menwith Hill dans la région des North York Moors au Royaume-Uni».

La diffusion de ce rapport par les médias a éveillé l'attention de certains gouvernements, français notamment, ainsi que de certains parlementaires belges.

L'enquête que le Comité R a menée à ce sujet a été ouverte sur l'initiative de membres du Parlement fédéral ainsi que de la commission spéciale chargée de l'accompagnement parlementaire des Comités P et R.

La demande d'enquête, introduite le 10 novembre 1998, a été rédigée en ces termes:

«Comment les services belges de renseignements réagissent-ils face à l'éventualité d'un système

teem, Echelon genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België? 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?» (1)

Het algemeen activiteitenverslag 1999 van het Vast Comité I, bevattende de eerste resultaten van het onderzoek aangaande de Echelonproblematiek, werd op 14 februari 2000 goedgekeurd door de verenigde commissies van de Kamer van volksvertegenwoordigers en van de Senaat, belast met de respectievelijke 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 een aanvullend verslag voor midden maart 2000 te bezorgen.

Overeenkomstig artikel 48, § 3, van de wet van 18 juli 1991 houdende toezicht op de politie- en inlichtingendiensten, heeft het Vast Comité I besloten zich hierbij te laten assisteren door twee experten:

— 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» te Namen, 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.

Het aanvullend verslag van het Comité I werd goedgekeurd op 13 maart 2000. Het werd opgevolgd door drie bijkomende aanvullingen, respectievelijk goedgekeurd op 9 mei 2000, 29 juni 2000 en 29 september 2000.

In algemene zin kan men stellen dat het Vast Comité I zich reeds in het verleden gebogen heeft over de bescherming van informatica- en communicatiesystemen.

In dit kader deed het reeds in 1994 de aanbeveling dat een officieel organisme zou belast worden met de ontwikkeling en de uitvoering van een globale veiligheidspolitiek voor het geheel van informatiesystemen van de overheidsdiensten.

Men kan eveneens, dezelfde gedachtegang volgend, de in 1998 uitgevoerde studie en het onderzoek vermelden aangaande de deelname van de Belgi-

(1) Vrije vertaling.

«Echelon» d'interception des communications téléphoniques et fax en Belgique? Nos services cherchent-ils à établir l'existence du système Echelon, et le cas échéant, à protéger les entreprises et les citoyens belges contre ces interceptions?» (1).

Le rapport général d'activités 1999 du Comité R comprenant les premiers résultats de l'enquête relative à la problématique d'«Echelon» 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.

Ces 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 un rapport complémentaire pour la mi-mars 2000.

Conformément à l'article 48, § 3, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le Comité R a décidé de se faire assister par deux experts pour mener à bien cette enquête. Ces deux experts sont:

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

ainsi que son collaborateur,

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

Le rapport complémentaire du Comité a été approuvé le 13 mars 2000. Il a été suivi de trois autres suivis approuvés respectivement les 9 mai 2000, 29 juin 2000 et 29 septembre 2000.

D'une manière générale, il convient de rappeler que le Comité R s'était 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, spéciale-

(1) Traduction libre.

sche inlichtingendiensten (in het bijzonder de ADIV) 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 Comité I — 1998 — blz. 173 en volgende).

Dit huidige verslag, geactualiseerd tot op 31 januari 2001, bevat het geheel van vaststellingen die reeds door het Comité I gepubliceerd werden over dit onderwerp evenals een aantal nieuwe gegevens die nog niet aan het Parlement bezorgd werden.

Het huidig verslag werd door het Comité I op 1 februari 2001 goedgekeurd.

Op 22 maart 2001 heeft de minister van Landsverdediging zijn opmerkingen in verband met dit verslag aan het Comité I gezonden. Hij verwijst naast het ontbreken van een wetgeving ter zake en eveneens naar het feit dat de bescherming van het wetenschappelijk of economisch potentieel van het land een opdracht is van de Veiligheid van de Staat en niet van de ADIV alsook naar het gebrek aan personeel om dergelijke gespecialiseerde opdrachten uit te voeren.

Op 4 april 2001 heeft het Comité I een brief ontvangen vanwege de minister van Justitie met de melding dat hij geen opmerkingen te formuleren had betreffende dit verslag.

2. Enkele reacties en uitingen van belangstelling uitgaandevanEuropeseinstellingen,parlementen en nationale regeringen inzake de problematiek van het bestaan van een « Echelon »-netwerk

2.1. De Europese instellingen

2.1.1. 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 Unieverdrag).

Dit verklaart de belangstelling die uitgaat van het Europees Parlement naar de mogelijkheid van een uitgebreid interceptiesysteem van telecommunicatie.

ment le SGR, à des programmes de satellites 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 — pp. 130 et suivantes).

Le présent rapport, actualisé à la date du 31 janvier 2001, présente l'ensemble des constatations déjà publiées par le Comité R au cours de son enquête sur le système Echelon auxquelles se sont ajoutées une série d'informations nouvelles qui n'avaient pas encore été communiquées au Parlement.

Le présent rapport a été approuvé par le Comité R le 1er février 2001 en vue de sa publication.

Par lettre du 22 mars 2001, le ministre de la Défense nationale a transmis ses observations au Comité R. Dans le cadre de la présente problématique le ministre de la Défense nationale a insisté sur l'absence de moyens légaux et humains permettant au SGR d'effectuer des missions spécialisées. Il a rappelé également que la protection du potentiel scientifique et économique du pays est une mission de la Sûreté de l'État et non du SGR.

Le 6 avril 2001, monsieur le ministre de la Justice a fait savoir au Comité R qu'il n'avait pas de remarque à formuler au sujet du présent rapport.

2. Quelques réactions et manifestations de l'intérêt des instances européennes, de parlements et de gouvernements nationaux concernant l'existence d'un réseau « Echelon »

2.1. Les instances européennes

2.1.1. Le 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).

Ceci explique l'intérêt porté par le Parlement européen à l'éventualité d'un système généralisé d'interception des communications.

Op 16 september 1998 heeft het Europees Parlement de volgende resolutie aangenomen:

«Het Europees Parlement (...)

is zich bewust van de cruciale rol van de internationale samenwerking, dank zij elektronische bewakingsmiddelen, om een einde te stellen aan de activiteiten van terroristen, drugshandelaars en van de georganiseerde misdaad of om deze activiteiten te verhinderen;

erkent echter ook dat het van het grootste belang is te kunnen steunen op democratische controlesystemen betreffende het aanwenden van bepaalde technologieën en het gebruiken van de informatie die men daarmee heeft verkregen;

vraagt dat over dergelijke bewakingstechnologieën een echt open debat zou worden gevoerd, zowel in elke lidstaat afzonderlijk als op het niveau van de Europese Unie, alsook dat deze technologieën zouden worden onderworpen aan procedures die instaan voor verantwoordelijkheid op democratisch vlak;

eist dat een gedragscode wordt aangenomen die verzekert dat vergissingen of misbruiken worden rechtgezet;

meent dat het groeiend belang van internet en meer in het algemeen van telecommunicatie op wereldschaal en in het bijzonder het systeem Echelon, alsmede de risico's verbonden met het bedrieglijk misbruik daarvan, het nodig maken maatregelen te nemen met het oog op de bescherming van economische informatie en een doeltreffend coderingssysteem in te voeren (...)».

Op 22 en 23 februari 2000 vergaderde 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 overzien 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/EC 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 2000 was in het bijzonder gewijd aan «Inbreuken op de bescherming van de gegevens buiten de gerechtelijke en politionele samenwerking: het probleem van de intercepties van telecommunicaties (Echelon)».

Le 16 septembre 1998, le Parlement européen a adopté la résolution suivante:

«Le Parlement européen, (...)

est conscient du rôle crucial que joue la coopération internationale, grâce aux moyens de surveillance électronique, lorsqu'il s'agit de mettre un terme ou d'empêcher les activités des terroristes, des trafiquants de drogue, du crime organisé;

reconnaît toutefois également qu'il est essentiel que l'on puisse s'appuyer sur des systèmes de contrôle démocratique en ce qui concerne le recours à des technologies et les informations obtenues;

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;

réclame l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus;

estime que l'importance croissante du réseau internet, et, plus généralement, des télécommunications à l'échelle mondiale et en particulier le système «Echelon», ainsi que les risques de leur utilisation abusive appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace (...)».

Les 22 et 23 février 2000, 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 (II^{e} pilier: politique étrangère et de sécurité commune, III^{e} pilier: coopération policière et judiciaire en matière pénale).

La réunion du mercredi 23 février 2000 était notamment consacrée aux «atteintes à la protection des données en dehors de la coopération judiciaire et policière: le problème des interceptions des télécommunications (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.

Het Europees Parlement besloot op 5 juli 2000 niet in te gaan op de eis van de Groenen om een onderzoekscommissie in te stellen, maar opteerde echter wel voor het principe van het inrichten van een tijdelijke commissie, die zou belast worden met het vaststellen van de reële omvang van het spionagenetwerk Echelon binnen de landen van de Europese Unie.

Tijdens een debat over het Echelon-netwerk op 30 maart 2000 riepen Europese parlementairen op om zo gauw mogelijk het Charter van de fundamentele rechten van de Europese Unie op te stellen en goed te keuren, teneinde de rechten van de burgers een betere juridische bescherming te bieden op het gebied van de nieuwe informatica-technologieën.

De tijdelijke commissie «Echelon» werd met de volgende opdrachten belast:

— nagaan of het systeem voor het intercepteren van communicatie, «Echelon» genaamd, bestaat;

— nagaan of en in welke mate dit systeem voldoet aan de normen van de Europese Gemeenschap met betrekking tot de volgende vragen:

• Zijn de rechten van de burgers beschermd tegen de activiteiten van de geheime diensten?

• Levert de cryptografie een gepaste en voldoende bescherming van het privé-leven van de burgers of moeten er bijkomende maatregelen worden genomen en zo ja, dewelke?

• Hoe kan men de instellingen van de Europese Unie meer bewust maken van de risico's tengevolge van dergelijke activiteiten en welke maatregelen moeten worden genomen?

— nagaan of de Europese industrie gevaar loopt als gevolg van het wereldwijd intercepteren van de communicatie;

— het formuleren van voorstellen voor politieke en wetgevende initiatieven.

Het Europees Parlement heeft een tijdelijke commissie opgericht, veeleer dan een onderzoekscommissie in de betekenis van artikel 193 van het Verdrag van de Europese Unie, aangezien deze laatste alleen binnen het strikte kader van de Europese aangelegenheden over reële onderzoeksbevoegdheden beschikt.

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.

Le 5 juillet 2000, le Parlement européen a décidé de ne pas créer la commission d'enquête réclamée sur l'initiative des «Verts», mais a cependant opté pour le principe de la création d'une commission temporaire chargée d'établir l'ampleur réelle de l'implantation du réseau d'espionnage Echelon dans les pays membres de l'Union européenne.

Lors d'un débat sur le réseau Echelon le 30 mars 2000, des parlementaires européens ont appelé à la rédaction et à l'adoption dans les meilleurs délais de la Charte des droits fondamentaux de l'Union européenne afin d'assurer une meilleure protection juridique des droits des citoyens dans les domaines des nouvelles technologies de l'information.

La commission temporaire d'enquête sur «Echelon» a reçu la mission suivante:

— vérifier l'existence du système d'interception des communications «Echelon»;

— évaluer la compatibilité de ce système avec les normes de la Communauté européenne en ayant égard aux questions suivantes:

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

• la cryptographie assure-t-elle une protection adéquate et suffisante de la vie privée des citoyens ou faut-il prendre des mesures complémentaires, si oui, lesquelles?

• comment rendre les institutions de l'Union européenne plus conscientes des risques causés par de telles activités et quelles mesures prendre?

— vérifier si l'industrie européenne court un risque par l'interception globale des communications;

— émettre des propositions pour des initiatives politiques et législatives.

Le Parlement européen a mis sur pied une commission temporaire plutôt qu'une commission d'enquête au sens de l'article 193 du Traité de l'Union européenne qui n'a de réel pouvoir d'investigation que dans le cadre strict des affaires européennes.

De activiteiten van de inlichtingendiensten noch het intercepteren van communicatie vallen onder de bevoegdheden van de Europese Unie. Bijgevolg zou een onderzoekscommissie van het Europees Parlement ter zake niet de minste bevoegdheid genieten.

De Commissie «Echelon» van het Europees Parlement wordt voorgezeten door het Portugese parlementslid Carlos Cuelho; zijn secretaris is het Duitse parlementslid Gerhard Schmid. De commissie telt drieëndertig parlementsleden, Gérard Deprez is de Belgische vertegenwoordiger.

De leden van deze commissie willen hun invloed en hun overtuigingskracht aanwenden teneinde de inlichtingen te verkrijgen die ze nodig hebben om hun opdracht uit te voeren.

Volgens de pers zou de secretaris van de commissie hebben verklaard dat de commissie wenst over te gaan tot de ondervraging van de heer Michael Hayden, directeur van het Amerikaanse veiligheidsorgaan NSA, over de activiteiten van het «Echelon»-systeem in Europa.

Voorts heeft de commissie blijk gegeven van haar voornemen om de debatten over «Echelon» in de diverse nationale parlementen en regeringen, onder meer in België, van nabij te volgen. Daarbij zal ze aandacht besteden aan de wettelijke grondslagen, de opdrachten, de activiteiten en aan het toezicht op de inlichtingendiensten in de lidstaten van de Europese Unie, de Verenigde Staten, Canada, Australië en Nieuw-Zeeland.

2.1.2. Standpunt van de Commissie van de Europese Unie

Toen hij kort na de vergadering van 23 februari 2000 werd geïnterpelleerd, verklaarde de Nederlandse commissaris Frits Bolkenstein in eerste instantie dat het Echelonsysteem niet meer dan een gerucht was, en dat hijzelf geen aandacht besteedde aan geruchten, alleen aan feiten.

In zijn interventie voor het Europees Parlement op donderdag 30 maart 2000 beantwoordde de heer Erkki Liikanen, de Finse commissaris bevoegd inzake ondernemingen en de informatiemaatschappij, de parlementaire interpellaties, en verklaarde hij dat het type aangehaalde activiteiten «buiten de bevoegdheden van de communautaire wet» viel.

De voorzitter van de Commissie, de heer Romano Prodi, verbond er zich daarentegen wel toe de Commissie haar taak van bewaker van de verdragen te laten vervullen. Hij vertrouwde het technisch beheer van het dossier niet alleen toe aan commissaris Liikanen, maar ook aan de commissaris voor Justitie, de Portugees Antonio Vittorino en aan de commissaris voor de interne markt, de Nederlander Frits Bolkenstein.

Ni l'activité des services de renseignement, ni les interceptions des communications ne tombent dans les compétences de l'Union européenne. Une commission d'enquête du Parlement européen n'aurait donc aucun pouvoir en la matière.

La commission «Echelon» du Parlement européen est présidée par le député portugais Carlos Cuelho et son secrétaire est le député allemand Gerhard Schmid. Elle est composée de trente trois députés; le représentant belge est le député Gérard Deprez.

Les membres de cette commission comptent user de leur influence et de leur pouvoir de persuasion pour obtenir les informations nécessaires à leur mission.

La presse rapporte que le secrétaire de la commission a émis le souhait de questionner M. Michael Hayden, le directeur de la NSA, l'organisme de sécurité américain, sur les actions du système Echelon en Europe.

La commission a également manifesté l'intention de s'intéresser aux discussions menées sur «Echelon» au sein de différents parlements et gouvernements nationaux, notamment en Belgique. Elle s'intéressera aux bases légales, aux missions, aux activités et aux contrôles des services de renseignement des pays membres de l'Union européenne, des États-Unis, du Canada, de l'Australie et de la Nouvelle-Zélande.

2.1.2. La position de la Commission de l'Union européenne

Interpellé peu après la réunion du 23 février 2000, le commissaire hollandais Frits Bolkenstein déclara d'abord que le système «Échelon» n'était qu'une rumeur et que lui-même n'intervenait pas sur des rumeurs, mais sur des faits.

Intervenant devant le Parlement européen le jeudi 30 mars 2000, M. Erkki Liikanen, commissaire finlandais chargé des entreprises et de la société de l'information a répondu aux interpellations parlementaires en déclarant que le type d'activités évoquées tombait «au-delà des compétences de la loi communautaire».

Par contre, le président de la Commission, M. Romano Prodi, s'est quant à lui engagé à ce que celle-ci joue son rôle de gardien des traités; il a confié la gestion technique du dossier au commissaire Liikanen, mais aussi au commissaire pour la Justice, le portugais Antonio Vittorino, et à celui pour le marché interne, le hollandais Frits Bolkenstein.

De Europese Commissie kan inderdaad optreden op verschillende gebieden die tot haar bevoegdheden behoren: de bescherming van het privé-leven van de burgers, de bescherming van technologische gegevens en onderzoek, industriële spionage en de bestrijding van de criminaliteit.

Bijgevolg heeft de Europese Commissie het Amerikaanse ministerie van Buitenlandse Zaken en de Britse overheden om opheldering gevraagd.

In zijn antwoord verklaarde de vice-minister van Buitenlandse Zaken voor Europese Aangelegenheden dat de Amerikaanse regering en de Amerikaanse geheime diensten elk verzoek tot spionage uitgaande van private ondernemingen weigeren, en geen financiële, technische of commerciële informatie inwinnen ten gunste van private ondernemingen.

Van zijn kant verklaarde de permanente vertegenwoordiger van het Verenigd Koninkrijk bij de Europese Unie dat de Britse inlichtingendiensten werken in een wettelijk kader dat het Britse Parlement heeft vastgelegd. In zijn brief preciseert hij dat deze diensten alleen toegelaten intercepties van communicatie verrichten, dit wil zeggen intercepties betreffende de nationale veiligheid, de bescherming van het economisch welzijn van het land en de grote criminaliteit. Voor het overige geeft de Britse regering «geen commentaar op een veronderstelde activiteit van interceptie, ongeacht het ongegrond karakter van de bewuste beweringen».

2.2. Frankrijk

2.2.1. Het Franse Parlement

Op 1 oktober 1998 vroeg de heer Jacques Legendre, senator, aan de Franse eerste minister of deze kon bevestigen dat de Verenigde Staten, Groot-Brittannië en enkele andere Angelsaksische landen een elektronisch spionagenetwerk, «Echelon» genaamd, hadden ingevoerd, en, of dit netwerk werd gebruikt voor het afluisteren van communicaties in het kader van de industriële spionage.

Hij vroeg de eerste minister ook welke maatregelen de regering overwoog om van de bondgenoten te eisen dat ze een einde maakten aan een dergelijke onduldbare operatie.

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 publieke fora aangaande het netwerk «Echelon» genaamd, dat het aan de Commissie Landsverdediging toekwam om een onderzoek in te stellen over een interceptiesysteem

Les lignes possibles d'intervention de la Commission européenne concernent en effet différentes compétences: la sauvegarde de la vie privée des citoyens, la protection des données technologiques et celle de la recherche, l'espionnage industriel et la lutte contre la criminalité.

La Commission européenne a donc adressé une demande de clarification au département d'État américain, ainsi qu'aux autorités britanniques.

Dans sa réponse, le sous-secrétaire d'État aux Affaires européennes déclare que le gouvernement américain et les services secrets américains n'acceptent aucune demande d'espionnage de la part de firmes privées et ne collectent aucune information financière, technique ou commerciale au bénéfice de firmes privées.

Le représentant permanent du Royaume-Uni auprès de l'Union européenne a pour sa part fait savoir que les services de renseignement britanniques travaillent dans un cadre légal fixé par le Parlement britannique. La lettre précise que ces services n'effectuent que des interceptions de communications autorisées, c'est-à-dire celles relatives à la sécurité nationale, la sauvegarde du bien-être économique de la nation et la grande criminalité. Pour le surplus, le gouvernement britannique ne «fait pas de commentaire à propos d'une activité d'interception présumée, quel que soit le caractère non fondé des allégations en question».

2.2. La France

2.2.1. L'Assemblée nationale française

Le 1er octobre 1998, monsieur le sénateur Jacques Legendre a demandé à monsieur le premier ministre de lui faire savoir s'il est exact qu'un réseau électronique d'espionnage connu sous le nom «d'Échelon» a été mis en place par les États-Unis, la Grande-Bretagne et quelques autres pays anglo-saxons et si ce réseau procède à des écoutes motivées par l'espionnage industriel.

Il lui a demandé quelles mesures le gouvernement comptait prendre pour exiger de nos alliés qu'il soit mis un terme à une action aussi intolérable.

Selon le compte-rendu nº 27 de la commission de la Défense nationale et des Forces armées du mardi 29 février 2001 (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'organisa-

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.

De Commissie van Landsverdediging heeft dientengevolge de heer Arthur Paecht benoemd als informatieverslaggever over «de elektronische bewakings- en interceptiesystemen die de nationale veiligheid kunnen in het gedrang brengen».

Op 6 maart 2000 diende de heer Yves Nicolin, volksvertegenwoordiger, een ontwerp van besluit in «strekkende tot het oprichten van een onderzoekscommissie naar de bedreiging van de Franse belangen door het communicatie-interceptienetwerk, Echelon genaamd, en naar de middelen aangewend om de vertrouwelijkheid van de telecommunicatie te beschermen» (1).

Dit laatste voorstel werd verworpen op 22 maart 2000, omdat men vond dat het voortzetten van de informatieopdracht van de heer Paecht binnen de Commissie voor Landsverdediging voorrang moest krijgen boven de oprichting van een onderzoekscommissie.

De heer Paecht overhandigde zijn rapport in oktober 2000 aan de Nationale Assemblee. De besluiten van dit rapport luiden als volgt:

«Er bestaat inderdaad een omvangrijk systeem voor het intercepteren en behandelen van gegevens, met name Echelon. Het bestaat onder vorm van een netwerk. Het gaat hier trouwens om het enige gekende multinationale systeem. Ja, de capaciteiten van dit systeem zijn reeël en performant gezien de veelvuldige zwakheden van informatie- en communicatiesystemen.

Inderdaad is het Echelon systeem afgeweken van zijn oorspronkelijke doelstellingen, die fundamenteel verbonden waren aan de context van de Koude Oorlog en in vergelijking met het eerste UKUSA-verbond tussen de 5 partnerlanden. Het is niet onmogelijk dat de verzamelde gegevens gebruikt werden voor economische doeleinden, zelfs tegen bepaalde leden van de Noord-Altlantische Verdragsorganisatie.

Er werden inderdaad bilaterale banden gesmeed tussen de USA, het UKUSA en andere inlichtingendiensten omwille van veiligheidsredenen in verband met militaire behoeften of omwille van de noodzaak om het terrorisme of het groot banditisme te bestrijden.

(1) Vrije vertaling.

tion 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.

La commission de la Défense nationale a dès lors 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».

Le 6 mars 2000, le député Yves Nicolin a déposé une proposition de résolution «tendant à la création d'une commission d'enquête sur la mise en cause des intérêts français par le réseau d'interception des communications dit 'système Echelon', ainsi que les moyens déployés pour préserver la confidentialité des télécommunications» (1).

Cette dernière proposition a été rejetée le 22 mars 2000 considérant que la poursuite de la mission d'information de M. Paecht au sein de la commission de la Défense nationale était préférable à la création d'une commission d'enquête.

M. Paecht a déposé son rapport à l'Assemblée nationale en octobre 2000 dont les conclusions générales sont les suivantes:

«Oui, il existe bien un vaste système d'interception et de traitement des informations nommé Échelon. Il est organisé en réseau. Il s'agit d'ailleurs du seul système multinational connu. Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. (...)

Oui, le système Échelon a divergé par rapport à ses objectifs initiaux, qui étaient fondamentalement liés au contexte de la guerre froide et par rapport même aux conditions du pacte initial UKUSA entre les cinq partenaires. Il n'est pas impossible que des informations recueillies soient utilisées à des fins économiques, voire à l'encontre de certains membres de l'alliance atlantique. (...)

Oui, des liens bilatéraux ont été organisés entre les États-Unis, l'UKUSA et d'autres services de renseignement pour des raisons de sécurité liées à des besoins militaires ou à la nécessité de lutter contre le terrorisme ou le grand banditisme.

(1) Traduction libre.

Inderdaad, Echelon kan een gevaar vormen voor de algemene en individuele vrijheden.» (1).

2.2.2. Het standpunt van de Franse regering

In antwoord op een vraag van senator Legendre, verklaarde de Franse eerste minister:

«(...) Er bestaat geen gezag dat technisch kan beletten dat radiocommunicaties worden onderschept wanneer deze circuleren in een wereld die niet stoffelijk begrensd is.

Overigens (...) de economische belangen van deze activiteiten zijn bijzonder groot, als je er rekening mee houdt dat de communicatienetwerken verbonden zijn met de interne systemen van ondernemingen. We moeten op deze onvermijdelijke technologische ontwikkelingen reageren door een voluntaristisch beleid te voeren in ten minste twee richtingen.(...)

(...) Enerzijds moedigt de Franse regering de ontwikkeling aan van middelen die het mogelijk maken de vertrouwelijkheid en de integriteit van gevoelige informatiesystemen te verzekeren.

(...)

(...) Het analyseren van de risico's, het ontwikkelen van beveiligingsinstrumenten, het evalueren van de veiligheid van informatiesystemen zijn taken waaraan voorrang moet worden verleend en die met name zijn toevertrouwd aan de centrale dienst voor de veiligheid van informatiesystemen van het algemeen secretariaat van het ministerie van Landsverdediging (...).

Anderzijds is het duidelijk dat de inspanningen die zijn geleverd voor het onderscheppen van communicatiesystemen voortvloeien uit belangrijke behoeften op het vlak van veiligheid en defensie.

Deze houden bijvoorbeeld verband met het controleren van misdadige of terroristische activiteiten, het voorkomen en opvolgen van militaire conflicten of met het bestrijden van clandestiene programma's voor de proliferatie van massavernietigingswapens. (...)

(...) Deze materies overstijgen het nationaal belang en het is onvermijdelijk dat staten zoeken naar nieuwe vormen van samenwerking.

Het ontwikkelen van beveiligingsinstrumenten enerzijds, het leveren van belangrijke inspanningen om het hoofd te bieden aan de versnelde ontwikkeling van technologieën anderzijds en, ten slotte, het opstellen van geloofwaardige juridische en samenwerkingskaders vormen de belangrijkste doelstellingen van het beleid dat de regering op dit vlak voert.» (1) (Franse Senaat, 3 december 1998 — Industrieel spionagenetwerk.)

(1) Vrije vertaling.

Oui, Échelon peut constituer un danger pour les libertés publiques et individuelles.» (1)

2.2.2. La position du gouvernement français

Répondant au sénateur Legendre, le premier ministre français a notamment déclaré:

«(...) Il n'existe pas d'autorité qui puisse empêcher techniquement, l'interception de communications radioélectriques lorsque celles-ci sont véhiculées dans un espace mondial qui ne connaît pas de frontière physique.

Par ailleurs, (...) les enjeux économiques de ces activités sont considérables, compte tenu de l'interconnexion des réseaux de communication avec les systèmes internes des entreprises. Il convient de répondre à ces développements inéluctables au plan des technologies par une politique volontariste dans au moins deux directions.

D'une part, le gouvernement français encourage le développement des moyens permettant de répondre aux besoins de confidentialité et d'intégrité des systèmes d'information sensibles.

(...)

L'analyse des risques, le développement des moyens de protection, l'évaluation de la sécurité des systèmes d'information constituent des tâches prioritaires confiées notamment au service central de la sécurité des systèmes d'information du secrétariat général de la défense nationale. (...)

D'autre part, il est également clair que les investissements consentis pour l'interception des systèmes de communication répondent à des besoins de sécurité et de défense importants.

Ceux-ci sont liés, par exemple à la surveillance des activités criminelles ou terroristes, à la prévention et au suivi des crises militaires ou encore à la lutte contre les programmes clandestins de prolifération des armes de destruction massive.

Ces sujets présentent un caractère transnational et les États recherchent nécessairement, dans ces domaines, des formes nouvelles de partenariat.

Le développement de moyens de protection d'un côté, la mise en place d'investissements nécessaires pour faire face à l'essor accéléré des technologies de l'autre, enfin l'établissement de cadres juridiques et de coopération crédibles constituent donc les principales orientations de la politique du gouvernement dans ces domaines.» (Sénat français, 3 décembre 1998 — Réseau d'espionnage industriel.)

(1) Traduction libre.

Terwijl hij officieel verwees naar de dreiging van het Echelon-netwerk of naar andere aanslagen met behulp van de informatica, heeft de Franse eerste minister Lionel Jospin zijn beleid inzake de veiligheid van informatiesystemen opnieuw gedefinieerd.

Op de Ministerraad van 15 maart 2000 benoemde de regering de heer Henri Serres, algemeen ingenieur telecommunicatie, tot directeur belast met de veiligheid van de informatiesystemen.

Deze maatregel past in het kader van het veiligheidsbeleid dat de Franse regering wenst te voeren, parallel met de versnelde ontwikkeling van de instrumenten van de informatiemaatschappij in de administratie en de overheidsdiensten.

Dit beleid, dat ten dienste staat van de burger en de onderneming, moet het ook mogelijk maken de vertrouwelijkheid van de omgang en het privé-leven te beschermen.

De nieuwe directeur krijgt de opdracht de «Centrale Dienst voor de veiligheid van de informatiesystemen» (SCSSI — Service central de la Sécurité des Systèmes d'information), die sinds 1 januari 1999 deel uitmaakt van het «Algemeen Secretariaat Nationale Veiligheid» (SGDN: Secrétariat général de la défense nationale), om te vormen tot een volwaardige directie van de SGDN, belast met de veiligheid van de informatiesystemen op interministerieel niveau.

Deze beslissing geeft niet alleen blijk van een schaalvergroting met betrekking tot de middelen waarmee de regering zichzelf op dit gebied wenst uit te rusten, maar ook van haar voornemen de inspanningen van de Staat beter te coördineren.

In het communiqué van de Franse regering lezen we:

«Begin 2000 hebben de aanval van niet-geïdentificeerde computerpiraten op de websites van grote Amerikaanse ondernemingen in de sector van de e-commerce, — en de blokkering ervan gedurende enkele uren —, alsook het bestaan van Echelon, een wereldwijd netwerk voor elektronische afluisteroperaties, of nog het in twijfel trekken van bepaalde, voor het «grote publiek» bestemde producten, de bezorgdheid over de nieuwe bedreigingen en de noodzaak om de bescherming van onze netwerken te verzekeren volop in de schijnwerpers geplaatst.

Op dit gebied moeten de regering en de administratie, alsook de openbare diensten, een voortrekkersrol spelen. Om al deze redenen heeft de regering beslist in 2000, uitgaand van de middelen van de SCSSI, een nieuwe centrale directie op te richten die, binnen het Algemeen Secretariaat Nationale Veiligheid, wordt belast met de veiligheid van de informatiesystemen (DCSSI).» (1).

(1) Vrije vertaling.

En évoquant officiellement la menace du réseau Échelon ou d'autres attaques informatiques, le premier ministre français Lionel Jospin a donc redéfini sa politique en matière de sécurité des systèmes d'information.

En Conseil des ministres du 15 mars 2000, le gouvernement a nommé monsieur Henri Serres, ingénieur général des télécommunications, comme directeur chargé de la sécurité des systèmes d'information.

Cette mesure intervient dans le cadre de la politique de sécurité qu'entend promouvoir le gouvernement français, parallèlement au développement accéléré des outils de la société de l'information dans l'administration et les services publics.

Cette politique, au service du citoyen et de l'entreprise, doit aussi permettre de protéger la confidentialité des échanges et la vie privée.

Il reviendra au nouveau directeur de transformer le «Service central de la sécurité des systèmes d'information», intégré au «Secrétariat général de la défense nationale» depuis le 1er janvier 1999, en direction de plein exercice du SGDN, chargée de la sécurité des systèmes d'information au niveau interministériel.

Cette décision marque à la fois un changement d'échelle dans les moyens dont le gouvernement souhaite se doter dans ce domaine et la volonté d'assurer une meilleure coordination des efforts de l'État.

Le communiqué du gouvernement français précise:

«Début 2000, l'attaque par des pirates informatiques non identifiés — et l'immobilisation pendant quelques heures — des sites internet de sociétés américaines majeures du commerce électronique, ainsi que l'existence du réseau mondial d'écoute électronique Échelon, ou la mise en cause de certains produits «grand public», ont mis au premier plan de l'actualité les préoccupations liées aux nouvelles menaces et la nécessité d'assurer la protection de nos réseaux.

Dans ce domaine, le gouvernement et l'administration, ainsi que les services publics, devront donner l'exemple. Pour cet ensemble de raisons, le gouvernement a décidé de la création, en 2000, à partir des moyens du SCSSI, d'une nouvelle direction centrale de la sécurité des systèmes d'informations (DCSSI) au Secrétariat général de la défense nationale.» (1).

(1) Traduction libre.

Op 23 februari 2000 herhaalde Elisabeth Guigou, minister van Justitie, in het Parlement de voorzorgsraadgevingen die ondernemingen moeten volgen om zich te beschermen tegen spionage en de veiligheid te verzekeren van gegevens die met behulp van de nieuwe technologieën circuleren: «Deze gegevens mogen nooit essentiële informatie bevatten, vooral wanneer de verbinding verloopt via satellieten, in hoofdzaak in het kader van internationale verbindingen.»

2.2.3. Het activiteitenverslag 1999 van de «Commission nationale de contrôle des interceptions de sécurité (CNCIS)»

De Franse wet van 10 juli 1991 betreffende de geheimhouding van briefwisselingen uitgegeven via de telecommunicatie, bepaalt de motieven die de administratieve intercepties van communicaties kunnen rechtvaardigen (met name terrorisme, georganiseerde misdaad, de nationale veiligheid), maar ook het behoud van het economisch en wetenschappelijk potentieel.

Het 8e activiteitenverslag 1999 van de «Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS)» toont aan dat, in de loop van het jaar 1999, 4 577 veiligheidsintercepties werden toegelaten in Frankrijk, waarvan er 186, i.e. 4 %, bedoeld waren om het economisch en wetenschappelijk potentieel veilig te stellen.

2.2.4. Reactie van de gerechtelijke macht

Op dinsdag 4 juli 2000 schreef de Franse krant «*Le Figaro*» dat de procureur van de Republiek van Parijs de «Direction de la surveillance du territoire» (DST: dienst belast met het bewaken van het grondgebied) de opdracht had gegeven een inleidend onderzoek te voeren naar het inlichtingennetwerk «Echelon».

Het parket van Parijs was van mening dat de illegale afluisterpraktijken, die met behulp van dit interceptiesysteem plaatsvonden, onder de toepassing van de artikelen 411-6 en 226-15 van het Franse Strafwetboek konden vallen en konden worden beschreven als «een schending op de wezenlijke belangen van de natie» en als «een schending van het briefgeheim via telecommunicatie».

Dit onderzoek werd op 24 mei 2000 geopend ingevolge een klacht die de Europees volksvertegenwoordiger Thierry Jean-Pierre op 2 mei had neergelegd, omdat hij zich zorgen maakte over praktijken «van aard om ernstig nadeel toe te brengen aan al onze medeburgers, alsmede aan onze economische en nationale belangen».

De DST is een politie- en inlichtingendienst die bevoegd is «om op het Franse grondgebied activiteiten op te sporen en te voorkomen, die geïnspireerd,

Le ministre de la Justice, Elisabeth Guigou, a rappelé devant l'Assemblée nationale le 23 février 2000 les conseils de prudence aux entreprises pour se préserver de l'espionnage et assurer la sécurité des renseignements qui transitent par les nouvelles technologies: «Le contenu de ces renseignements ne doit jamais comporter d'information vitale, surtout lorsque la liaison est relayée par un satellite de rediffusion, principalement dans les connexions internationales.»

2.2.3. Le rapport d'activité 1999 de la «Commission nationale de contrôle des interceptions de sécurité» (CNCIS)

La loi française du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit les motifs qui justifient la conduite d'interceptions administratives de communications, à savoir, le terrorisme, la criminalité organisée, la sécurité nationale, mais aussi la sauvegarde du potentiel économique et scientifique.

Le 8e rapport d'activités 1999 de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) indique qu'au cours de l'année 1999, 4 577 interceptions de sécurité ont été autorisées en France dont 186 à des fins de sauvegarde du potentiel économique et scientifique, soit 4 %.

2.2.4. Réactions du pouvoir judiciaire

Le journal français *Le Figaro* du mardi 4 juillet 2000 annonce que le procureur de la République de Paris a chargé la Direction de la surveillance du territoire (DST) d'effectuer une enquête préliminaire sur le réseau de renseignement «Échelon».

Selon le parquet de Paris, les écoutes illégales qui seraient pratiquées par ce système d'interception pourraient être visées par les articles 411-6 et 226-15 du Code pénal et qualifiées ainsi d'«atteinte aux intérêts fondamentaux de la nation» et d'«atteinte au secret des correspondances émises par voie de télécommunications».

Cette enquête a été déclenchée le 24 mai 2000 suite à une plainte déposée le 2 mai 2001 par le député européen Thierry Jean-Pierre qui s'inquiète de pratiques «de nature à porter un préjudice considérable à l'ensemble de nos concitoyens, de nos intérêts économiques et nationaux».

La DST est un service de police et de renseignement qui a pour compétence de rechercher et de prévenir, sur le territoire de la République française, les activi-

gelanceerd of gesteund worden door vreemde mogendheden, en die van aard zijn de veiligheid van het land te bedreigen en, meer in het algemeen, om dergelijke activiteiten te bestrijden».

In die hoedanigheid oefent de «Direction de la surveillance du territoire» een opdracht uit die verband houdt met de landsverdediging (1).

2.3. De Duitse Bondsrepubliek

2.3.1. Besprekingen die plaatsvonden in het Parlement (Deutscher Bundestag)

Parlementsleden van de FDP-partij (Freie Democraten) hebben op 11 april 2000 vragen gesteld aan de Duitse federale regering betreffende «het afluistersysteem per satelliet 'Echelon', aangewend door de Verenigde Staten en vier andere Staten» (verwijzingen 14/2964).

Deze fractie heeft de regering aangespoord haar aandacht te richten op het STOA-verslag dat besproken werd in het Europees Parlement.

In haar antwoord merkt de Duitse federale regering op dat er geen enkele vaststelling voorhanden is volgens welke het privé-leven van de burgers of de commerciële mogelijkheden van de Duitse economie in gevaar zouden gebracht worden door een algemeen afluistersysteem.

2.4. Nederland

2.4.1. De belangstelling van de Nederlandse overheden

Op 20 januari 2001 bracht de Nederlandse minister van Landsverdediging aan de regering naar aanleiding van de beroering over Echelon en na onderzoek van onder meer open bronnen, zoals de verslagen van het Vast Comité I, een omstandige notitie uit over het «grootschalig afluisteren van telecommunicatiesystemen» (2).

De Nederlandse regering verklaart dat zij niet beschikt over eigen en door de in verband met Echelon genoemde regeringen, bevestigde informatie over het bestaan van «Echelon», maar op grond van de thans beschikbare informatie, onderzoeken en openbare bronnen, acht zij het aannemelijk dat het Echelonnetwerk bestaat.

(1) Decreet nr. 82-1100 van 22 december 1982 tot vaststelling van de bevoegdheden van de «Direction de la surveillance du territoire».

(2) Beschikbaar op www.nrc.nl/W2/Lab/Echelon/doc010120.html.

tés inspirées, engagées ou soutenues par des puissances étrangères et qui sont de nature à menacer la sécurité du pays, et, plus généralement, de lutter contre ces activités.

À ce titre, la direction de la surveillance du territoire exerce une mission se rapportant à la défense (1).

2.3. La République fédérale d'Allemagne

2.3.1. Les discussions au Parlement (Deutscher Bundestag)

Des parlementaires du parti FDP (Freie Democraten) ont posé des questions au gouvernement fédéral le 11 avril 2000 concernant le système d'écoutes par satellites «Échelon» mis en œuvre par les États-Unis et quatre autres États (références 14/2964).

Ce groupe parlementaire a exhorté le gouvernement à porter son attention sur le rapport STOA discuté au Parlement européen.

Dans sa réponse, le gouvernement fédéral constate qu'il n'existe aucune constatation selon laquelle la vie privée des citoyens ou les capacités commerciales de l'économie allemande seraient mises en péril par un système d'écoutes généralisé.

2.4. Les Pays-Bas

2.4.1. L'intérêt des autorités néerlandaises

Le 20 janvier 2001, suite aux remous causés par Echelon, et après examen de diverses sources ouvertes, parmi lesquelles les rapports du Comité R, le ministre néerlandais de la Défense nationale a présenté une note circonstanciée intitulée «l'écoute à grande échelle des systèmes de télécommunication» (2).

Le gouvernement néerlandais déclare qu'il ne dispose pas d'information propre, confirmée par les gouvernements cités dans l'affaire «Echelon», sur l'existence de ce réseau. Mais sur base de l'information disponible par enquêtes et sources ouvertes, il estime l'existence du réseau Echelon plausible.

(1) Décret nº 82-1100 du 22 décembre 1982 fixant les attributions de la direction de la surveillance du territoire.

(2) Disponible sur www.nrc.nl/W2/Lab/Echelon/doc010120.html.

Niet alleen overheden maar ook burgers, het bedrijfsleven en criminele organisaties kunnen dergelijke activiteiten plegen.

Voor de Nederlandse regering is het grootschalig afluisteren van telecommunicatiesystemen een activiteit van opsporings-, veiligheids- en inlichtingendiensten van «vele landen met uiteenlopende politieke kleur».

In open bronnen worden melding gemaakt van de Verenigde Staten, het Verenigd Koninkrijk, Rusland, China, Frankrijk, Duitsland, Zwitserland en Denemarken. Ook Nederland wordt genoemd, maar de regeringsnotitie laat achterwege te bevestigen of te ontkennen of dit laatste ook klopt.

In Nederland bestaat er een wettelijk kader voor interceptie en selectie van zowel kabelgebonden als niet-kabelgebonden telecommunicatie.

De feitelijke uitvoering van de interceptie en selectie van niet-kabelgebonden telecommunicatie ten behoeve van de Militaire Inlichtingendienst gebeurt bij de Afdeling Verbindingsinlichtingen van de Militaire Inlichtingendienst (de MID).

Politiediensten en de BVD (Binnenlandse Veiligheidsdienst) zijn binnen de daartoe door de wet gestelde grenzen bevoegd tot het aftappen van kabelgebonden telecommunicatie.

Volgens de Nederlandse regering schept de Nederlandse wetgeving voldoende waarborgen tegen onbevoegde inbreuken op de privacy van de burger.

De bevoegdheden van de BVD en de MID op dit terrein worden momenteel besproken in een wetsvoorstel dat tevens een aantal grenzen stelt (onder meer lastgeving vooraf, toetsing op proportionaliteit en subsidiariteit).

Bij het grootschalig afluisteren van internationaal telecommunicatieverkeer speelt de vraag naar de toepassing van nationale rechtsmacht versus internationaal recht.

Bij de beantwoording van deze vraag bestaat er op dit moment in Nederland een voorkeur voor de opvatting dat het internationaal recht geen beperkingen kan opleggen aan de uitoefening van rechtsmacht over handelingen die verricht worden op eigen grondgebied of op een plaats waar andere landen geen rechtsmacht bezitten, bijvoorbeeld op een schip op volle zee of op een satelliet in de ruimte.

Er bestaat in Nederland geen wetgeving die mogelijkheden biedt om het afluisteren van telecommunicatie in dit verband tegen te gaan. Het staat vrijwel vast dat dergelijke wetgeving ook niet handhaafbaar zou zijn.

De bescherming van het telecommunicatiegeheim van burgers dient te worden gezocht in het maken van

Non seulement les autorités, mais aussi les citoyens, les entreprises et les organisations criminelles sont en mesure de pratiquer de telles activités.

Le gouvernement néerlandais estime que l'écoute à grande échelle des systèmes de télécommunication est une activité pratiquée par les services d'enquêtes, de sécurité et de renseignement de «beaucoup de pays de couleurs politiques différentes».

Les sources ouvertes citent les États-Unis, le Royaume-Uni, la Russie, la Chine, la France, l'Allemagne, la Suisse et le Danemark. Les Pays-Bas sont aussi cités mais la note du Gouvernement s'abstient de le confirmer ou de le démentir.

Il existe aux Pays-Bas un cadre légal pour l'interception et le repérage des communications aussi bien par câbles que sans fil.

L'interception et le repérage des communications sans fil au profit des services de renseignement militaire (MID) et civil (Binnenlandse inlichtingendienst — BVD) est effectuée par la section COMINT du Militaire Inlichtingendienst (MID).

Les services de police et le BVD peuvent procéder à l'interception de communication par câbles dans les limites que la loi leur impose.

Selon le gouvernement néerlandais, la législation de ce pays offre des garanties suffisantes contre les atteintes intempestives à la vie privée des citoyens.

Les compétences du BVD et du MID en la matière sont actuellement discutées à l'occasion d'une proposition de loi qui fixe en même temps un certain nombre de limites (entre autres, un mandat préalable et une appréciation de la mesure sur base du principe de la proportionnalité et de la subsidiarité).

L'interception à grande échelle du trafic international des télécommunications pose la question de l'application du droit national à l'encontre du droit international.

Pour répondre à cette question, les Pays-Bas privilégient l'idée que le droit international ne peut poser de limite à l'exercice d'une juridiction sur des actes posés sur son propre territoire ou à un endroit où les autres pays n'ont aucune juridiction, par exemple, sur un navire de haute mer ou sur un satellite dans l'espace.

À cet égard, il n'existe aucune législation aux Pays-Bas qui donne la possibilité de s'opposer à l'interception des télécommunications. Une telle législation serait par ailleurs impossible à faire appliquer.

La protection du secret des télécommunications des citoyens devrait être recherchée dans la conclusion

internationale afspraken, die aan de burger de mogelijkheid bieden zich te verweren tegen het onbevoegd afluisteren en intercepteren. De juridische consequenties van bovengenoemde stellingnamen dienen nog verder te worden bediscussieerd. De Nederlandse regering neemt zich voor haar standpunt te verduidelijken.

Toch ontkent de Nederlandse minister van Landsverdediging dat er een verband zou bestaan tussen de afluisteractiviteiten van de Amerikaanse regering, en die van de Europese politie- en veiligheidsdiensten.

Hij vermeldt dat de vergaderingen van het «International Law Enforcement Telecommunications Seminar (ILETS)» en van de werkgroep «Politiële Samenwerking» binnen de derde pijler van de Europese Unie, niet bedoeld zijn om als dergelijke schakel te functioneren.

Tevens ontkent hij dat deze relatie zou moeten leiden tot een pan-Europees afluistersysteem waarop de Amerikaanse regering, door middel van het FBI, grote invloed zou hebben.

Voor de minister is het «ILETS» een informele conferentie van vertegenwoordigers van Europese politie- en veiligheidsdiensten en vertegenwoordigers van deze diensten uit Australië, Canada, Nieuw-Zeeland, Noorwegen en de Verenigde Staten. Het «ILETS» is bedoeld om informatie uit te wisselen over methoden en technieken voor het bevoegd aftappen van telecommunicatiesystemen binnen de eigen landsgrenzen.

De EU-werkgroep «Politiële Samenwerking» tracht het beleid aangaande het bevoegd aftappen van telecommunicatiesystemen op Europees niveau te harmoniseren.

Op 22 januari 2001 vond een openbare hoorzitting plaats door de Vaste Kamercommissie van Justitie. Zij onderzocht in hoeverre Nederland aan het internationale spionagenetwerk Echelon heeft deelgenomen.

Verschillende personen namen aan dit rondtafelgesprek deel, onder wie landgenoot Jean-Marc Dinant, (expert door het Vast Comité I gekozen voor het verslag aan de Belgische Senaat), de Britse journalist Duncan Campbell, de Nederlandse journalist Cees Wiebes (co-auteur van het boek *Villa Maarheeze* — de locatie van de voormalige Nederlandse Buitenlandse Veiligheidsdienst) en Maurice Wesseling (auteur van «Bits of Freedom — organisatie voor burgerrechten op de elektronische snelweg»).

Volgens deze laatstgenoemde moet er meer parlementaire controle op afluistersystemen komen.

d'accords internationaux destinés à donner la possibilité aux citoyens de se défendre contre les écoutes et interceptions illégales. Les conséquences juridiques des prises de position précitées doivent encore être discutées de façon plus approfondie. Le Gouvernement néerlandais s'emploie à préciser sa position.

Le ministre néerlandais de la Défense nationale dément cependant qu'il puisse exister un lien entre les interceptions du Gouvernement américain et celles des services européens de police et de renseignement.

Il indique que les réunions du «International Law Enforcement Telecommunications Seminar (ILETS)» et celles du groupe de travail «Coopération policière» organisées dans le cadre du troisième pilier de l'Union européenne ne sont pas destinées à faire ce lien.

Il dément également que cette relation devrait conduire à un système d'écoutes pan-européen sur lequel le gouvernement américain exercerait une grande influence par le biais du FBI.

Suivant le ministre, ILETS est une conférence informelle rassemblant des représentants de services européens de police et de sécurité ainsi que des représentants de ces mêmes services de l'Australie, du Canada, de la Nouvelle Zélande, de la Norvège et des États-Unis. Elle est destinée à échanger de l'information sur les méthodes et techniques d'interception légale de systèmes de télécommunications à l'intérieur des frontières de ces États.

Le groupe de travail «Coopération policière» tente d'harmoniser au niveau européen la politique des interceptions légales des systèmes de télécommunications.

Le 22 janvier 2001 s'est tenue une réunion publique de la commission permanente de la Justice du parlement néerlandais. Celle-ci a examiné en quoi les Pays-Bas seraient impliqués dans le réseau international d'espionnage Echelon.

Parmi les intervenants à cette table ronde, notre compatriote Jean-Marc Dinant (un des experts choisis par le Comité R pour rédiger son rapport au Sénat), le journaliste britannique Duncan Campbell, le journaliste néerlandais Cees Wiebes (co-auteur du livre *Villa Maarheeze* consacré au défunt IDB, Inlichtingendienst Buitenland, le service de renseignement extérieur des Pays-Bas) et M. Maurice Wesseling (de l'organisation «Bits of Freedom» qui lutte pour le droit des citoyens sur les autoroutes de l'information).

Selon ce dernier, il devrait y avoir plus de contrôle parlementaire sur les systèmes d'écoute.

2.5. De Verenigde Staten

2.5.1. De interesse van het Amerikaans Congres : het verslag van het NSA aan het Congres

Naar aanleiding van een bepaling die werd ingediend in de « Intelligence Authorisation Act for Fiscal Year 2000 » op aanvraag van de Amerikaanse afgevaardigde Bob Barr (Republikein van de staat Georgia), hebben de « Director of Central Intelligence », de « Director of the National Security » en de « Attorney General » van de Verenigde Staten in februari 2000 een verslag voorgelegd aan het Amerikaanse Congres « describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance ».

Het Comité I heeft in mei 2000 kennis genomen van dit omvangrijk verslag (1).

De vraag van het Amerikaanse Congres vertolkte de vrees voor de aantasting van de grondwettelijke rechten van de Amerikaanse burgers door het Echelon-netwerk.

De benaderingswijze van afgevaardigde Barr is inderdaad enkel en alleen gericht op de bescherming van het privé-leven van de Amerikaanse burgers. Hij gaat uit van de vaststelling dat een groot deel van het wetgevend arsenaal betreffende het domein van de privé-sfeer enerzijds en de inlichtingsactiviteiten van de Staat anderzijds, teruggaan tot de jaren '70 en de nieuwe instrumenten voor de gegevensuitwisseling niet langer naar behoren dekken.

Het door de Amerikaanse administratie voorgelegde verslag bevestigt eens te meer op gedetailleerde wijze dat het NSA en het FBI nauwgezet de « Foreign Intelligence Surveillance Act (FISA) — the Executive Order No 12333 », evenals het 4de Amendement van de Amerikaanse Grondwet, dat aan elke burger uit het land de waarborg biedt van « the right to be secure in their persons, their houses, papers and effects against unreasonable searches and seizures », in acht nemen.

De elektronische bewaking wordt uitgevoerd door agenten van de Amerikaanse inlichtingengemeenschap met als doel informatie in te winnen over het buitenland en de contraspionage.

Gelet op haar indringend karakter en de gevolgen voor het privé-leven, wordt deze bewakingswijze onderworpen aan een strikte wetgeving en aan een grondige controle, waarbij de wederzijdse belangen

(1) « Legal Standards for the Intelligence Community in Conducting Electronic Surveillance », beschikbaar op http://www.fas.org/irp/nsa/standards.html, http:/cryptome.org/dod5240-l-r.htm, http://cryptome.org/nsa-ussid18.htm en http://cryptome.org/fbi-fic-fci.htm.

2.5. Les États-Unis

2.5.1. L'intérêt du Congrès américain : le rapport de la NSA

Suite à une disposition introduite dans « The Intelligence Authorisation Act for Fiscal Year 2000 » à la demande du député américain Bob Barr (Républicain, Géorgie), le « Director of Central Intelligence », le « Director of the National Security » et l'« Attorney General » des États Unis ont présenté en février 2000 un rapport au Congrès américain « describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance ».

Le Comité R a pris connaissance de ce volumineux rapport en mai 2000 (1).

La demande du Congrès américain traduisait ses craintes que les droits constitutionnels de citoyens américains soient atteints par le réseau Echelon.

L'angle d'approche du député Barr est effectivement concentré sur la protection de la vie privée des citoyens américains seulement, en partant de la constatation qu'une bonne partie de l'arsenal législatif relatif au domaine de la vie privée d'une part et des activités de renseignements de l'État, d'autre part, date des années 70 et ne recouvre plus adéquatement les nouveaux instruments d'échange d'informations.

Le rapport présenté par l'administration américaine réaffirme donc de manière circonstanciée que la NSA et le FBI respectent scrupuleusement le « Foreign Intelligence Surveillance Act (FISA) — the Executive Order N° 12333 » ainsi que le quatrième amendement de la Constitution américaine qui garantit à chaque citoyen de ce pays « the right to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures ».

La surveillance électronique est menée par des agents de la communauté américaine du renseignement à des fins de renseignement extérieur et de contre-espionnage.

Etant donné son caractère intrusif et ses implications pour la vie privée, ce mode de surveillance est soumis à une réglementation stricte ainsi qu'à un contrôle approfondi qui traduit une mise en balance

(1) « Legal Standards for the Intelligence Community in Conducting Electronic Surveillance » disponible sur : http://www.fas.org/irp/nsa/standards.html , http://cryptome.org/dod5240-l-r.htm, http://cryptome.org/nsa-ussid18.htm et http://cryptome.org/fbi-fic-fci.htm.

van de regering en de rechten van de « United States persons » tegen mekaar worden afgewogen.

Dit verslag omschrijft als « US person » : elke burger van de Verenigde Staten, elke buitenlander die de wettelijke toelating heeft om er permanent te wonen, elke vennootschap waarvan een aanzienlijk deel van haar leden Amerikaanse staatsburgers zijn of buitenlanders die een wettelijke toelating hebben om in de Verenigde Staten te wonen, of nog, elke in dat land gevestigde vennootschap, op voorwaarde dat er zich tussen haar aandeelhouders geen vertegenwoordiger bevindt van een buitenlandse mogendheid.

Om een elektronische bewakingsoperatie te kunnen uitvoeren op een Amerikaans burger die woont in de Verenigde Staten, moet men dus een ordonnantie verkrijgen van de « Foreign Intelligence Surveillance Court ».

Bevindt deze persoon zich in het buitenland, dan moet de Attorney General (nb. de minister van Justitie) de bewaking goedkeuren. De bewaking zal toegestaan worden als de persoon in kwestie bijvoorbeeld ervan verdacht wordt een agent te zijn van een buitenlandse mogendheid.

De toestemming wordt slechts verleend als de gezochte informatie op geen enkele andere, en minder indringende manier kan bekomen worden.

De elektronische bewaking moet in elk geval zo uitgevoerd worden dat ze de inzameling, de weerhouding en de verspreiding van informatie betreffende niet-toestemmende Amerikaanse burgers tot een minimum herleidt.

De Amerikaanse beschermingsvoorschriften inzake elektronische bewaking die het verkrijgen van inlichtingen en contraspionage beogen, zijn uitsluitend van toepassing op Amerikaanse burgers.

Volgens de krant *Le Monde* van 10 maart 2000, zou Georges Tenet, de huidige directeur van de CIA, voor het Amerikaanse Congres verklaard hebben dat de Verenigde Staten hun inlichtingendiensten niet zouden gebruiken om hun economische activiteiten te promoten.

De CIA zou nochtans wel tussenkomen indien ze zou merken dat de belangen van een Amerikaans bedrijf geschaad worden door een tegenstander die oneerlijk handelt tegenover een klant.

Het dossier zou dan doorgegeven worden aan de leden van het Congres, aan het Ministerie van Buitenlandse Handel of aan het Secretariaat voor Handel, opdat zij er de nodige conclusies zouden kunnen uit trekken. Het betreft dus een loutere defensieve actie.

des intérêts du Gouvernement et des droits des « United States persons ».

Le rapport définit comme « US person » tout citoyen des États-Unis, tout étranger légalement admis à y résider de manière permanente, toute société dont un nombre substantiel de membres sont citoyens américains ou étrangers légalement admis à résider aux États-Unis ou encore toute société implantée dans ce pays à condition qu'elle ne compte aucun représentant d'une puissance étrangère parmi ses membres.

Ainsi, pour pouvoir mener une opération de surveillance électronique sur un citoyen américain situé aux États-Unis, il est nécessaire d'obtenir une ordonnance de la « Foreign Intelligence Surveillance Court ».

Si cette personne se trouve à l'étranger, l'Attorney General (le ministre de la Justice), doit approuver la surveillance. La surveillance sera autorisée si la personne cible est, par exemple, suspectée d'être un agent d'une puissance étrangère.

L'autorisation n'est accordée que si l'information recherchée ne peut être recueillie par aucun autre moyen technique moins intrusif.

En toute circonstance, la surveillance électronique doit être menée de manière telle qu'elle réduise au minimum la collecte, la détention et la diffusion d'informations au sujet de citoyens américains non consentants.

Les règles américaines de protection à l'égard de la surveillance électronique à des fins de renseignement et de contre-espionnage ne s'appliquent pas à d'autres personnes que les citoyens américains.

Selon le journal *Le Monde* du 10 mars 2000, Georges Tenet, directeur actuel de la CIA, aurait déclaré devant le Congrès américain que les États-Unis n'utilisaient pas leurs services de renseignement pour promouvoir leurs activités économiques.

La CIA interviendrait néanmoins lorsqu'elle observe qu'une entreprise américaine est grugée dans ses intérêts par un concurrent qui agit malhonnêtement envers un client.

Le dossier serait alors soumis aux membres du Congrès, au ministre des Affaires Etrangères ou au Secrétariat au Commerce pour qu'ils en tirent les conclusions nécessaires. Il s'agirait donc d'une démarche purement défensive.

2.5.2. Reactie van de heer James Rubin, woordvoerder van het Amerikaanse ministerie van Buitenlandse Zaken (CBS News — februari 2000: «US Accused of Industrial spionage», document overgenomen van de website http://cbsnews.cbs.com/now/story/o, 1597)

«In Washington, State Department spokesman James P. Rubin denied any involvement in commercial spionage 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 spionage or obtain trade secrets for the benefit of any US company or companies.»

2.5.3. Andere reacties en commentaren in de Verenigde Staten

Naar aanleiding van de voorstelling van het rapport van de heer Campbell over het Echelonsysteem in het Europees Parlement, heeft de Amerikaanse pers verslag uitgebracht over de ongerustheid van de Europeanen en over de ontkenningen van de Amerikaanse en Britse overheden.

Reeds op 24 februari 1999 publiceerde de *New York Times* een artikel, waarin het Echelonsysteem in algemene bewoordingen wordt beschreven als een vorm van samenwerking tussen Australië, Canada, Nieuw Zeeland, het Verenigd Koninkrijk en de Verenigde Staten, met het oog op het «afluisteren» van alle telefoon- en elektronisch verkeer overal ter wereld.

Het artikel vermeldt echter dat de afluistermiddelen van dit systeem niet opwegen tegen de enorme hoeveelheid uitwisselingen, vooral tengevolge van de grote verspreiding van informatie op het internet. Het benadrukt ook dat dit systeem de laatste jaren het statuut van een 'mythe' heeft aangenomen.

Een artikel dat op 28 maart 2000 in het Franse tijdschrift *Le Figaro* verscheen, is van dezelfde strekking. Het brengt het relaas van de confidenties van een «deskundige» van de Amerikaanse inlichtingendiensten, die verklaart:

«Voor de tegenstander wordt het dag na dag gemakkelijker om zijn werkelijke bedoelingen te verbergen te midden van de chaos die er heerst. Voor ons daarentegen wordt het elke dag moeilijker datgene op het spoor te komen wat ons interesseert. Dit is een groot probleem voor het NSA. En vast en zeker ook voor het GCHQ in Engeland en de DGSE in Frankrijk.» (1)

(1) Vrije vertaling.

2.5.2. Réaction de M. James Rubin, porte-parole du Département d'État (CBS News — février 2000: «US Accused of Industrial spionage», document repris du site: http://cbsnews.cbs.com/now/story/o,1597)

«In Washington, State Department spokesman James P. Rubin denied any involvement in commercial spionage 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 spionage or obtain trade secrets for the benefit of any US company or companies.»

2.5.3. Autres réactions et commentaires aux États-Unis

À l'occasion de la présentation du rapport de M. Campbell sur le système Echelon au Parlement européen, la presse américaine s'est fait l'écho des alarmes européennes et des dénégations des autorités américaines et britanniques.

Déjà le 24 février 1999, le *New York Times* avait publié un article décrivant en termes généraux le système Echelon comme une coopération entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis visant à «écouter» l'ensemble des échanges téléphoniques et électroniques dans le monde.

L'article note cependant que les moyens d'écoutes de ce système ne sont pas à la hauteur de l'immensité des échanges existants du fait en particulier de la prolifération d'informations sur l'Internet et souligne que ce système a acquis ces dernières années un «statut mythologique».

Dans le même sens, on trouve un article paru dans le magazine français *Le Figaro* du 28 mars 2000 relatant les confidences d'un «expert» des services de renseignement américains:

«Pour l'adversaire, il est chaque jour plus aisé de cacher son jeu dans le brouhaha. Et pour nous, il devient chaque jour plus difficile de déchiffrer les partitions qui nous intéressent. C'est un vrai problème pour la NSA, et sûrement aussi pour les Anglais du GCHQ et les Français de la DGSE.» (1)

(1) Traduction libre.

Reactie van Zbigniew Brzezinski, voormalig Adviseur Nationale Veiligheid van President Carter

In zijn nummer van 10/16 december 1998 publiceerde het Franse tijdschrift *Le Nouvel Observateur* een interview onder de provocerende titel:

«Een gewezen medewerker van het Witte Huis verbreekt het stilzwijgen: We hebben ervoor gekozen alles te willen weten. Zbigniew Brzezinski, voormalig Adviseur Nationale Veiligheid van President Carter, en nog steeds een gezaghebbend specialist in internationale zaken, windt er geen doekjes om: Ja, Amerika bespioneert de hele wereld, zowel bevriende als vijandige naties. Hij vindt daar niets immoreel aan» (1).

In het interview verklaart Brzezinski onder meer het volgende:

«(...) Amerika heeft verantwoordelijkheden en belangen die over de hele wereld verspreid zijn. Elke nieuwe tendens en elke onvoorziene beweging waar ook ter wereld kunnen het welzijn en de veiligheid van Amerika beïnvloeden. Bijgevolg moet Amerika gelijk waar in staat zijn om inlichtingen te verzamelen, niet alleen over zijn vijanden maar ook over zijn vrienden.

Het verzamelen van inlichtingen staat niet gelijk met spionage in de klassieke betekenis van het woord: het in dienst nemen van geheim agenten. Deze vorm van inlichtingenvergaring brengt heel wat risico's met zich mee en kan schandalen veroorzaken die bijzonder nadelig kunnen zijn voor de betrekkingen met de betrokken bevriende natie. (...)

(...) Het afluisteren van communicaties of het maken van beelden uit de ruimte daarentegen zijn als het ware open, vrij en weinig risicovol. Deze technische middelen maken het mogelijk systematisch inlichtingen in te winnen op een manier die niemand in een lastig parket brengt.

Zowat iedereen kan over deze middelen beschikken. Elk land beslist of het deze al dan niet wenst aan te wenden, afhankelijk van de middelen waarover het beschikt en van zijn doelstellingen. Amerika heeft deze keuze gemaakt.

Volgens mij is er slechts sprake van een ethisch debat over het inlichtingenwezen in het geval van de klassieke spionage. Men kan zich inderdaad afvragen of het in dienst nemen van geheime agenten een gepaste vorm is om in Bonn of in Parijs inlichtingen te verzamelen. Is er echter sprake van een ethisch probleem wanneer men gesprekken afluistert of foto's maakt? Is het immoreel om de wereld te fotograferen?» (1)

(1) Vrije vertaling.

Réaction de M. Zbigniew Brzezinski, ancien conseiller pour la Sécurité Nationale du Président Carter

Le périodique français *Le Nouvel Observateur* du 10/16 décembre 1998, publie une interview de M. Brzezinski sous le titre provocateur:

«Un ancien de la Maison Blanche brise le tabou. Nous avons fait le choix de tout savoir. Zbigniew Brzezinski, qui fut conseiller pour la sécurité nationale du Président Carter et reste un spécialiste très écouté en matière internationale, est catégorique: oui, l'Amérique espionne le monde entier. Ses amis comme ses ennemis. Et il ne voit là rien d'immoral» (1).

Selon M. Brzezinski:

«(...) L'Amérique a des responsabilités et des intérêts globaux mondiaux. Toute nouvelle tendance, tout mouvement imprévu sur la planète peuvent avoir un impact sur son bien-être et sa sécurité. Elle doit donc avoir la capacité d'être renseignée partout, non seulement sur ses ennemis mais aussi sur ses amis.

Le renseignement ne veut pas forcément dire espionnage, au sens classique du terme: le recrutement d'agents. Cette forme de renseignement est risquée, et peut conduire à des scandales très dommageables pour les relations avec le pays ami en question.

Mais les écoutes ou l'imagerie spatiale sont, pour ainsi dire, ouvertes, libres et relativement peu risquées. Ces moyens techniques permettent un recueil systématique — et non compromettant — de renseignements.

Ils sont plus ou moins à la portée de tout le monde. Chaque pays, selon ses moyens et ses objectifs, décide ou non de les mettre en œuvre. L'Amérique a fait ce choix.

Je pense que le débat éthique sur le renseignement ne se pose vraiment que dans le cas de l'espionnage classique. On peut en effet se demander: le recrutement d'agents est-il une forme appropriée de renseignement à Bonn ou à Paris? Mais, en matière d'écoutes ou de photos, quelle est la question éthique? Est-ce immoral de photographier le monde?» (1)

(1) Traduction libre.

Reactie van de heer Thomas D. Grant, Amerikaans advocaat en professor aan het Instituut voor internationaal recht Max Planck in Heidelberg, Duitsland (artikel verschenen op 2 maart 2000 in de «Wall Street Journal» *— Europe: «Spy Games: Don't let Echelon spook you»)*

Volgens de heer Grant zijn de beweringen van Duncan Campbell voor het Europees Parlement niet bijzonder geloofwaardig en zouden ze nadelige gevolgen kunnen hebben op twee gebieden van de samenwerking tussen de Angelsaksische wereld en het Europese vasteland, nl. het Europees industrieel beleid en de Noord-Atlantische militaire samenwerking: «A breakdown of relations in these areas could, in turn, lead to the weakening of the West as the unique bastion of democratic rights and values.»

Ten eerste versterken deze beweringen de positie van diegene in Europa die gekant zijn tegen de noodzakelijke politieke en economische hervormingen, die moeten toelaten de markten (arbeidsmarkt, kapitaalmarkt) flexibeler en meer concurrentieel te maken.

«The current accusation against the United States is widely challenged and little corroborated. It would foolishly imperil the economic recovery if Europe fixed on the idea that American wins in the game of economic competition were the result of legerdemain».

Ten tweede brengen deze beschuldigingen de oude «gaullistische» antipathieën tegen de Verenigde Staten en Groot-Brittannië weer tot leven: ze zouden schade kunnen toebrengen aan de Atlantische Alliantie en nefaste gevolgen kunnen hebben voor de wereldveiligheid bij het begin van de 21e eeuw.

Reactie van de heer James Woolsey, Advocaat in Washington en voormalig directeur van de «Central Intelligence Agency» (CIA)

Tijdens een persconferentie op 7 maart 2000, en in een artikel dat op woensdag 22 maart 2000 in de *«Wall Street Journal»* — Europe verscheen, bevestigde de heer James Woolsey, voormalig directeur van de CIA, dat de Amerikanen Europese ondernemingen bespioneren.

In dit artikel, waarvan de bijzonder provocerende titel luidt *«Why America Spies On Its Allies — Because They Bribe»*, windt de heer Woolsey er geen doekjes om: «Yes, my Continental European friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?»

Met betrekking tot technologische spionage is de heer Woolsey van mening dat de Europese technologie niet de moeite waard is, aangezien ze, op enkele uitzonderingen na, ver achterop loopt in vergelijking met de Amerikaanse technologie.

Réaction de M. Thomas D. Grant, avocat américain et professeur à l'Institut de droit international «Max Planck» à Heidelberg (RFA) — (article paru le 2 mars 2000 dans le «Wall Street Journal» *— Europe: «Spy Games: Don't let Echelon spook you»)*

Selon M. Grant, les allégations de Duncan Campbell devant le Parlement européen ne sont pas plausibles. Elles pourraient avoir des conséquences fâcheuses sur deux domaines de la coopération entre le monde anglo-saxon et le continent européen: la politique industrielle européenne et la coopération militaire Nord-Atlantique: «A breakdown of relations in these areas could, in turn, lead to the weakening of the West as the unique bastion of democratic rights and values.»

Tout d'abord, ces allégations renforcent la position de ceux qui, en Europe, refusent les nécessaires réformes politiques et économiques à entreprendre pour rendre les marchés (marchés du travail, marché des capitaux) plus flexibles et plus compétitifs.

«The current accusation against the United States is widely challenged and little corroborated. It would foolishly imperil the economic recovery if Europe fixed on the idea that American wins in the game of economic competition were the result of legerdemain.»

En second lieu, ces accusations réveillent les vieilles antipathies Gaullistes à l'égard des États-Unis et de la Grande Bretagne: elles pourraient porter préjudice à l'Alliance Atlantique et avoir des conséquences néfastes pour la sécurité du monde en ce début du 21e siècle.

Réactions de M. James Woolsey, avocat à Washington et ancien directeur de la «Central Intelligence Agency» (CIA)

L'espionnage américain sur des firmes européennes a été confirmé par M. James Woolsey, ancien directeur de la CIA, lors d'une conférence de presse le 7 mars 2000, ainsi que dans un article paru dans le *«Wall Street Journal»* — Europe, mercredi 22 mars 2000.

Dans cet article au titre très provocateur *«Why America Spies on its Allies — because they bribe»*, M. Woolsey reconnaît sans détour: «Yes, my Continental European friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?»

En ce qui concerne l'espionnage technologique, M. Woolsey estime que la technologie européenne n'en vaut pas la peine car, à quelques exceptions près, elle serait très inférieure à la technologie américaine.

Maar waarom zouden de Verenigde Staten de Europeanen dan bespioneren?

Volgens de heer Woolsey is het antwoord op deze vraag te vinden in het rapport van de heer Campbell. In de twee gevallen van spionage die de auteur in zijn rapport aanhaalt (een Braziliaans contract voor Thomson-CSF en de verkoop van vliegtuigen door Airbus aan Saoedi-Arabië), wordt er gewag gemaakt van corruptie vanwege deze Europese ondernemingen om de begeerde contracten in de wacht te slepen.

Dit zou de spionageactiviteiten van de Amerikanen rechtvaardigen. Toch ontkent de heer Woolsey dat hij contact heeft opgenomen met de Amerikaanse bedrijven die deze contracten eveneens probeerden te verkrijgen; de Amerikanen zouden alleen de regeringen die op oneerlijke wijze werden benaderd, hebben gewaarschuwd dat ze de zaak niet licht opnamen.

De heer Woolsey had ook kritiek op het interventionisme van de Europese regeringen die, vaak op oneerlijke wijze, hun ondernemingen steunen, ook al kosten ze meer en leveren ze minder goede prestaties dan Amerikaanse bedrijven. Hij merkte op: «It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith.»

De heer Woolsey gaf toe dat de CIA economische inlichtingen inwint, maar bevestigde tegelijk dat 95% van de verzamelde inlichtingen afkomstig is van open bronnen. Hij verklaarde ook dat de CIA geen economische spionageactiviteiten verricht ten gunste van Amerikaanse ondernemingen of vennootschappen.

Indien de CIA de handel in supercomputers en chemische producten op de voet volgt, dan is dat omdat deze producten ook kunnen worden gebruikt om massavernietigingswapens te produceren. Het economisch toezicht kan ook betrekking hebben op landen die het voorwerp zijn van economische sancties, zoals Servië en Irak.

De heer Woolsey daagt de Fransen ook uit om te bevestigen dat zij geen economische spionage toepassen. Hoewel de heer Woolsey toegeeft dat de Amerikanen inderdaad spioneren in Europa, en hij deze activiteiten ook rechtvaardigt, zegt hij niet welke middelen daarbij worden ingezet. Nergens bevestigt hij het bestaan of de doelstellingen van het Echelonnetwerk, zoals de heer Campbell dit in zijn rapport beschrijft.

In een interview met het Franse tijdschrift *«Le Figaro»* van 28 maart 2000, verklaarde de heer Woolsey alleen dat de Verenigde Staten drie methodes gebruiken om in het geheim inlichtingen in te winnen: via het gebruik van spionnen, satellieten en via afluisteroperaties. Meer gaf hij echter niet prijs.

In een nieuwe verklaring, waarbij hij nogmaals bevestigde wat hij aan de *«Wall Street Journal»* had gezegd, herhaalde de heer Woolsey dat de Ameri-

Pourquoi alors les États-Unis espionneraient-t-ils les Européens?

Pour M. Woolsey, la réponse à cette question se trouve dans le rapport même de M. Campbell. Dans les deux cas d'espionnage allégués par ce rapport, (un marché brésilien de Thomson-CSF et la vente d'avions à l'Arabie Saoudite par Airbus), il y est fait mention d'actes de corruption de la part de ces entreprises européennes pour obtenir les marchés convoités.

Ceci justifierait l'espionnage américain. M. Woolsey se défend pourtant d'avoir averti les entreprises américaines en compétition dans les marchés précités; seuls les gouvernements faisant l'objet de manœuvres de corruption auraient été avertis que les Américains ne le prenaient pas à la légère.

Et M. Woolsey de critiquer l'interventionnisme des gouvernements européens qui soutiennent, souvent de manière déloyale, leurs entreprises plus coûteuses et moins performantes que les entreprises américaines: «It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith.» note-t-il.

M. Woolsey admet que la CIA pratique le renseignement économique mais il affirme que 95% des informations collectées proviennent de sources ouvertes. Il affirme également que la CIA n'est pas engagée dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines.

Si la CIA surveille de près le commerce des superordinateurs et celui des produits chimiques, c'est parce que ces produits peuvent aussi être utilisés à produire des armes de destruction massive. La surveillance économique peut aussi concerner des pays soumis à des sanctions économiques tels que la Serbie et l'Iraq.

M. Woolsey défie également les Français d'affirmer qu'ils ne pratiquent pas l'espionnage économique. Si M. Woolsey reconnaît pour sa part la réalité de l'espionnage américain sur l'Europe, en le justifiant, il n'indique pas quels moyens ont été employés pour le pratiquer. Il ne confirme en rien l'existence du réseau Echelon ni ses objectifs tels que décrits dans le rapport de M. Campbell.

Dans une interview accordée au périodique français *«Le Figaro»* (mardi 28 mars 2000), M. Woolsey se contente de préciser que les États-Unis ont trois méthodes de renseignement clandestin: les espions, le satellite de reconnaissance et les écoutes. Il n'en dit pas plus.

Confirmant les propos qu'il a tenu dans le *«Wall Street Journal»*, M. Woolsey réaffirme que le but de l'espionnage américain en matière économique est de

kaanse spionageactiviteiten op economisch gebied tot doel hadden de corruptie te bestrijden, niet om contracten aan Amerikaanse concurrenten te doen toewijzen.

Gevraagd naar het feit of de CIA dan in staat was politiek-economische schandalen uit te lokken (bijvoorbeeld: de zaak-Elf in Duitsland), antwoordde de heer Woolsey: «Normaal niet (...). Dat is niet het beleid van de Verenigde Staten. Maar weet u, er zijn veel dingen waarvan we geen weet hebben. Persoonlijke vetes bijvoorbeeld (...)».

Het is ook interessant te vernemen wat de heer Woolsey vindt van het rapport van de heer Campbell: «Bepaalde elementen van het document (...) zijn intellectueel eerlijk. Andere elementen proberen anti-Amerikaanse gevoelens aan te wakkeren.»

Tot slot roept de heer Woolsey de Europese regeringen op hun door de staat gestuurde economieën om te vormen, wat hun doeltreffendheid en vernieuwingskracht moet versterken, zodat ze niet langer hun toevlucht moeten nemen tot corruptie om contracten binnen te halen. «And then we won't need to spy on you», besluit hij.

faire reculer la corruption, pas de faire attribuer le contrat au concurrent américain.

Interrogé sur le fait de savoir si la CIA était alors susceptible de provoquer des scandales politico-économiques (l'affaire Elf en Allemagne, par exemple), M. Woolsey répond: «Normalement, non (...) ce n'est pas la politique des États-Unis. Mais vous le savez, il y a beaucoup de choses que l'on ignore. Les rancunes personnelles, par exemple ...».

Il est aussi intéressant de noter l'appréciation que M. Woolsey porte sur le rapport présenté par M. Campbell: «Certains points du document (...) sont intellectuellement honnêtes. D'autres cherchent à faire vibrer la corde antiaméricaine.»

Et M. Woolsey de lancer un appel aux gouvernements européens pour qu'ils réforment leurs économies étatiques, ce qui les conduira à plus d'efficacité et à plus d'innovation, et leur évitera ainsi de devoir recourir à la corruption pour gagner des marchés. «And then we won't need to spy on you» conclut-il..

Reactie van de heer James Bamford, auteur van het boek over het NSA — «The Puzzle Palace»

In een artikel dat verscheen op 14 november 1999 in de *«Washington Post»* met als titel *«Loud and Clear — the most secret of secret agencies operates under outdated laws»*, geeft de heer Bamford commentaar op de beweringen in het rapport over het Echelon-netwerk en op de vrees die daaruit blijkt.

Hij schrijft: «As one of the few outsiders who have followed the agency for years, I think the concerns are overblown — so far. Based on everything I know about the agency, and countless conversations with current and former NSA personnel, I am certain that the NSA is not overstepping its mandate. But that doesn't mean it won't.

My real concern is that the technologies it is developing behind closed doors, and the methods that have given rise to such fears, have given the agency the ability to extend its eavesdropping network almost without limits. And as the NSA speeds ahead in its development of satellites and computers powerful enough to sift through mountains of intercepted data, the federal laws (now a quarter-century old) that regulate the agency are still at the starting gate. (...) It is highly unlikely that Echelon is monitoring everyone everywhere, as critics claim.

It would be impossible for the NSA to capture all communications. It has had personnel cutbacks in the past five years as its national security targets have increased in number. North Korean missile development, nuclear testing in India and Pakistan, the movement of suspected terrorists and so on.

Commentaires de M. James Bamford, auteur du livre consacré à la NSA «The Puzzle Palace»

Dans un article paru le 14 novembre 1999 dans le *«Washington Post»* intitulé *«Loud an Clear — the most secret of secret agencies operates under outdated laws»*, James Bamford commenta les allégations et les craintes concernant le réseau Echelon.

Il écrit notamment: «As one of the few outsiders who have followed the agency for years, I think the concerns are overblown-so far. Based on everything I know about the agency, and countless conversations with current and former NSA personnel, I am certain that the NSA is not overstepping its mandate. But that doesn't mean it won't.

My real concern is that the technologies it is developing behind closed doors, and the methods that have given rise to such fears, have given the agency the ability to extend its eavesdropping network almost without limits. And as the NSA speeds ahead in its development of satellites and computers powerful enough to sift through mountains of intercepted data, the federal laws (now a quarter-century old) that regulate the agency are still at the starting gate. (...) It is highly unlikely that Echelon is monitoring everyone everywhere, as critics claim.

It would be impossible for the NSA to capture all communications. It has had personnel cutbacks in the past five years as its national security targets have increased in number. North Korean missile development, nuclear testing in India and Pakistan, the movement of suspected terrorists and so on.

Listening in on European business to help American corporations would be a very low priority, and passing secret intercepts to companies would quickly be discovered.»

In maart 2000 blijft James Bamford volhouden dat de beweringen in het Campbell-rapport «nergens op slaan». Het NSA speelt de informatie die het verzamelt niet door aan Amerikaanse private ondernemingen: «The NSA is a very, very secretive place. Even if you are in the government, even if you're another intelligence agency, it's hard to get information from the NSA.»

En de heer Bamford herhaalt dat het terrorisme en de proliferatie van kernwapens de huidige prioriteiten van het NSA vormen [verklaring geciteerd door Kevin Poulsen in *«Security Focus News»* op 23 maart 2000 (http://www.securityfocus.com)].

Reactie van David Ignatius, journalist van de «Washington Post»

In een artikel dat verscheen op 18 april 2000 onder de titel *«Despite What Europe Thinks, It Benefits From US Spying»*, geeft deze Amerikaanse journalist commentaar op de zaak Echelon. Zijn standpunt leunt nauw aan bij dat van James Bamford.

Zo schrijft David Ignatius: «Rather than the omnipotent agency its critics imagine, it seems these days to be struggling to keep its head above water. (...) And according to NSA officials, its systems aren't capable of processing the vastly increased flow of signals in a «broadband» world where voice and data traval as «packets» along a global tangle of fiber optic cables. (...)».

Vervolgens schrijft deze journalist dat Luitenant-Generaal Michael Hayden, de directeur van het NSA, het volgende zou hebben verklaard: «The notion that the agency can scoop up every signal and electronic emanation in the world was never true — and is really not true now.» David Ignatius merkt echter op: «Now, the whole world essentially shares the same communications system. The «enemy» potentially is everywhere, and America's «friends» inevitably are targets of American surveillance. Europeans who worry about a global NSA surveillance program known as Echelon are probably right, in that sense. (...) That doesn't mean the agency wants to steal foreign industrial secrets or violate people's privacy gratuitously as the Europeans fear, but without a global collection and processing capability, the NSA won't be able to monitor biological terrorists or other 21st century bad guys.»

En Ignatius richt een oproep tot de Europeanen:

«Trust us — is the NSA's implicit message. Trust us to distinguish between the good guys and the bad

Listening in on European business to help American corporations would be a very low priority, and passing secret intercepts to companies would quickly be discovered.»

En mars 2000, James Bamford persiste à affirmer que les allégations du rapport Campbell sont du «non-sens». Les renseignements collectés par la NSA ne sont pas transmis aux entreprises privées américaines. «The NSA is a very, very secretive place. Even if you are in the government, even if you're in another intelligence agency, it's hard to get information from the NSA.»

Et M. Bamford de réaffirmer que les priorités actuelles de la NSA sont le terrorisme et la prolifération des armes nucléaires [propos cités par Kevin Poulsen dans *«Security Focus News»* le 23 mars 2000 (http://www.securityfocus.com)].

Réaction de David Ignatius, journaliste au «Washington Post»

Dans un article intitulé *«Despite What Europe Thinks, It Benefits From US Spying»* paru le 18 avril 2000, ce journaliste américain commente l'affaire «Echelon» plutôt dans le même sens que James Bamford.

David Ignatius déclare notamment: «Rather than the omnipotent agency its critics imagine, it seems these days to be struggling to keep its head above water. (...) And according to NSA officials, its systems aren't capable of processing the vastly increased flow of signals in a «broadband» world where voice and data travel as «packets» along a global tangle of fiber optic cables. (...)».

Le journaliste rapporte alors des propos qu'aurait tenu le lieutenant général Michael Hayden, directeur de la NSA: «The notion that the agency can scoop up every signal and electronic emanation in the world was never true — and is really not true now» David Ignatius fait toutefois remarquer: «Now, the whole world essentially shares the same communications system. The «enemy» potentially is everywhere, and America's «friends» inevitably are targets of American surveillance. Europeans who worry about a global NSA surveillance program known as Echelon are probably right, in that sense. (...) That doesn't mean the agency wants to steal foreign industrial secrets or violate people's privacy gratuitously as the Europeans fear, but without a global collection and processing capability, the NSA won't be able to monitor biological terrorists or other 21st century bad guys.»

Et Ignatius de lancer un appel aux européens:

«'Trust us' is the NSA's implicit message. Trust us to distinguish between the good guys and the bad

guys and to use our powerful surveillance tools for the good of humankind.»

Ignatius voegt er nog aan toe, aangezien hij beseft dat niet iedereen deze boodschap zal begrijpen:

«But it is unrealistic to expect the rest of the world to be enthusiastic.»

2.6. Het Verenigd Koninkrijk

2.6.1 De belangstelling van het Britse parlement

Het Comité I heeft kennis genomen van twee jaarverslagen van het «Intelligence and Security Committee»?(1) die door de Eerste minister aan het Britse parlement werden voorgelegd, het eerste op 25 november 1999, het tweede in november 2000.

Deze verslagen duiden de vier actuele prioriteiten aan van de Britse inlichtingendiensten:

— inlichtingen als hulpmiddel bij de vredesmissies van de Strijdkrachten;

— de proliferatie van massa-vernietigingswapens;

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

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

Het «Committee» buigt zich eveneens over de werking van het CCHQ (het «General Communication Headquarter»), dat — volgens het verslag van Campbell —, de operationele Britse dienst zou zijn die deelneemt aan het «Echelon»-netwerk.

Er wordt vermeld dat het CCHQ vanuit strategisch, politiek en militair oogpunt gezien, Rusland als doelwit beschouwt. Het speelt tevens een belangrijke rol in de strijd tegen de georganiseerde misdaad en het terrorisme. Het levert inlichtingen ter ondersteuning van de vredesmissies van de strijdkrachten in de Balkan. Deze inlichtingen worden aan de regering, aan de geallieerde militaire commando's en aan het opperbevel van de NAVO doorgegeven.

Het verslag 2000 van het «Committee» benadrukt de kwaliteit van de samenwerking in het kader van het UKUSA-verdrag(2), en geeft hiervoor als voorbeeld dat toen een panne het Amerikaanse systeem

(1) Het «The Intelligence and Security Committee» werd opgericht door de «Intelligence Services Act 1994» en voert een parlementair toezicht uit op de Britse inlichtingendiensten. Zie ook activiteitenverslag Comité I — 1998, blz. 2 tot 47.

(2) Voor zover het Comité I bekend, is het de eerste maal dat het IKUSA-verdrag officieel erkend word in een Brits parlementair stuk.

guys and to use our powerful surveillance tools for the good of humankind.»

Conscient toutefois que ce message ne pourra être compris par tout le monde, Ignatius ajoute:

«But it is unrealistic to expect the rest of the world to be enthusiastic.»

2.6. Le Royaume-Uni

2.6.1. L'intérêt du Parlement britannique

Le Comité R a pris connaissance de deux rapports annuels de l'«Intelligence and security committee»(1) déposé par le premier ministre devant le Parlement britannique, le premier le 25 novembre 1999, le second en novembre 2000.

Ces rapports indiquent 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,

— les attaques terroristes et la croissance du crime organisé,

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

Le «Committee» se penche aussi sur le fonctionnement du GCHQ (General Communication Headquarter), qui serait, d'après le rapport Campbell, le service opérationnel britannique participant au réseau «Echelon».

Il est signalé que le GCHQ cible la Russie d'un point de vue stratégique, politique et militaire. Il joue aussi un rôle significatif dans la lutte contre le crime organisé et le terrorisme. Il fournit des renseignements en appui des missions de maintien de la paix des forces armées dans les Balkans. Ces renseignements sont adressés au gouvernement, à des commandements militaires alliés et à celui de l'OTAN.

Le rapport 2000 du «Committee» souligne la qualité de la coopération dans le cadre du traité UKUSA(2) en en donnant pour preuve que le GCHQ a fourni des renseignements à la NSA améri-

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

(2) À la connaissance du Comité R, c'est la première fois que l'existence du traité UKUSA est reconnue officiellement dans un document parlementaire britannique.

kompleet platlegde en diens klanten noodzakelijke informatie moesten ontberen, het CGHQ gedurende drie dagen inlichtingen leverde aan het Amerikaanse NSA en andere diensten.

Het «Committee» roept het CGHQ tenslotte nog op tot een grotere budgettaire gestrengheid voor de realisatie van nieuwe infrastructuren.

Het is belangrijk er even op te wijzen dat het «Committee» de wens van de regering bijtreedt om de nodige wetgeving inzake elektronische handel en cryptografie te voorzien, in het bijzonder om het aanmaken van sleutels, die het ontcijferen van boodschappen toelaten, op te starten.

Het rapport van het «Committee» (waarbij men uit de presentatie van bepaalde passages kan afleiden dat zeker een deel van de inhoud niet publiek gemaakt werd) maakt geen enkele melding van het bestaan van het Echelonsysteem, dat gericht zou zijn op economische spionage-operaties.

2.6.2. Andere reacties en commentaren in Groot-Brittannië

Ook in de Britse pers zijn talrijke commentaren verschenen op de Echelon-zaak, waarvan de volgende het vermelden waard zijn:

Op 28 februari 2000 verklaarde de conservatieve volksvertegenwoordiger Daniel Hannan in de *«Daily Telegraph»:* «I'm proud we're spying on Europe.»

Voortgaand op het thema van de spionageactiviteiten die gerechtvaardigd zijn omdat Franse ondernemingen aan corruptie doen, en op het thema van de Angelsaksische solidariteit, voegde de heer Hannan eraan toe:

«When truly vital matters are at stake, the blood of the English-speaking peoples is thicker than the water of the Channel. We don't mind sharing our military secrets with Her Majesty's Canadian subjects, but how many of us could honestly claim to feel the same about the Belgians?» (sic)

De bemerkingen van de heer Jonathan Eyal, Director of studies van het «Royal United Services Institute for Defense Studies» te Londen (1)

Volgens Jonathan Eyal:

«zijn het de inlichtingendiensten die de oprichting van een Europese Defensiestructuur belemmeren. In veel opzichten berust het huidige debat over het «Echelon» systeem op een dwaling en doet het merkwaardig ouderwets aan. Enerzijds omdat de Angelcaine et à d'autres services pendant trois jours durant lesquels une panne du système américain privait ses clients habituels d'informations.

Le «Committee» appelle enfin le GCHQ à une plus grande rigueur budgétaire dans la réalisation de nouvelles infrastructures.

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.

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

2.6.2. Autres réactions et commentaires en Grande Bretagne

La presse britannique aussi a publié de nombreux commentaires sur l'affaire «Echelon» dont les suivants méritent d'être cités:

Le député conservateur Daniel Hannan déclare dans le *« Daily Telegraph»* du 28 février 2000: «I'm proud we're spying on Europe.»

Développant le thème de l'espionnage justifié par les pratiques de corruption des firmes françaises et celui de la solidarité anglo-saxonne, M. Hannan ajoute:

«When truly vital matters are at stake, the blood of the English-speaking peoples is thicker than the water of the Channel. We don't mind sharing our military secrets with Her Majesty's Canadian subjects, but how many of us could honestly claim to feel the same about the Belgians?» (sic)

Les commentaires de M. Jonathan Eyal, Director of Studies au «Royal United Services Institute for Defence Studies» à Londres (1)

Selon Jonathan Eyal:

«c'est le renseignement qui freine la construction d'une structure européenne de la Défense. À de nombreux égards, le débat actuel sur le système «Echelon» se fourvoie et est complètement dépassé. D'une part, parce que les gouvernements anglo-

(1) Artikel verschenen in *«NRC Handelsblad»* op 30 mei 2000.

(1) Article paru le 30 mai 2000 dans le journal néerlandais *«NRC Handelsblad»*.

saksische regeringen niet de enigen zijn in het uitoefenen van de elektronische bewaking van communicaties: ook Frankrijk beschikt over «grote oren» (DGSE) die gericht zijn op de Verenigde Staten.

Anderzijds omdat de huidige vraag van de inlichtingendiensten er niet meer in bestaat om te weten hoe zij aan gegevens moeten komen, maar wel hoe zij greep moeten krijgen op de immense hoeveelheid beschikbaar materiaal. Het idee dat alle Europese e-mails zouden worden gelezen is absurd: geen enkele inlichtingendienst zou zulke hoeveelheden kunnen verwerken.

Als spionage daarentegen vaak geassocieerd wordt met oorlogvoering, zijn de moderne elektronische bewakingssystemen in feite vaak de beste waarborg voor de vrede. Om die reden is de elektronische bewaking het enige middel waarover de Westerse landen beschikken in hun strijd tegen de uitbreiding van chemische, bacteriologische en andere wapens.

Het grootste probleem doet zich voor wanneer de communicatie tussen particuliere ondernemingen wordt afgetapt. Zulke praktijk is uiteraard verwerpelijk en waarschijnlijk illegaal. Maar de zaak ligt ingewikkelder.

Op de internationale markten vinden we vaak heel wat Amerikaanse bedrijven die wedijveren met elkaar: in zo'n situatie is het belachelijk te geloven dat Washington de ene partij zou helpen ten nadele van de andere partij omdat dit uiteindelijk toch aan het licht zou komen. Het is bovendien opmerkelijk dat de meeste beschuldigingen van commerciële spionage betrekking hebben op wapencontracten, wat in de internationale handel de minst representatieve transacties zijn. Wapenfabrikanten onderhouden inderdaad altijd nauwe banden met hun regeringen en kunnen niet werken op een vrije markt.

Het is trouwens niet alleen in landen waar de Staat het economisch leven grotendeels beheerst dat er nauwe banden bestaan tussen bedrijven en de inlichtingendiensten. Dit geldt niet voor de Verenigde Staten maar wel voor Frankrijk.

Maar het tijdperk van de zuiver nationale bedrijven is voorbij en daardoor ook de banden met de inlichtingendiensten. Veel defensiebedrijven zijn niet meer zuiver Amerikaans of zuiver Europees; zij ontwikkelen gezamenlijke projecten aan weerszijden van de Atlantische Oceaan. Sommige van hen verhandelen tegenwoordig aandelen op de beurs.

In de meeste crisissen die zich thans in de wereld voordoen, zijn de Europeanen en Amerikanen bondgenoten die hun inlichtingen met elkaar delen.

Onlangs nog nam Londen het initiatief voor een Europees defensiesysteem. Maar door zijn relatie met de Verenigde Staten, behoudt Groot-Brittannië een

saxons ne sont pas les seuls à pratiquer la surveillance électronique des communications: la France aussi dispose de «grandes oreilles» tournées vers les États-Unis (la DGSE).

D'autre part, parce que le problème actuel des services de renseignement n'est plus de savoir comment collecter l'information, mais bien comment maîtriser l'immense quantité de données disponibles. L'idée que tous les courriers électroniques européens sont interceptés est absurde car aucun service de renseignement n'est en état de les traiter en totalité.

Par ailleurs, si l'espionnage est le plus souvent associé à la conduite de la guerre, les systèmes modernes de surveillance électronique sont en réalité les meilleures garanties possibles pour la paix. Ainsi, la surveillance électronique est le seul moyen disponible dont disposent les pays occidentaux pour lutter contre la prolifération des armes chimiques, bactériologiques et autres.

Le problème le plus délicat survient lorsque des communications entre entreprises privées sont interceptées. Une telle pratique est assurément blâmable et probablement illégale. Mais les choses ne sont pourtant pas si simples.

Dans les marchés internationaux, on trouve souvent plusieurs entreprises américaines en concurrence l'une avec l'autre; en pareille situation, il est absurde de croire que Washington aiderait l'une au détriment de l'autre, car cela finirait bien par se savoir. De plus, la plupart des accusations d'espionnage commercial concernent des contrats d'armement qui sont les transactions les moins représentatives du commerce international. En effet, les fabricants d'armes ont toujours des liens étroits avec leurs gouvernements et ils ne peuvent opérer sur un marché libre.

Il n'y a d'ailleurs que dans les pays ou la vie économique est pour une bonne part dans les mains de l'État que des liens étroits peuvent se nouer entre les entreprises et les services de renseignement. Ceci n'est pas le cas des États-Unis, mais bien de la France.

Mais le temps des entreprises purement nationales est bien révolu, et par là même, celui des liens avec les services de renseignement. Beaucoup de firmes de défense ne sont plus purement américaines ni purement européennes; elles développent ensemble des projets de part et d'autre de l'Océan Atlantique. Certaines sont cotées en bourse. (...)

Enfin, dans la plupart des crises qui se sont produites dans le monde, les Européens et les Américains sont des alliés qui partagent leurs renseignements.

Londres a pris récemment l'initiative d'un plan de système de défense européen. Mais par sa relation avec les États-Unis, la Grande-Bretagne conserve cette

unieke positie als het land dat toegang heeft tot het inlichtingenpotentieel van een supermogendheid.

De Europese Unie blijft, zoals de conflicten in de Balkan hebben uitgewezen, afhankelijk van de Verenigde Staten voor inlichtingen en Groot-Brittannië handhaaft zijn tweeslachtige positie in Europa. De debatten in het Europees Parlement en in de Commissie zullen daarin waarschijnlijk niet veel verandering brengen.

De grootste belemmering voor de uitbouw van een Europese defensiestructuur blijven dus de inlichtingendiensten», aldus de heer Eyal.

2.7. Canada

2.7.1. De jaarlijkse verslagen van de commissaris van het «Centre de la sécurité des télécommunications» (CST)

Volgens het verslag van de heer Campbell is Canada één van de staten die deelneemt aan het «Echelon»-netwerk.

Dat land beschikt inderdaad over een instelling die vergelijkbaar is met het Amerikaanse NSA of het Britse GCHQ.

Het gaat hier over het CST, een instelling van het ministerie van Landsverdediging, waarvan de opdracht erin bestaat aan de Canadese regering elektromagnetische inlichtingen (SIGINT) te verschaffen over andere landen.

Het CST verkrijgt haar inlichtingen via de onderschepping en de analyse van uitzendingen afkomstig van radio, radar en andere high tech-middelen die niet gepreciseerd worden. In het kader van haar programma over veiligheid van de technologie, verstrekt het CST ook adviezen over de beveiliging van de computertechnologie van de regering.

Over de wettelijkheid van de activiteiten van het CST wordt een bijzonder toezicht uitgeoefend. Het CST wordt gecontroleerd door een commissaris, benoemd door de minister van Landsverdediging, die als taak heeft zich ervan te vergewissen dat deze instelling handelt overeenkomstig de fundamentele principes van de Canadese wettelijkheid en de bescherming van de persoonlijke levenssfeer.

Het CST heeft geen toestemming om de communicatie van Canadese burgers, noch die van buitenlandse permanente ingezetenen in Canada, te onderscheppen.

De commissaris moet een jaarlijks verslag voorleggen aan de minister van Landsverdediging. Dit verslag wordt eveneens ingediend bij het Parlement.

De verslagen van de commissaris van het CST zijn gepubliceerd, en het Comité I heeft kennis genomen

position unique d'avoir accès au potentiel de renseignement d'une super puissance.

Ainsi que les conflits dans les Balkans l'ont montré, l'Union européenne est donc dépendante des États-Unis pour le renseignement et la Grande-Bretagne conserve sa position ambivalente en Europe. Les débats au Parlement européen et à la Commission n'y changeront probablement rien.

Le frein le plus important à la construction d'une structure européenne de défense reste donc les services de renseignement», selon M. Eyal.

2.7. Le Canada

2.7.1. Les rapports annuels du commissaire du Centre de la sécurité des télécommunications

Le Canada est, d'après le rapport de M. Campbell, l'un des États qui participe au réseau «Echelon».

Ce pays dispose en effet d'un organisme équivalent à la NSA américaine ou au GCHQ britannique.

Il s'agit du Centre de la sécurité des télécommunications (CST), organisme du ministère de la Défense nationale, dont la mission est de fournir au gouvernement du Canada des renseignements électromagnétiques (SIGINT) sur des pays étrangers.

Le CST obtient ces renseignements en interceptant et en analysant les transmissions par radio, par radar et par d'autres moyens électroniques très perfectionnés non précisés. Dans le cadre de son programme de sécurité des technologies, le CST donne aussi des conseils sur la sécurité des technologies de l'information du gouvernement.

Le CST est contrôlé par un commissaire, nommé par le ministre de la Défense nationale, dont la tâche est de s'assurer que cet organisme agit conformément aux principes fondamentaux de la légalité canadienne et de la protection de la vie privée.

Le CST n'est pas autorisé à cibler les communications des citoyens canadiens ni celles des résidents permanents au Canada.

Le commissaire doit présenter un rapport annuel au ministre de la Défense nationale. Ce rapport est également déposé au Parlement.

Les rapports du commissaire du CST sont publiés et le Comité R a pris connaissance des rapports des

van de verslagen over de dienstjaren 1998/1999 en 1999/2000. Er werden mogelijke aanwijzingen gezocht in verband met het bestaan van het «Echelon»-netwerk.

Het bestaan van het «Echelon»-netwerk wordt echter op geen enkele manier in de verslagen ter sprake gebracht.

Zonder haar rechtstreeks bij name te noemen, erkent de Canadese commissaris van het CST officieel het bestaan van de wederzijdse overeenkomst «UKUSA»:

«Het CST krijgt elektromagnetische inlichtingen die andere regeringen hebben ingewonnen. Tegelijkertijd verschaft het CST hen de door haarzelf ingewonnen inlichtingen. (...) Deze «partnership»-overeenkomsten met de Verenigde Staten, het Verenigd Koninkrijk, Australië en Nieuw-Zeeland werden opgesteld tijdens de Tweede Wereldoorlog en werden onderhouden tijdens de Koude Oorlog.»

In verband hiermee merkt de commissaris op dat de regeringen van de landen die deelnemen aan deze uitwisseling van inlichtingen ook een beleid voeren om het privé-leven van hun burgers te beschermen. Elke regering is overeengekomen om, voor rekening van de ander, geen gegevens in te zamelen die illegaal zouden zijn in één van de landen die deelnemen aan de overeenkomst.

Volgens de commissaris worden de inlichtingen die verzameld werden door het CST doorgespeeld aan de ministeries die belast zijn met de belangenbescherming van Canada op het gebied van veiligheid, inlichtingen, economie en defensie.

De verslagen vermelden geen verspreiding aan particuliere vennootschappen. De verslagen van de Canadese commissaris weerspiegelen zijn obsessie dat het CST het privé-leven van de Canadese burgers toch niet zou schenden.

In zijn bevindingen hieromtrent merken wij de volgende vaststelling op:

«Canadese communicaties kunnen in het aanbod van inlichtingen van het CST teruggevonden worden, want op dit ogenblik is het technisch onmogelijk om ze volledig uit te sluiten; het CST gebruikt de technische middelen die tot haar beschikking staan om het onopzettelijk afluisteren van Canadese communicaties te beperken; (...)

(...) het CST beschikt over politieke en praktische middelen, die erop gericht zijn de bescherming en de correcte behandeling van Canadese communicaties te garanderen, die onopzettelijk zouden ingewonnen worden, overeenkomstig de Canadese wetten (...).»

2.7.2. Andere reacties en commentaren in Canada

De internationale pers heeft de verklaringen overgenomen uit een boek van de Canadees Mike Frost.

exercices 1998/1999 et 1999/2000. Il y a recherché d'éventuelles indications relatives à l'existence du réseau «Echelon».

L'existence du réseau «Echelon» n'est évoquée en aucune manière dans les rapports.

Cependant, sans la nommer de manière explicite, le commissaire canadien du SCT reconnaît officiellement l'existence de l'entente «UKUSA»:

«Le SCT reçoit des renseignements électromagnétiques recueillis par d'autres gouvernements. Il fournit également à ceux-ci des renseignements qu'il a lui-même recueillis. Ces accords de partenariat avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande ont été établis au cours de la Deuxième Guerre mondiale et maintenus pendant toute la durée de la Guerre froide.»

Le commissaire relève à ce propos que les gouvernements des pays qui participent à cet échange de renseignements ont des politiques destinées à protéger la vie privée de leurs citoyens. Chaque gouvernement a convenu de ne pas effectuer, pour le compte de l'autre, de travail de collecte qui serait illégal dans un des pays partie prenante à l'entente.

Les renseignements recueillis par le CST sont, selon le commissaire, diffusés aux ministères chargés de protéger les intérêts du Canada sur les plans de la sécurité, du renseignement, de l'économie et de la défense.

Les rapports ne font pas état d'une quelconque diffusion à des sociétés privées. Les rapports du commissaire canadien traduisent son obsession que le CST n'enfreigne pas la vie privée des citoyens canadiens.

À ce sujet, on relève notamment les constatations suivantes:

«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 utilise les moyens techniques à sa disposition pour réduire l'interception involontaire de communications canadiennes;

le CST possède des politiques et des pratiques destinées à assurer la protection et le traitement approprié des communications canadiennes recueillies involontairement, conformément aux lois du Canada (...).»

2.7.2. Autres réactions et commentaires au Canada

La presse internationale a relayé les déclarations contenues dans un livre du canadien Mike Frost.

Hij stelt zich voor als een voormalig lid van het Centrum voor de veiligheid van de telecommunicatie (CST).

Hij verklaart dat het CST in het verleden de communicatie van twee ministers van de regering Thatcher heeft geïntercepteerd, op uitdrukkelijk verzoek van deze Britse eerste minister. Het zou gaan om een politieke spionagezaak. Aangezien de Britse wetgeving niet toelaat dat Britse onderdanen worden afgeluisterd, zou men de gewoonte hebben aangenomen daarvoor een beroep te doen op een bevriende dienst in het buitenland.

In een artikel met als titel « A Vast Conspiracy? », dat op 4 april 2000 verscheen in de « *National Post* », een Canadese Engelstalige krant, geeft de auteur commentaar op de reacties van de Franse regering op de beweringen betreffende het Echelon-systeem :

« What such comments seek to insinuate is that lackluster performance of the French and other European economies is the result not of over-regulation and excessive taxation, but of the perfidious ways of English-speaking countries. (...)

(...) French firms did not lose contracts because they were overpriced and inefficient, but because « les Anglo-Saxons » cheated.

And in all this indignation, no one mentions the existence of the European Union's K4 Committee, which is busy establishing its own Euro-Echelon to spy on electronic telecommunication traffic. But Europe's economic stagnation is not caused by Echelon and it will not be cured by a Euro-imitation of it. »

3. De houding van de Belgische inlichtingendiensten ten aanzien van de Echelon-problematiek

De vaststellingen van het Vast Comité I hebben aangetoond dat de Belgische inlichtingendiensten globaal genomen passief reageerden op de problematiek, daarbij vooral het feit inroepend dat zij niet over de wettellijke, technische en menselijke middelen beschikten die hen in staat zouden stellen om zelf het bestaan van het Echelon-systeem vast te stellen.

De bescherming van het wetenschappelijk of economisch potentieel van het land is een opdracht van de Veiligheid van de Staat en niet van de ADIV. Hun kennis over het onderwerp is uitsluitend gebaseerd op gegevens afkomstig uit de consultatie van open bronnen.

Celui-ci se présente comme étant un ancien membre du Centre de la sécurité des télécommunications (CST).

Il y affirme que le CST a autrefois intercepté les communications de deux ministres du gouvernement de Mme Thatcher, sur demande expresse de ce premier ministre britannique. Il s'agirait d'un cas d'espionnage politique. La législation britannique ne permettant pas l'écoute de ses propres citoyens, la pratique aurait été de s'adresser à un service ami étranger pour le faire.

Dans un article paru le 4 avril 2000 et intitulé « A Vast Conspiracy ? », le journal anglophone canadien « *National Post* » commente les réactions du gouvernement français sur les allégations concernant le système « Echelon » :

« What such comments seek to insinuate is that lacklustre performance of the French and other European economies is the result not of over-regulation and excessive taxation, but of the perfidious ways of English-speaking countries.

French firms did not lose contracts because they were overpriced and inefficient, but because les « Anglo-saxons » cheated.

And in all this indignation, no one mentions the existence of the EU's K4 Committee, which is busy establishing its own Euro-Echelon to spy on electronic telecommunication traffic. But Europe's economic stagnation is not caused by Echelon and it will not be cured by a Euro-imitation of it. »

3. L'attitude des Services de renseignement belges à l'égard de la problématique « Echelon »

Il ressort des constatations faites par le Comité R que les services de renseignement belges sont globalement restés passifs sur le sujet en invoquant principalement le fait qu'ils ne disposaient pas des possibilités légales techniques et humaines qui leur permettraient de constater eux-mêmes l'existence du système « Echelon ».

La protection du potentiel scientifique et économique du pays est une mission de la Sûreté de l'État et non du SGR. Les seules informations dont ils disposaient sur le sujet provenaient de la consultation des sources ouvertes.

3.1. De Veiligheid van de Staat

Na een onderhoud van het Vast Comité I met de administrateur-generaal van de Veiligheid van de Staat, verklaarde deze dat:

«(...) de dienst geen enkele technische of wettelijke bevoegdheid bezat om zich met de problematiek van beveiliging van communicatiesystemen bezig te houden;

de dienst niet de nodige middelen ter beschikking heeft, zowel wat personeel als materieel betreft, om na te gaan of het systeem Echelon wel degelijk bestaat;

de dienst niet overgaat tot het verzamelen van inlichtingen per satelliet en geenszins toegang heeft tot dit soort informatiebron;

de dienst trouwens over geen enkele wettelijke bevoegdheid beschikt die toelaat intercepties per satelliet te verrichten en ze bijgevolg evenmin gesprekken kan afluisteren via satelliet; deze situatie was trouwens schadelijk voor de Veiligheid van de Staat, gezien zij in contact stond met buitenlandse inlichtingendiensten die wel over een dergelijke mogelijkheid beschikten;

het bestaan van het Echelon-systeem daarom moeilijk te bewijzen viel; buiten de mededeling van elementen uit open bronnen aan de minister van Justitie in februari 1999, om deze toe te laten te antwoorden op parlementaire interpellaties, heeft de Veiligheid van de Staat nooit een rapport of nota opgesteld over het Echelon-systeem».

Wat de economische doelwitten betreft die door het Echelon-systeem zouden geviseerd zijn, geeft de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten in haar artikel 7 een nieuwe specifieke opdracht aan de Veiligheid van de Staat, die de bescherming inhoudt van «(...) 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 (...).»

De administrateur-generaal preciseerde verder dat haar dienst nog geen instructies had ontvangen van het ministerieel Comité voor Inlichtingen en Veiligheid aangaande de bescherming van het wetenschappelijk of economisch potentieel.

Bij een uitgevoerde controle door de enquêtedienst van het Vast Comité I werd vastgesteld dat, op het moment dat het Comité I belast werd door het Parlement met het onderhavige onderzoek, een agent van de Veiligheid van de Staat op eigen initiatief een informatiegaring naar inlichtingen aangaande het Echelon-netwerk was begonnen, via de raadpleging van open bronnen, meerbepaald het internet.

3.1. La Sûreté de l'État

Questionnée par le Comité R, l'administration générale de la Sûreté de l'État a déclaré que ce service:

«(...) n'avait aucune compétence technique ou légale pour s'occuper de problèmes de sécurité des communications;

manquait de moyens, tant en personnel qu'en matériel, pour pouvoir vérifier la réalité de l'existence du système «Echelon»;

ne procédait pas au recueil de renseignements par satellites et qu'il n'avait aucun accès à ce type de source d'information;

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 «Echelon» lui était par conséquent impossible à démontrer; qu'à part la communication en février 1999 d'informations tirées de sources ouvertes 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 «Echelon».

En ce qui concerne les objectifs économiques que viserait le système «Echelon», la loi organique du 30 novembre 1998 des services de renseignements, en son article 7, assigne une nouvelle mission spécifique à la Sûreté de l'État qui est la protection du «potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel.»

L'administrateur général 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.

Une vérification effectuée par le Service d'enquêtes du Comité R a permis de constater qu'au moment même où celui-ci était chargé de la présente enquête par le Parlement, un agent de la Sûreté de l'État avait entrepris d'initiative une recherche de renseignements sur le réseau «Echelon» en consultant des sources ouvertes, notamment l'internet.

Het resultaat van zijn zoektocht werd toegezonden aan de directie van de Veiligheid van de Staat, die hieraan echter geen enkel gevolg gaf.

3.2. De Algemene Dienst Inlichting en Veiligheid (ADIV)

De ADIV zegt geen weet te hebben van het bestaan van buitenlandse netwerken voor het intercepteren van telecommunicaties, buiten hetgeen ze vernam uit open bronnen, waar men echter zowel informatie als desinformatie terugvindt.

De ADIV beschouwt de bedreiging komende van grote landen als plausibel en past dus het zorgvuldigheidsprincipe toe. De dienst volgt dus niet in het bijzonder het Echelon-systeem, maar ze werkt wel vanuit de veronderstelling dat intercepties van communicaties wel degelijk bestaan, en, — ongeacht het land dat ze uitvoert — men zich er moet tegen weren. Ze meent tevens dat eender welke informatica-cijfercode kan verbroken worden.

De ADIV beschikt niet over de wettelijke, technische en menselijke middelen die noodzakelijk zijn om het bestaan van het Echelon-netwerk te ontleden.

De ADIV voert geen actief onderzoek naar dit netwerk, zich daarbij baserend op enerzijds het gegeven dat de bescherming van het wetenschappelijk en economisch potentieel niet tot haar opdrachten behoort (volgens de nieuwe wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten), en anderzijds op de wettelijke beperkingen aangaande het onderscheppen van radiocommunicaties.

Zou het gaan om een militair spionagesysteem, wat wel degelijk tot de bevoegdheid van de ADIV behoort, dan nog verleent deze dienst geen prioriteit aan spionage uitgaande van geallieerden van België. In deze materie blijken andere landen veel meer bedreigender activiteiten te vertonen voor de Belgische militaire belangen.

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

De uitbreiding van de opdrachten voor niet-militaire belangen wordt niet expliciet voorzien in de wet.

Evenwel stelt de ADIV voor mee te werken zowel aan het ontwerpen van federale structuren als aan het opstarten van een algemene beveiligingspolitiek ten opzichte van informaticanetwerken.

De dienst is het idee genegen om ofwel een federaal agentschap op te richten voor de bescherming van de

Le produit de ces recherches a été transmis à la direction de la Sûreté de l'État qui n'y a cependant donné aucune suite.

3.2. Le Service général du renseignement et de la sécurité (SGR)

Le SGR n'a pas connaissance de l'existence de réseaux étrangers d'interceptions des communications autrement que par les sources ouvertes, dans lesquelles on trouve de l'information mais aussi de la désinformation.

Le SGR considère néanmoins la menace venant des grands pays comme plausible et il applique donc le principe de précaution. Le service ne «suit» donc pas le système «Echelon» en particulier mais ce service considère que les interceptions de communications existent réellement, et que, quel que soit le pays qui les pratique, il faut s'en prémunir.

Le SGR considère également que n'importe quel système de chiffrement informatique est susceptible d'être cassé.

Le SGR ne dispose pas de moyens légaux techniques et humains nécessaires pour déceler l'existence du réseau «Echelon». Le SGR n'effectue 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 pas une des compétences qui lui est attribuée par la nouvelle loi organique du 30 novembre 1998 sur les services de renseignement et, d'autre part, sur les restrictions légales qui lui sont imposées en matière de captage des radiocommunications.

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.

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.

Une extension d'une telle mission à des intérêts autres que militaires n'est pas mentionnée explicitement dans la loi.

Toutefois, le SGR 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 SGR est donc favorable à l'idée de créer une agence fédérale pour la protection de l'information

informatie, ofwel om een reeds bestaand organisme te belasten met dit beleid inzake codering in België. België heeft trouwens eminente specialisten in de cryptografie.

De ADIV volgt van dichtbij 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- en handelsbelangen, de veiligheid en de bescherming van het privé-leven.

Deze uiteenlopende belangen geven in de Verenigde Staten aanleiding tot een hevige machtsstrijd tussen het NSA en de lobby van internetgebruikers.

4. Het debat rond de NSA-KEY van Microsoft

Volgens het Franse tijdschrift «Le Monde du Renseignement» (nr. 376 van 17 februari 2000) zou het Franse ministerie van Landsverdediging in het bezit zijn van een verslag van de «Délégation des Affaires stratégiques» (DAS) getiteld «Veiligheid van de Computersystemen: afhankelijkheid en kwetsbaarheid» (1).

Dit verslag zou niet alleen wijzen op een tekort aan betrouwbaarheid van de Microsoft software, maar vooral op een tekort aan doorzichtigheid en het gevaar voor het samenspannen met de Amerikaanse inlichtingendiensten.

Deze medeplichtigheid van Microsoft zou toelaten dat technische mogelijkheden geleverd worden aan het Amerikaanse inlichtingenagentschap om elektronische communicaties binnen te dringen en te onderscheppen.

Het verslag van de heren Poullet en Dinant (nb. beide heren zijn experten aan wie het Vast Comité I de opdracht gaf om alle beschikbare documenten, die verkrijgbaar zijn via open bronnen en die het bestaan van het Echelonsysteem toegeven, te onderzoeken, te analyseren en te verklaren) vermeldt met betrekking tot dit probleem het volgende:

«Internet raakte in vuur en vlam toen men in een registerbestand van het Windows systeem een variabele ontdekte, NSA-KEY genaamd. Velen beweerden dat de NSA door deze geheime sleutel alle gecodeerde berichten zou kunnen lezen aan de hand van cijferfuncties die Microsoft zou verstrekken.

(1) Vrije vertaling.

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.

Par conséquent, 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 et commerciaux, la sécurité, la protection de la vie privée.

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.

4. Le débat sur la NSA-KEY de Microsoft

Selon le périodique français *Le Monde du Renseignement* nº 376 du 17 février 2000, le ministère français de la Défense nationale serait en possession d'un rapport de la Délégation aux affaires stratégiques (DAS) intitulé «Sécurité des systèmes d'information: dépendance et vulnérabilité» (1).

Ce rapport pointerait les défauts de fiabilité des logiciels Microsoft, mais surtout les manques de transparence et les risques de collusion avec les services de renseignement américains que ceux-ci impliquent.

Cette complicité de Microsoft permettrait d'offrir des facilités techniques à l'agence de renseignement américaine pour réaliser des intrusions et des interceptions de communications électroniques.

Le rapport de Messieurs Yves Poullet et Jean-Marc Dinant, experts à qui le Comité R a confié la mission d'examiner, analyser et commenter tous les documents disponibles issus de sources ouvertes traitant de l'existence du réseau Echelon, mentionne ce qui suit à propos de ce problème:

«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) Traduction libre.

1. Deze hypothese werd tegengesproken door Microsoft terwijl de «zwakke plekken» die hieronder in punt 3.1 vermeld worden door Microsoft zijn toegegeven.

2. Men kan zich moeilijk voorstellen dat een geheime ontcijferingsleutel zou opgeslagen worden op een zo zichtbare plaats als een gegevensbestand.

3. Men kan zich nog minder voorstellen dat de naam van die sleutel NSA-KEY zou zijn.

Ondanks dit vals alarm hoeft men niet te denken dat de door Microsoft geleverde cijferfuncties betrouwbaar zijn. De ondertekenaars van dit verslag delen samen met vele andere deskundigen de mening dat elke export van vercijferingsprocédés buiten de USA slechts toegestaan is wanneer de Amerikaanse diensten over de technische mogelijkheid beschikken om de codering te breken. Wat er ook van zij, tegenwoordig wordt algemeen aangenomen dat in de wereld van het geheimschrift een softwarecodering slechts te vertrouwen is wanneer men in bezit is van haar broncode(1)».

In nr. 383 van 1 juni 2000 komt het Franse tijdschrift *Le Monde du Renseignement* terug op het probleem van mogelijke «backdoors», die geïnstalleerd werden door het NSA, in het software programma waarop het Windows-systeem gebouwd is. Voor Microsoft betekent de NSA-KEY slechts een bewaringssleutel.

De journalist Duncan Campbell, die dit onderwerp onderzoekt, vroeg aan een hoge verantwoordelijke bij Microsoft om hem de details toe te sturen van het omstreden programma. Deze laatste weigerde om de reden dat deze verspreiding de intellectuele eigendom van Microsoft zou schenden.

Een onderzoeker op het gebied van geheimschrift van de Polytechnische School van Lausanne gelooft dat de argumenten die naar voren worden gebracht door Microsoft waarschijnlijk wel op waarheid berusten maar hij sluit de mogelijkheid niet uit dat het NSA een sleutel bezit.

Het Vast Comité I vroeg wederom de mening van de heer Dinant(2) aangaande deze controverse, en of hij na lezing van de bovenvermelde informatie zijn standpunt zou handhaven volgens dewelke de NSA-KEY geen geheime sleutel is die het NSA zou toelaten om boodschappen te ontcijferen. Het antwoord van de Heer Dinant luidde als volgt (brief van 14 juni 2000):

«Na lezing van het artikel verschenen in *Le Monde du Renseignement* en na consultatie van verschillende

(1) Vrije vertaling.

(2) De heer J.-M. Dinant is promovendus in de informatica en onderzoeker bij het «Centre de recherche informatique et droits» bij de universitaire faculteiten Notre-Dame de la Paix te Namen.

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

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.(1)»

Dans son numéro 383 du 1er juin 2000, le périodique français *Le Monde du Renseignement* revient sur ce problème de l'éventualité de «backdoors» installés par la NSA dans le programme informatique sur lequel est bâti le système «Windows». Pour Microsoft, la NSA-Key ne représente qu'une clé de sauvegarde.

Le journaliste Duncan Campbell, qui enquête sur la question, a demandé à un haut responsable de Microsoft de lui transmettre le détail du programme litigieux. Ce dernier a refusé au motif que cette diffusion violerait la propriété intellectuelle de Microsoft.

Un chercheur en cryptographie de l'Ecole polytechnique de Lausanne croit que les arguments avancés par Microsoft sont tout à fait vraisemblables, mais il n'exclut cependant pas l'éventualité d'une clé en possession de la NSA.

Le Comité R a redemandé l'avis de M. Dinant(2) sur cette controverse et si, après lecture des informations précitées, il maintenait son point de vue selon lequel la NSA-Key n'est pas une clé secrète permettant à la NSA de décrypter des messages. La réponse de M. Dinant est la suivante (lettre du 14 juin 2000):

«Après lecture de l'article paru dans *Le Monde du Renseignement* et consultation de plusieurs sources

(1) Traduction libre.

(2) Monsieur Jean-Marc Dinant est doctorant en informatique et chercheur au Centre de recherches informatique et droit des facultés universitaires Notre-Dame de la Paix à Namur.

open bronnen volgend op het verslag van februari 2000 over het Echelon- netwerk, behoud ik volledig en herbevestig ik met klem mijn standpunt uiteengezet in sectie 4.2 van vermeld verslag.

Ik voeg er aan toe dat sindsdien Microsoft op een doorzichtige en eerlijke manier antwoord heeft gegeven op de twaalf eerste vragen die schriftelijk aan dit bedrijf gesteld werden door Duncan Campbell. Als gevolg daarop heeft deze laatste op een aanvallende en agressieve manier bepaalde vragen, waarop hij reeds een antwoord had gekregen, opnieuw geformuleerd en heeft hij er andere vragen aan toegevoegd. Het is pas op dat moment dat Microsoft besloten heeft om de «niet opbouwende uitwisselingen» te onderbreken.

Het is technisch mogelijk — maar weinig waarschijnlijk — dat deze tweede sleutel (de NSA-KEY) uitgegeven is door het NSA. Zelfs indien dit het geval zou zijn, zou het amper de mogelijkheid bieden aan het NSA om de controlerende volmacht van cryptografie-programma's te vervalsen. Verder zou men het te bespioneren toestel dienen te voorzien van een cryptografieprogramma dat een «Trojaans paard» bevat, zonder dat de gebruiker er zich van bewust is. Bovendien zou deze techniek hoogstwaarschijnlijk heel wat sporen nalaten op de machine die bespioneerd wordt. Het zou dus niet gaan om een afluistering die door iedereen toepasbaar zou zijn en die geen sporen zou nalaten.

Het is eerder aannemelijk dat deze NSA_KEY een soort wisselsleutel is van Microsoft, die gebruikt zou worden als de eerste, originele sleutel vernietigd of onderschept is.

In dit geval is het belangrijkste verwijt aan Microsoft dat de gebruiker niet weet of het de originele sleutel of de wisselsleutel is die gebruikt wordt voor de validiteit van de cryptografieprogramma's op zijn machine. Zulke waarschuwing zou de NSA-KEY weinig bruikbaar maken in de praktijk.

Volgens de mening van verscheidene experten vertoont de cryptografie «Made in Microsoft» heel wat andere fouten en gebreken die veel gemakkelijker uit te buiten zijn, en mag heel de mediaheisa rond deze zaak onze aandacht niet afleiden van deze fouten en gebreken.

Als conclusie wil ik stellen dat het mogelijk is dat de NSA_KEY door het NSA gesmeed werd en dat momenteel het tegendeel niet kan bewezen worden (*probatio diabolica*). Maar indien deze sleutel het werk is van het NSA, is het onmiddelijke gevaar dat veroorzaakt wordt door kennis van deze sleutel abso-

ouvertes postérieures au rapport de février 2000 sur le réseau Echelon, je maintiens tout à fait et réaffirme avec force mon point de vue exposé à la section 4.2 du dit rapport.

J'y ajoute que, depuis lors, Microsoft a répondu, selon moi, de manière transparente et honnête aux douze premières questions qui lui furent posées par écrit par Duncan Campbell. Par la suite ce dernier a reformulé de manière vexatoire et agressive certaines des questions auxquelles il avait déjà été répondu et en a rajouté d'autres. C'est à ce moment que Microsoft a décidé d'interrompre des «échanges non constructifs».

Il est techniquement possible mais peu vraisemblable que cette deuxième clé (la NSA-KEY) soit issue de la NSA. Même si cela était le cas, cela permettrait tout juste à cette dernière de falsifier la signature de contrôle de programmes cryptographiques. Encore faudrait-il pouvoir télécharger sur la machine à espionner un programme cryptographique doté d'un cheval de Troie sans que l'utilisateur s'en aperçoive. En outre cette technique laisserait probablement pas mal de traces sur la machine espionnée elle-même. Il ne s'agirait donc pas d'une écoute applicable à tous et qui ne laisserait aucune trace.

Il est plus vraisemblable que cette NSA_KEY soit une clé de rechange de Microsoft, utilisable si la première clé originale venait à être détruite ou compromise.

Dans ce cadre, le principal reproche fait à Microsoft est que l'utilisateur ne sait pas si c'est la clé originale ou la clé de rechange qui est utilisée pour valider les programmes cryptographiques installés sur sa machine. Un tel avertissement rendrait cette NSA-KEY peu utilisable dans la pratique.

De l'avis de nombreux experts, la cryptographie «Made in Microsoft» présente bien d'autres lacunes et failles bien plus faciles à exploiter et le brouhaha médiatique autour de cette affaire ne doit pas distraire notre attention de ces failles et lacunes.

En conclusion, il est possible que la NSA-KEY ait été forgée par la NSA et il est actuellement impossible de prouver le contraire (*probatio diabolica*). Même si cette clé est l'œvre de cette dernière, le danger directement créé par la connaissance de cette clé pour la sécurité des informations est minime dans l'absolu et

luut miniem voor de veiligheid van de informatie, en hangt het ook af van andere structurele en punctuele gebreken van de cryptografie «Made in Microsoft» (1).

Ondertekend: Jean-Marc Dinant

5. De conclusies van het Comité I

Het Comité I besluit het volgende:

1) wat betreft het bestaan van Echelon en zijn activiteiten:

— noch het bestaan, noch de omvang, noch het gebruik van het interceptienetwerk voor telecommunicaties, zoals werd beschreven in het STOA-verslag van de heer Campbell, werd officieel erkend door de betrokken regeringen (de Verenigde Staten, Groot-Brittannië, Canada, Australië en Nieuw-Zeeland);

— welke ook de codenaam mag zijn die aan hun systemen wordt gegeven (de codenaam «Echelon» verschijnt nooit in officiële recente documenten), het blijft vanzelfsprekend dat de Verenigde Staten en Groot-Brittannië over officiële diensten beschikken (het NSA en het GCHQ), die belast zijn met het intercepteren van telecommunicaties om veiligheidsredenen, en omwille van «the interest of the national well-beeing» (het belang van het nationaal welzijn) van de betrokken landen;

— het bestaan van het UKUSA-Verdrag, en dit van een technische samenwerking tussen de interceptieorganismen van de vijf Angelsaksische landen zijn heden ten dage officieel erkend;

— de technische- en personeelscapaciteiten van deze diensten zijn enorm; »Echelon» zou in staat zijn het geheel van communicaties van alle satellieten op te vangen (ongeveer een honderdste van alle internationale telefooncommunicaties);

— de technologie zou evenwel nog geen verkennend en algemeen toezicht toelaten op telefonische communicaties, die enkel op een automatisch opzoekingsysteem met trefwoorden zijn gebaseerd. Momenteel bestaan er enkel systemen die, — via het herkennen van de stem —, een specifiek individu kunnen opsporen als deze een internationale communicatie uitvoert;

— zo'n interceptiesysteem heeft ook te kampen met het probleem om de enorme hoeveelheid aan ingezamelde gegevens te beheren;

— er bestaan ernstige aanwijzingen, maar geen enkel sluitend bewijs, dat de afluistercapaciteiten kunnen gebruikt worden voor economische spionage, gericht op de landen van de Europese Unie;

— dit soort toepassingen vormen ongetwijfeld een aanslag op het privé-leven van burgers en zouden de

(1) Vrije vertaling.

relativement aux autres failles structurelles et ponctuelles de la cryptographie made in Microsoft» (1).

Signé: Jean-Marc Dinant

5. Conclusions du Comite permanent R

Le Comité R conclut ce qui suit:

1) en ce qui concerne l'existence «d'Echelon» et ses activités:

— ni l'existence, ni les capacités, ni les pratiques du réseau d'interception de communications, telles que décrites par le rapport STOA de M. Campbell n'ont jamais été reconnues officiellement par les gouvernements mis en cause (États-Unis, Grande-Bretagne, Canada, Australie, Nouvelle-Zélande);

— quel que soit le nom de code donné à leurs systèmes (le code «Echelon» n'apparaît jamais dans les documents officiels récents), il est évident que les États-Unis, la Grande-Bretagne, le Canada et l'Australie notamment, disposent de services officiels (la NSA, le GCHQ, le CST, le DSD) 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;

— l'existence du traité UKUSA et celle d'une collaboration technique entre les organismes d'interception de ces cinq pays anglo-saxons sont à présent reconnues officiellement;

— les capacités techniques et en personnel de ces services sont énormes: «Echelon» serait capable de capter la totalité des communications passant par satellites (environ un pour-cent des communications téléphoniques internationales);

— toutefois, la technologie ne permettrait pas encore une surveillance exploratoire et généralisée sur base d'un système de recherche automatique de mots clés dans des conversations téléphoniques; seuls existent actuellement des systèmes de reconnaissance d'empreintes vocales qui permettent de repérer la voix d'un individu spécifique lorsque celui-ci passe une communication internationale;

— un tel système d'interception se heurte aussi à la maîtrise de l'immense quantité de données récoltées;

— 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 entreprises de pays de l'Union européenne;

— une telle pratique constituerait assurément une atteinte à la vie privée des citoyens et violerait les prin-

(1) Traduction libre.

algemene richtlijnen van de Europese Unie, die het intercepteren van tele-communicaties strikt aan banden legt, overtreden;

— de dubbelzinnige verklaringen van de Amerikaanse en Britse overheden over dit onderwerp laten niet toe om de twijfel weg te nemen;

— 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 en residenten van deze twee landen en niet tot onderdanen van andere Staten;

— de heer J. Woolsey, voormalig directeur van de CIA, geeft toe dat de CIA economische inlichtingen behandelt, maar hij bevestigt dat 95% van de ingewonnen gegevens van open bronnen afkomstig zijn. Hij bevestigt tevens dat de CIA niet optreedt op gebied van economische spionage ten voordele van Amerikaanse ondernemingen of instellingen. Voor de heer Woolsey gaat het om beschermende maatregelen die gerechtvaardigd zijn omwille van de corrupte handelingen van sommige Europese ondernemingen. De heer Woolsey verwijst niet naar andere middelen die gebruikt worden bij het inzamelen van inlichtingen.

2) wat betreft de houding van de Belgische inlichtingendiensten:

— zowel de Administrateur-generaal van de Veiligheid van de Staat als de Chef van de ADIV 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 ADIV verklaart dat de eventuele militaire spionage uitgaande van de aan België geallieerde landen voor haar geen prioriteit in haar opdrachten betekent;

— de Veiligheid van de Staat heeft nog geen instructies ontvangen van het Ministerieel Comité voor Inlichtingen en Veiligheid inzake de bescherming van het economisch en wetenschappelijk potentieel; zij heeft nog geen belangrijke middelen ingezet voor deze nieuwe opdracht;

— zowel de Veiligheid van de Staat als de ADIV betreuren dat zij niet kunnen overgaan tot veiligheidsintercepties binnen een wettelijk kader;

— de ADIV werkt evenwel vanuit de hypothese dat de interceptie van communicaties werkelijk bestaat en, — ongeacht het land dat ze uitvoert —, dat men er zich tegen moet beschermen; de ADIV vindt eveneens dat éénder welk systeem van informatica-cijfercode kan verbroken worden;

— belast zijnde met de veiligheid van de communicaties van de Strijdkrachten, heeft de ADIV verschillende regels opgesteld met als doel de vertrouwelijkheid te vrijwaren van geclassificeerde gegevens die door telecommunicatie worden doorgezonden of door informaticasystemen behandeld worden;

cipes généraux du Conseil de l'Europe qui limitent strictement les interceptions de télécommunications;

— les déclarations ambiguës des autorités américaines et britanniques à ce sujet ne permettent pas de lever le doute;

— les garanties pour le respect de la vie privée et les recours offerts par les législations américaine, britannique et canadienne ne s'adressent d'ailleurs qu'aux citoyens et résidents de ces pays et non aux ressortissants des autres États;

— M. James Woolsey, ancien directeur de la CIA, admet que la CIA pratique le renseignement économique mais il affirme que 95% des informations collectées proviennent de sources ouvertes. Il affirme également que la CIA n'est pas engagée dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines. Pour M. Woolsey, il s'agit de mesures de protection justifiées par les manouvres de corruption pratiquées par certaines entreprises européennes; M. Woolsey n'indique pas les autres moyens mis en ouvre pour recueillir le renseignement;

2) en ce qui concerne l'attitude des services de renseignement belges:

— les responsables de la Sûreté de l'État et du SGR déclarent que leurs services ne suivent pas le système «Echelon» étant donné qu'ils ne disposent pas des moyens humains, techniques et légaux nécessaires pour le faire;

— le SGR déclare que l'espionnage militaire éventuel émanant de pays alliés de la Belgique ne constitue pas pour lui une priorité dans ses missions;

— 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;

— 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, qu'il faut donc s'en prémunir , quel que soit le pays qui les pratique, 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;

— de ADIV volgt van dichtbij de ontwikkeling van de wetgeving inzake cryptografie; zij stelt voor dat een officieel organisme belast zou worden met het veiligheidsbeleid inzake informatie in België.

6. Aanbevelingen

— Vaststellende dat de Belgische inlichtingendiensten (Veiligheid van de Staat en de ADIV) geen enkele taak van informatie-inwinning en -analyse hebben uitgevoerd met betrekking tot het mogelijk bestaan van een interceptienetwerk voor telecommunicaties, genaamd Echelon, dat gestuurd zou worden door de Verenigde Staten en Groot-Brittannië;

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

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

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

— zich baserend op de conclusies en aanbevelingen van de heren Poullet en Dinant;

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

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

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

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

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

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

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

— 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.

6. Recommandations

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

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

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

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

— S'associant aux conclusions et recommandations de MM. Poullet et Dinant;

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

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

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

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

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

— 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.

7. De brondocumenten

De documenten op basis waarvan het huidige verslag werd samengesteld, zijn de volgende: documenten van het Europees Parlement:

— «Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control)»:

deel 1/4: «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception» (mei 1999);

deel 2/4: «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law» (april 1999);

deel 3/4: «Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues» (April 1999);

deel 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);

volume 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»; (oktober 1999);

volume 2/5: «The state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition» (oktober 1999) - Duncan Campbell;

volume 3/5: «Chiffrement, cryptosystèmes et surveillance électronique: un survol de la technologie» (oktober 1999) - professor Frank Leprévot;

volume 4/5: «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law» (oktober 1999) - professor Chris Elliot;

volume 5/5: «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception» (oktober 1999).

7. Les documents «Sources»

Les documents sur base desquels le présent rapport a été rédigé sont les suivants: les 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» (mai 1999);

part 2/4: «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law» (avril 1999);

part 3/4: «Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues» (avril 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» (avril 1999);

volume 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);

volume 2/5: «The state of the art in communications intelligence (COMINT) of auto mated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition» (octobre 1999) - Duncan Campbell;

volume 3/5: «Chiffrement, cryptosystèmes et surveillance électronique: un survol de la technologie» (octobre 1999) - professeur Frank Leprévot;

volume 4/5: «The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law» (octobre 1999) - professor Chris Elliot;

volume 5/5: «The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception» (octobre 1999).

— Lexicon —

Definitie «Open Bronnen» : in zijn activiteitenverslag van 1996 definieerde het Comité I open bronnen als volgt:"(...) zijn alle bronnen die wettelijk en ethisch gezien voor het publiek toegankelijk zijn, al dan niet tegen betaling» (Activiteitenverslag Comité I - 1996, Titel III, Hoofdstuk 3, blz. 214)

BND: *Bundesnachrichtendienst* (Deutschland)

CIA: *Central Intelligence Agency* (USA)

CSE: Canadian Communications Security Establishment - provides the Government of Canada with foreign Sigint Intelligence

DGSE: Direction Générale de la Sécurité extérieure (France)

DSD: *Defense Signals Directorate (Australia)*

FBI: *Federal Bureau of Investigation, the National Law Enforcement and Counter intelligence agency of the USA*

GCHQ: *Government Communications Headquarters - the SIGINT-agency of the UK*

GCSB: *Government Communications Security Bureau (New Zealand)*

INTELSAT: *International Telecommunications Satellite*

JIC: *Joint Intelligence Committee (UK)*

LMR: «Le Monde du Renseigement», een tweemaandelijks periodiek uitgegeven in het Frans en het Engels door de groep *Indigo Publications*, Parijs, Frankrijk

MI 6: *Secret Intelligence Service (UK)*

NSA: *National Security Agency USA, the SIGINT-Agency of the USA*

STOA: *Science and Technology Options Assessment of the European Parliament*

UKUSA: *United States of America, United Kingdom, Canada, Australia and New Zealand (UKUSA Agreement)*

Het «NSA» (USA) en het «GCHQ» (UK) hebben in 1948 een geheim akkoord afgesloten, dat hen verenigde met het Canadese «CSE».

Het Australische «DSD» en nadien het Nieuw-Zeelandse «GCSB» hebben zich eveneens aangesloten bij dit consortium, die op de politieke en militaire inlichting; het drugverkeer; het terrorisme en de economische wereld werken.

— Lexicon —

Définition «Source Ouverte»: dans son rapport d'activités 1996, le Comité R a définit les sources ouvertes comme suit:«les sources qui, d'un point de vue éthique ou légal, sont accessibles au public moyennant paiement ou non». (Rapport d'activités 1996 - Titre III - Chapitre 3, p. 208).

BND: *Bundesnachrichtendienst* (Allemagne-Duitsland)

CIA: *Central Intelligence Agency (USA)*

CSE: *Canadian Communications Security Establishment - provides the Government of Canada with foreign Sigint Intelligence*

DGSE: Direction Générale de la Sécurité extérieure (France-Frankrijk)

DSD: *Defense Signals Directorate (Australia)*

FBI: *Federal Bureau of Investigation, the National Law Enforcement and Counter-intelligence agency of the USA*

GCHQ: *Government Communications Headquarters - the Sigint- agency of the UK*

GCSB: *Government Communications Security Bureau (New Zealand)*

INTELSAT: *International Telecommunications Satellite*

JIC: *Joint Intelligence Committee (UK)*

LMR: Le Monde du Renseigement, périodique bimensuel édité en français et en anglais par le groupe *Indigo Publications*, Paris, France

MI6: *Secret Intelligence Service (UK)*

NSA: *National Security Agency USA, the Sigint Agency of the USA*

STOA: *Science and Technology Options Assessment of the European Parliament*

UKUSA *agreement:* Accord associant les États-Unis, la Grande-Bretagne (UK-USA), le Canada, l'Australie et la Nouvelle Zélande.

La NSA et le GCHQ ont conclu en 1948 un accord secret, les unissant avec le CSE Canadien.

Le DSD australien , puis le GCSB néo-zélandais ont rejoint le consortium, qui travaille sur le renseignement politique et militaire, sur le trafic de drogue, le terrorisme et sur le monde économique .

HOOFDSTUK 2

VERSLAG VAN HET ONDERZOEK NAAR DE WIJZE WAAROP DE INLICHTINGENDIENSTEN GEREAGEERD HEBBEN OP EVENTUELE SPIONAGEFEITEN OF POGINGEN TOT INDRINGING IN HET INFORMATICASYSTEEM VAN EEN BELGISCH ONDERZOEKSCENTRUM

1. Inleiding

Op 19 juli 2000 hebben een aantal parlementsleden, leden van de Commissies van de Senaat en de Kamer van volksvertegenwoordigers, die respectievelijk belast zijn met het opvolgen van de Vaste Comités I en P, aan het Comité I gevraagd aandacht te besteden aan mogelijke pogingen van indringing in het computersysteem van een universitair onderzoekscentrum, waarvan ze kennis hadden gekregen.

Deze vraag paste in het kader van het onderzoek van deze commissies over het verslag van het onderzoek naar de manier waarop de Belgische inlichtingendiensten hebben gereageerd op het mogelijk bestaan van een Amerikaans systeem, 'Echelon' genaamd, voor het intercepteren van het telefoon- en faxverkeer.

Gevolg gevend aan dit verzoek heeft een delegatie van het Comité I op dinsdag 25 juli 2000 een onderhoud gehad met de directeur en de verantwoordelijke inzake computerbeveiliging van het centrum. Uit dit inleidend onderhoud heeft het Comité I vooral de volgende zaken onthouden:

— nadat het centrum in 1999 met een vreemd land een belangrijk contract had gesloten betreffende de levering van experimenteermaterieel, waren pogingen ondernomen om binnen te dringen in het computersysteem van het centrum. De directie van het centrum situeerde de herkomst van deze pogingen in Duitsland en de Verenigde Staten (Washington);

— het centrum had dit contract kunnen sluiten nadat de regering van de Verenigde Staten aan een Amerikaanse onderneming het verbod had opgelegd hetzelfde soort materieel uit te voeren om redenen van non-proliferatie;

— volgend op deze pogingen tot elektronische indringing, werd er ingebroken in de gebouwen van het centrum. De daders hebben computers gemanipuleerd en onderdelen van computers gestolen (een toetsenbord):

— de politie heeft een onderzoek gevoerd naar deze diefstal met braak. In het kader van dit onderzoek heeft een inspecteur van de Veiligheid van de Staat een onderhoud gehad met de verantwoordelijken van het centrum. De directeur van het centrum heeft de feiten ook gemeld aan een aantal parlementsleden;

CHAPITRE 2

RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LES SERVICES DE RENSEIGNEMENT (SURETÊ DE L'ÉTAT ET SGR) ONT RÉAGI À PROPOS D'ÉVENTUELS FAITS D'ESPIONNAGE OU DE TENTATIVES D'INTRUSION DANS LE SYSTÈME INFORMATIQUE D'UN CENTRE DE RECHERCHE BELGE

1. Introduction

Le 19 juillet 2000, des parlementaires, membres des Commissions du Sénat et de la Chambre des représentants chargées respectivement de l'accompagnement des Comités permanents R et P, ont demandé au Comité R de s'intéresser à d'éventuelles tentatives d'intrusion dans le système informatique d'un centre de recherche universitaire dont ils avaient eu connaissance.

Cette demande s'inscrivait dans le cadre de l'examen par lesdites commissions du rapport d'enquête sur la manière dont les services belges de renseignement réagissaient face à l'éventualité d'un système américain «Echelon» d'interception des communications téléphoniques et fax en Belgique.

Faisant suite à cette demande, une délégation du Comité R a rencontré le directeur et le responsable de la sécurité informatique de ce centre le mardi 25 juillet 2000. De cet entretien préliminaire, le Comité R a retenu les éléments qui suivent:

— alors qu'il venait de conclure en 1999 un contrat important de fourniture d'un certain matériel d'expérimentation avec un pays étranger, le centre a été la cible de tentatives d'intrusions dans son système informatique dont la direction situe la provenance en Allemagne et aux États-Unis (Washington);

— ce contrat avait été obtenu après que le gouvernement des États-Unis eût interdit à une firme américaine d'exporter ce même type de matériel pour des raisons de non prolifération;

— ces tentatives d'intrusions électroniques furent suivies d'une effraction dans les bâtiments du centre au cours de laquelle les ordinateurs ont été manipulés et des composants informatiques volés (un clavier d'ordinateur);

— une enquête a été menée par la police sur ce vol avec effraction et c'est à cette occasion que les responsables du centre ont reçu la visite d'un inspecteur de la Sûreté de l'État. Le directeur du centre a également mis au courant certains parlementaires des faits précités;

— volgens de directeur waren de feiten van indringing niet zozeer gericht op de technologische gegevens van het centrum, omdat deze gegevens beschikbaar zijn in de wetenschappelijke literatuur. Bijgevolg is het helemaal niet nodig zijn toevlucht te nemen tot spionage om de hand te leggen op deze gegevens. Hij beweert dat zijn centrum geen gevoelige, hoogtechnologische informatie bezit. De daders hadden het veeleer gemunt op de commerciële gegevens betreffende het contract dat het centrum met een vreemd land had gesloten.

Niettemin meende het Comité I dat dit centrum een interessant doelwit kon zijn, niet alleen van economische en/of technologische spionage, maar ook van militaire spionage. Tijdens het onderhoud was immers gebleken dat dit centrum binnen afzienbare tijd militair materieel ging testen.

De directeur van het centrum had ook verklaard dat hij een aanvraag had ingevuld om voor zichzelf en voor zijn personeel een veiligheidsmachtiging te verkrijgen. Hij had ook heel strikte veiligheidsinstructies gekregen betreffende de opslag van dit materieel in de lokalen van het centrum.

2. Procedure

Op 11 augustus 2000 nam het Comité I contact op met het parket van de procureur des Konings om informatie te krijgen over de diefstal met braak die in 1999 in het onderzoekscentrum was gepleegd. Het Comité I ontving deze informatie op 23 augustus 2000.

Op 23 augustus 2000 besliste het Comité I een onderzoek te openen naar «de wijze waarop de inlichtingendiensten (Veiligheid van de Staat en de Algemene Dienst inlichting en veiligheid) gereageerd hebben op eventuele spionagefeiten of pogingen tot binnendringen in het informaticasysteem van een Belgisch onderzoekscentrum».

Op 28 augustus 2000 stuurde het Comité I een kantschrift naar het hoofd van de Dienst enquêtes.

Overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, heeft de voorzitter van het Comité I de voorzitter van de Senaat, per brief van 31 augustus 2000, kennis gegeven van de opening van dit onderzoek.

Overeenkomstig artikel 43, 1º, van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten heeft het hoofd van de dienst enquêtes de minister van Justitie en de minister van Landsverdediging, per brief van 31 augustus 2000, op de hoogte gebracht van de opening van dit onderzoek.

— selon le directeur, ce ne seraient pas tant les données technologiques du centre qui auraient été la cible de ces intrusions, car celles-ci sont disponibles dans la littérature scientifique et il n'est donc pas nécessaire de recourir à l'espionnage pour se les procurer. Selon lui, son centre ne détient aucune information sensible de haute technologie. Ce seraient plutôt les données commerciales du marché conclu avec le pays étranger qui auraient été visées.

Néanmoins, le Comité R a estimé que le centre en question pouvait être une cible intéressante non seulement pour l'espionnage économique et/ou technologique, mais également pour l'espionnage militaire puisqu'il est apparu au cours de l'entretien que ce centre devait prochainement tester du matériel militaire.

D'ailleurs, le directeur du centre a déclaré avoir rempli une demande d'habilitation de sécurité pour lui et son personnel et avoir reçu des consignes de sécurité très strictes pour l'entreposage de ce matériel dans ses locaux.

2. Procédure

Le 11 août 2000, le Comité R s'est adressé au parquet du procureur du Roi afin d'obtenir des informations concernant le vol avec effraction au centre de recherche en 1999. Ces informations ont été obtenues le 23 août 2000.

Le Comité R a décidé le 23 août 2000 d'ouvrir une enquête «sur la manière dont les services de renseignement (Sûreté de l'État et SGR) ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge».

Une apostille a été adressée au chef du Service d'enquêtes le 28 août 2000.

Par courrier du 31 août 2000, conformément à l'article 32, de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le président du Comité R a informé le président du Sénat de l'ouverture de la présente enquête.

Par courrier du 31 août 2000, le chef du Service d'enquêtes, conformément à l'article 43, 1º, de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, a informé les ministres de la Justice et de la Défense nationale de l'ouverture de la présente enquête.

De Dienst enquêtes van het Comité I heeft in het vierde trimester van het jaar 2000 diverse onderzoeksopdrachten vervuld. Op 11 januari 2001 heeft deze Dienst zijn verslag ingediend.

Na dit verslag en het onderzoeksdossier te hebben bestudeerd, heeft het Comité I op 13 maart 2001 een als geheim geclassificeerd verslag, krachtens de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, goedgekeurd.

Dezelfde dag heeft het Comité I de vertrouwelijke versie van dit verslag goedgekeurd in de zin van de wet d.d. 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, bestemd voor de leden van de Commissies van de Senaat en de Kamer van Volksvertegenwoordigers, die respectievelijk belast zijn met de opvolging van de Vaste Comités I en P.

De vertrouwelijke versie is bestemd om te worden gepubliceerd in het activiteitenverslag van het Comité I.

3. Vaststellingen

3.1 Vaststellingen bij de Veiligheid van de Staat

Een agent van de buitendiensten van de Veiligheid van de Staat heeft de zaak van de diefstal van computermaterieel in het onderzoekscentrum inderdaad gevolgd, alsook de pogingen tot indringing in het computersysteem.

Dit onderzoek steunt op de twee wettelijke opdrachten waarmee de Veiligheid van de Staat is belast, nanmelijk het opsporen, analyseren en verwerken van inlichtingen betreffende bedreigingen zoals proliferatie en economische en wetenschappelijke spionage (artikelen 7 en 8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten).

Dit onderzoek heeft geleid tot een interne uitwisseling van geclassificeerde rapporten tussen de verschillende afdelingen van de Veiligheid van de Staat die met voornoemde materies zijn belast.

Deze rapporten bevatten een aantal heel relevante opmerkingen, in het bijzonder over de houding van het universitair wetenschappelijk milieu ten overstaan van het probleem van de veiligheid van informatiesystemen, de risico's die het gebruik van bepaalde software met zich meebrengt, de tekortkomingen van beveiligingssystemen, de uitvoer van materieel voor tweeërlei gebruik, enz.

Er werden interessante voorstellen gedaan inzake openstelling naar en samenwerking met het wetenschappelijk milieu. In één rapport lezen we zelfs dat het centrum een beroep zou hebben gedaan op de expertise van de Veiligheid van de Staat.

Le service d'enquêtes du Comité R a procédé à divers devoirs d'enquêtes au cours du quatrième trimestre de l'année 2000. Il a rentré son rapport le 11 janvier 2001.

Après avoir examiné ce rapport, ainsi que le dossier de l'enquête, le Comité R a approuvé, à la date du 13 mars 2001, un rapport classifié «secret» en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

À la même date, le Comité R a également approuvé la version confidentielle du présent rapport au sens de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements destinée aux membres des commissions du Sénat et de la Chambre des représentants chargées respectivement de l'accompagnement des Comités permanents R et P.

Cette version confidentielle est destinée à être publiée dans le rapport d'activités du Comité R.

3. Constatations

3.1. Les constatations à la Sûreté de l'État

Un agent des services extérieurs de la Sûreté de l'État a bien suivi l'affaire du vol de matériel informatique au centre de recherche ainsi que les tentatives d'intrusion dans son système informatique.

Cette enquête trouve bien son fondement dans deux des missions légales attribuées à la Sûreté de l'État, à savoir rechercher, analyser et traiter le renseignement relatif à des menaces telles que la prolifération et l'espionnage économique et scientifique (articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).

Cette enquête a donné lieu à un échange interne de rapports classifiés entre les différents services de la Sûreté de l'État en charge des matières précitées.

Des observations particulièrement pertinentes y ont été consignées, notamment en ce qui concerne l'attitude du milieu scientifique universitaire à l'égard du problème de la sécurité des systèmes d'information, les risques liés à l'emploi de certains logiciels, les failles des systèmes de protections, l'exportation de certains matériels à usage dual, etc..

Des propositions intéressantes d'ouverture et de collaboration avec les milieux scientifiques ont été émises. Un rapport indique même que le centre aurait sollicité l'expertise de la Sûreté de l'État.

Blijkbaar werd echter niet het minste gevolg gegeven aan deze opmerkingen en voorstellen. De Veiligheid van de Staat beschikt niet over de vereiste bekwaamheden om in te staan voor het beveiligen van de computersystemen van onderzoekscentra. Bijgevolg heeft ze deze opdracht niet vervuld.

Nergens hebben we vastgesteld dat artikel 19 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten zou zijn toegepast. Dit betekent dat er blijkbaar niet de minste informatie werd bezorgd aan enige, ter zake bevoegde, gerechtelijke, politieke of administratieve overheid.

Het Comité I is nochtans van mening dat bepaalde inlichtingen en aanbevelingen in de rapporten die het heeft bestudeerd, hadden kunnen worden gedeclassificeerd en op nuttige wijze ter kennis gebracht konden worden van bepaalde overheden.

3.2. Vaststellingen bij de Algemene Dienst inlichting en veiligheid

De ADIV kent het bewuste onderzoekscentrum omdat dit centrum een veiligheidsmachtiging heeft gekregen krachtens dewelke het occasioneel voor Landsverdediging kan werken. Dit belang berust op de opdrachten waarmee de ADIV is belast krachtens artikel 11 van de wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en de veiligheidsdiensten.

De ADIV verklaart alleen tengevolge van het openen van dit onderzoek kennis te hebben gekregen van de veiligheidsincidenten in het centrum.

De ADIV verklaart in deze zaak niet te zijn tussengekomen, omdat deze dienst geloof hechtte aan de uitleg van de veiligheidsverantwoordelijke van het centrum. Deze laatste had verklaard dat de incidenten de activiteiten inzake «Landsverdediging» van het centrum niet hadden ondermijnd. De ADIV heeft nadien geen enkel onderzoek gevoerd om de gegrondheid van deze verklaringen na te gaan.

De ADIV verantwoordt het gebrek aan interventie ook door het tekort aan bekwame medewerkers op deze dienst.

Het feit dat het centrum momenteel is belast met een opdracht in het kader van een internationaal project inzake militaire ontwikkeling waaraan de Belgische regering wil meewerken, lijkt niet in het bijzonder de aandacht van de ADIV te hebben getrokken.

3.3. Vaststellingen betreffende de samenwerking tussen de Veiligheid van de Staat en de ADIV

Deze twee diensten hebben niet samengewerkt, hoewel ze beide wettige belangen hadden om aandacht te besteden aan dit centrum.

Aucune suite ne semble avoir été donnée à ces remarques et propositions. La Sûreté de l'État ne dispose pas des compétences nécessaires pour assurer la sécurisation des systèmes informatiques des centres de recherche, elle n'a donc pas pu pourvoir à cette tâche.

Aucune application de l'article 19 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité n'a été constatée, à savoir qu'aucune information relative à cette affaire ne paraît avoir été communiquée à une quelconque autorité judiciaire, politique ou administrative compétente dans les matières traitées.

Le Comité R estime pourtant que certaines informations et recommandations contenues dans les rapports qu'il a examinés pouvaient être déclassifiées et utilement communiquées à certaines autorités.

3.2. Les constatations au SGR

Le SGR connaît le centre de recherche dans le cadre de l'habilitation de sécurité accordée pour lui permettre de travailler occasionnellement pour la Défense nationale. Cet intérêt trouve son fondement dans les missions attribuées au SGR par l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le SGR déclare ne pas avoir été mis au courant des incidents de sécurité du centre, autrement que par le déclenchement de la présente enquête.

Le SGR justifie son absence d'intervention dans cette affaire en acceptant pour argent comptant les explications du responsable de la sécurité du centre qui déclare que les incidents n'ont pas affecté l'activité «Défense nationale» du centre. Le SGR n'a mené aucune enquête subséquente pour vérifier le bien fondé de cette allégation.

Le SGR justifie également son absence d'intervention par le manque de moyens humains qualifiés dont il dispose.

Pourtant, le fait que le centre soit actuellement investi d'une mission dans le cadre d'un projet international de développement militaire auquel le gouvernement belge veut s'associer ne semble pas avoir attiré spécialement l'attention du SGR.

3.3. Les constatations en ce qui concerne la collaboration entre la Sûreté de l'État et le SGR

Cette collaboration fut inexistante alors que ces deux services avaient chacun leurs intérêts légitimes pour s'occuper du centre.

Bijgevolg kan men stellen dat de ADIV en de Veiligheid van de Staat geen gevolg hebben gegeven aan hun verplichting tot samenwerking krachtens artikel 20 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

3.4. Vaststellingenbetreffendedesamenwerkingmet de politiediensten en het openbaar ministerie

Het Comité I stelt vast dat de Veiligheid van de Staat bij de politie informatie heeft ingewonnen over de diefstal met braak in het onderzoekscentrum. Op basis van deze informatie kon de Veiligheid van de Staat een onderzoek openen. Ze heeft deze informatie verkregen op informele wijze.

De politie heeft de diefstal behandeld onder de hoofdnoemer « diefstal met braak en inklimming », en de feiten werden als zodanig gecodeerd. Dit komt inderdaad overeen met de strafrechtelijke kwalificatie van de vastgestelde feiten, maar zegt niets over de eventuele onderliggende intentie van spionage. Het laat evenmin een statistische, analytische en criminalistische exploitatie van dit fenomeen toe op nationaal laat staan internationaal niveau.

Voor zover het Comité I weet, bestaat er op het openbaar ministerie geen notitienummer dat het mogelijk maakt een verband te leggen tussen processen-verbaal die worden opgemaakt naar aanleiding van de hierboven beschreven feiten enerzijds en economische of wetenschappelijke spionage anderzijds.

4. Algemene besluiten

Deze zaak kan tot voorbeeld dienen. Hij toont immers aan dat er in België onderzoekscentra bestaan die een interessant doelwit kunnen zijn, niet alleen van economische en/of technologische spionage, maar ook van militaire spionage.

De bescherming van het wetenschappelijk en economisch potentieel van het land behoort tot de nieuwe opdrachten van de Veiligheid van de Staat. Het behoud van de militaire veiligheid en van de veiligheid van de installaties, de informatica- en de telecommunicatiesystemen die Landsverdediging aangaan, is één van de opdrachten van de ADIV.

De Veiligheid van de Staat heeft slechts bij toeval kennis gekregen van de pogingen tot indringing en diefstal in het onderzoekscentrum. De ADIV werd pas op de hoogte gebracht tengevolge van dit onderzoek.

De Veiligheid van de Staat heeft op actieve wijze inlichtingen ingewonnen over deze zaak. Het Comité I betreurt echter dat de ADIV ter zake geen enkel initiatief heeft genomen. Beide diensten hebben niet met elkaar samengewerkt.

En ce sens, le SGR et la Sûreté de l'État n'ont pas fait application de leur devoir de collaboration prescrit par l'article 20 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

3.4. Les constatations en ce qui concerne la collaboration avec les services de police et le ministère public

Le Comité R constate que la Sûreté de l'État a recueilli auprès de la police une information concernant le vol avec effraction commis au centre de recherche, ce qui lui a permis de démarrer son enquête. Cette information a été recueillie de manière informelle.

Au niveau policier, ce vol a été traité sous le registre principal de « vol à l'aide d'effraction et escalade » et encodé comme tel. Si ce traitement correspond bien à la qualification pénale des faits constatés, il ne rend pas compte de l'intention sous-jacente éventuelle d'espionnage; il ne permet pas non plus une exploitation statistique, analytique et criminalistique spécifique de ce phénomène au niveau national, voire international.

À la connaissance du Comité R, il n'existe pas au sein du ministère public de notice permettant de relier les procès-verbaux dressés à l'occasion des faits précités au thème de l'espionnage économique ou scientifique.

4. Conclusions générales

La présente affaire est exemplative car elle démontre qu'il existe en Belgique des centres de recherches susceptibles d'être une cible intéressante non seulement pour l'espionnage économique et/ou technologique, mais également pour l'espionnage militaire.

La protection du potentiel scientifique et économique du pays est l'une des nouvelles missions de la Sûreté de l'État. Le maintien de la sécurité militaire, celle des installations, des systèmes informatiques et de télécommunications qui intéressent la Défense nationale, est une des missions du SGR.

Or, les tentatives d'intrusion et de vol au centre de recherche ne sont parvenus aux oreilles de la Sûreté de l'État que de manière fortuite. Le SGR n'en a été informé qu'à la suite de la présente enquête.

Si la Sûreté de l'État s'est activement investie à recueillir des informations sur cette affaire, le Comité R regrette la passivité du SGR en la matière. Les deux services n'ont pas collaboré.

Het Comité I betreurt ook dat geen enkel gevolg werd gegeven aan de vragen om bijstand en de voorstellen tot samenwerking tussen het wetenschappelijk milieu en de Veiligheid van de Staat.

Geen enkele dienst beschikt immers over de vereiste bekwaamheden om in te staan voor het beveiligen van de computersystemen van onderzoekscentra.

Tot slot betreurt het Comité I dat de interessante informatie die de Veiligheid van de Staat heeft ingewonnen, niet is doorgespeeld aan enige, ter zake bevoegde, gerechtelijke, politieke of administratieve overheid.

In deze zaak werden de artikels 19 en 20 van de wet d.d. 30 november 1998 houdende regeling van de inlichtingen- en de veiligheidsdiensten, die enerzijds de mededeling van inlichtingen en anderzijds de samenwerking tussen diensten onderling regelen, niet toegepast.

5. Aanbevelingen

Het sluiten van een specifiek akkoord tussen de gerechtelijke overheden en de inlichtingendiensten, in het kader van artikel 14 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, zou in het bijzonder tot doel moeten hebben de uitwisseling van informatie over militaire, economische en wetenschappelijke spionage tussen deze overheden te bevorderen.

Binnen dat kader vraagt het Comité I zich af of er niet tevens dient te worden nagedacht over de uitwerking van een specifiek notitienummer met betrekking tot economische, wetenschappelijke en industriële spionage. Dit notitienummer zou bij de klassieke notitienummers van gemeen strafrecht worden gevoegd.

Voorts kan het Comité I slechts de aanbevelingen herhalen die het had geformuleerd bij het afsluiten van zijn onderzoek « naar de manier waarop de Belgische inlichtingendiensten reageren op het mogelijk bestaan van een netwerk, « Echelon » genaamd, voor het intercepteren van communicatie ». De bovenstaande feitelijke vaststellingen illustreren de relevantie van die aanbevelingen voldoende.

Ter herinnering, de aanbevelingen van het Comité I :

— ervan uitgaan dat het mogelijk bestaan van systemen voor het intercepteren van communicatie, ontwikkeld door vreemde landen met bedoelingen die strijdig zijn met de wettige belangen van België (in het bijzonder de bescherming van het wetenschappelijk en economisch potentieel), heel waarschijnlijk is, ook al bestaan daar nog geen bewijzen van;

— bijgevolg aan de Belgische inlichtingendiensten de opdracht geven samen te werken met het oog op

Le Comité R regrette également qu'aucune suite n'ait été donnée aux demandes d'aide et propositions de collaboration entre le milieu scientifique et la Sûreté de l'État.

Aucun service ne dispose en effet des compétences nécessaires pour assurer la sécurisation des systèmes informatiques des centres de recherche.

Le Comité R regrette enfin que l'intéressant travail de recueil de renseignements par la Sûreté de l'État n'ait trouvé aucun débouché vers une quelconque autorité judiciaire, politique ou administrative compétente dans les matières traitées.

Dans cette affaire, il n'a été fait aucune application des articles 19 et 20 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité, réglant la communication des informations d'une part, et la collaboration entre services d'autre part.

5. Recommandations

La conclusion d'un accord spécifique entre les autorités judiciaires et les services de renseignement, dans le cadre de l'article 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, devrait notamment viser à faciliter les échanges d'informations sur l'espionnage militaire, économique et scientifique entre ces autorités.

Dans un tel cadre, le Comité R se demande s'il ne faudrait pas réfléchir également à l'élaboration d'une notice spécifique relative à l'espionnage économique, scientifique et industriel. Celle-ci s'ajouterait aux notices classiques du droit pénal commun.

Par ailleurs, le Comité R ne peut que réitérer les recommandations qu'il a formulées à l'issue de son enquête menée « sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau « Echelon » d'interception des communications » et dont les constatations matérielles qui précèdent illustrent parfaitement la pertinence.

Pour mémoire, le Comité R a recommandé :

— 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

het verzamelen van alle beschikbare informatie (uit open bronnen en andere) ter zake;

— aan de inlichtingendiensten de vereiste technische en personele middelen toekennen om deze opdracht uit te voeren (in het bijzonder door hun de mogelijkheid te bieden een beroep te doen op externe experts zoals informatici, ingenieurs in telecommunicatie, specialisten inzake cryptografie, analisten, enz.);

— het algemeen principe van voorzorg hanteren bij het uitwerken van een globaal en gecentraliseerd beleid inzake veiligheid van de informatie;

— onderzoeken of een dienst kan worden opgericht, belast met het ontwikkelen van een oplossing voor de hele problematiek van het beveiligen van de informatie.

6. Voortzetting

Het huidig verslag, dat werd goedgekeurd op 13 maart 2001, werd, overeenkomstig artikel 37 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, op 16 maart 2001 toegezonden aan de bevoegde ministers (minister van Justitie en minister van Landsverdediging) teneinde hun advies in te winnen wat de publicatie betreft.

Op 11 april 2001 heeft de minister van Justitie schriftelijk zijn advies meegedeeld aan het Comité I. De minister verklaart dat hij zich aansluit bij het standpunt, uitgebracht door de administrateur-generaal van de Veiligheid van de Staat zoals weergegeven in een nota van 5 april 2001. In deze nota bevestigt de administrateur-generaal dat de Veiligheid van de Staat nog geen directieven heeft ontvangen van het Ministerieel Comité voor inlichting en veiligheid met betrekking tot de invulling van haar taak tot vrijwaring van het wetenschappelijk en economisch potentieel. Het ontwerp van definitie dat de Veiligheid van de Staat had ontwikkeld, na overleg met het kabinet van de minister van Economische Zaken en het kabinet van de minister van Telecommunicatie, wordt nog besproken binnen het College voor inlichting en veiligheid.

In een brief van 28 maart 2001 gericht aan het hoofd van de Dienst enquêtes van het Comité I, laat de Veiligheid van de Staat weten dat zij «in het kader van prospectie op 26 september 2000 is ingegaan op een uitnodiging van de universiteit van (x), met het oog op een sensibilisering van haar nieuwe opdracht.» Naar aanleiding van dit gesprek zouden er op het niveau van het onderzoekscentrum, vermeld in dit verslag, de nodige maatregelen getroffen worden, meer bepaald werd er een werkgroep samengesteld die de veiligheidsproblematiek in kaart moet brengen. Op basis van haar specifieke expertise verklaart de Veiligheid van de Staat zich bereid om met de verantwoordelijken samen te werken om hun aandacht

de recueillir toute information disponible (de source ouverte et autres) sur la question;

— de donner aux services de renseignement les moyens techniques et humains nécessaires pour 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.

6. Prolongements

Le présent rapport, approuvé le 13 mars 2001, a été adressé aux ministres compétents (ministre de la Justice et ministre de la Défense nationale) le 16 mars 2001 afin de recueillir leurs avis préalables en vue de sa publication, ceci conformément à l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le ministre de la Justice a communiqué son avis au Comité permanent R par lettre du 11 avril 2001. Celui-ci déclare se rallier au point de vue exprimé par l'administrateur général de la Sûreté de l'État dans une note du 5 avril 2001. Dans cette note, l'administrateur général confirme que la Sûreté de l'État n'a pas encore reçu de directive de la part du comité ministériel du renseignement et de la sécurité concernant la manière d'exécuter sa mission de protection du potentiel scientifique et économique. Le projet de définition de cette notion que la Sûreté de l'État a élaboré après concertation avec le cabinet du ministre des Affaires économiques et celui du ministre des télécommunications, fait encore l'objet de discussions au sein du collège du renseignement et de la sécurité.

Dans une lettre adressée le 28 mars 2001 au chef du Service d'enquêtes du Comité R, la Sûreté de l'État a fait savoir qu'elle avait «réagi par une démarche de prospection le 26 septembre 2000, à l'invitation de l'Université de (x), en vue d'une sensibilisation à (sa) nouvelle mission». À la suite de cette rencontre, les mesures nécessaires auraient été prises au niveau du centre de recherche cité dans la présente enquête, notamment en constituant un groupe de travail chargé d'examiner les mesures de sécurité à prendre. Sur base de son expérience spécifique, la Sûreté de l'État se déclare disposée à collaborer avec les responsables pour attirer leur attention sur des problèmes ponctuels de sécurité en ne pouvant toutefois pas se

te vestigen op punctuele veiligheidsproblemen, maar de dienst kan echter niet garant staan voor de uitvoering van de beveiligings-maatregelen, noch op het vlak van informatiesystemen noch qua infrastructuur en personeel.

De Veiligheid van de Staat beschouwt het inwinnen, verzamelen, verwerken en analyseren van veiligheidsinlichtingen als haar wettelijke taak en niet het garanderen van de veiligheid van informatiesystemen. Zij kan niet de kostbare middelen en personeel ter beschikking stellen voor het vervullen van dergelijke opdracht, die eerder een bevoegdheid is van de federale regering. Deze dienst verklaart trouwens dat de externe expertise wordt toevertrouwd aan het project FEDICT, dat ernaar streeft een organisme op te richten, belast met de veiligheid van de informatiesystemen.

Volgens de Veiligheid van de Staat moet nogmaals duidelijk gesteld worden dat, behoudens taken inzake prospectie en taken in het kader van haar traditionele opdrachten, zij de initiatieven op het vlak van inlichtingen steeds met veel voorzichtigheid moet uitvoeren, in afwachting van de nodige richtlijnen van het Ministerieel Comité voor Inlichting en Veiligheid.

Op 25 april 2001 heeft het Vast Comité I een brief ontvangen van de minister van Landsverdediging met zijn opmerkingen. Hij dringt erop aan dat er geen verwarring zou gemaakt worden tussen twee afzonderlijke opdrachten van de ADIV.

Enerzijds, de wettelijke opdracht hernomen in de organieke wet van de inlichtingendiensten, in het bijzonder de bescherming van het geheim van de informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert en anderzijds, de controle bij de officieel erkende firma's die werken in het belang van Landsverdediging en waar geclassificeerde informatie wordt bewaard en verwerkt, opdracht die voortvloeit uit de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen. Wat betreft het centrum is het vooral in het kader van de tweede opdracht dat de ADIV is tussengekomen, de bescherming van het wetenschappelijk en economisch potentieel is een wettelijke opdracht van de Veiligheid van de Staat, voorzien in de organieke wet.

Het Vast Comité I blijft ervan overtuigd dat de bovenstaande besluiten en verderzettingen nog steeds vragen doen oproepen over de wijze waarop de Veiligheid van de Staat en de ADIV het besproken probleem hebben behandeld; het Comité I blijft bijgevolg bij zijn beslissing om het onderzoek ter zake verder te zetten.

porter garante de l'exécution des mesures prises par ceux-ci, tant sur le plan des systèmes d'information que de l'infrastructure et du personnel.

La Sûreté de l'État considère également que sa mission légale est de recueillir, de traiter et d'analyser le renseignement de sécurité, mais non d'assurer elle-même la sécurité des systèmes d'informations. Elle ne peut donc s'engager à acquérir elle-même les compétences humaines et techniques nécessaires à remplir une telle mission qui relève plutôt des compétences du gouvernement fédéral. Ce service déclare d'ailleurs qu'il offre son expertise extérieure au projet FEDICT qui tend à la mise sur pied d'un organe chargé de la sécurité des systèmes d'information.

Pour la Sûreté de l'État, il est donc clair qu'en cette matière, les tâches de prospection et celles en rapport avec ses missions traditionnelles mises à part, elle ne peut encore s'engager dans la voie du recueil de renseignements qu'avec prudence, et ce, aussi longtemps qu'elle n'aura pas reçu les directives nécessaires du comité ministériel du renseignement et de la sécurité.

Par courrier du 25 avril 2001, le ministre de la Défense nationale a fait part au Comité R de ses observations. Il a insisté pour qu'une confusion ne soit pas faite entre deux missions distinctes du SGR.

D'un côté, la mission légale reprise dans la loi organique des services de renseignements, en particulier la protection du secret des systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense gère et de l'autre côté le contrôle dans les firmes agréées travaillant au profit de la Défense dans lesquelles des informations classifiées sont détenues ou traitées, mission issue de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité. En ce qui concerne le Centre de recherche concerné c'est surtout dans le cadre de la seconde mission que le SGR est intervenu, la protection du potentiel scientifique ou économique étant une mission légale de la Sûreté de l'État prévue dans la loi organique.

Le Comité R reste persuadé que les conclusions et prolongements qui précèdent suscitent toujours des interrogations sur la manière dont la Sûreté de l'État et le SGR ont traité le problème ici abordé; il maintient par conséquent sa décision de poursuivre son enquête sur le sujet.

B. Onderzoeken op initiatief van het Comité I

HOOFDSTUK 1

VERSLAG BETREFFENDE HET ONDERZOEK NAAR DE WERKING VAN DE SECTIE « WAPENWETGEVING » VAN DE VEILIGHEID VAN DE STAAT

1. Inleiding

In 1998 voerde het Comité I een onderzoek naar de bevoegdheden van de dienst Wapenwetgeving van de Veiligheid van de Staat, teneinde na te gaan of deze materie wel degelijk tot de bevoegdheid behoorde van deze inlichtingendienst (1).

We herinneren eraan dat de Veiligheid van de Staat bevoegd is om de hierna genoemde vergunningen uit te reiken aan vreemdelingen zonder woonplaats in België, alsook aan Belgen die in het buitenland wonen :

— vergunningen tot het voorhanden hebben van een verweer- of oorlogsvuurwapen;

— vergunningen tot het dragen van een verweerwapen;

— tijdelijke vergunningen tot het voorhanden hebben van een verweer- of oorlogswapen;

— tijdelijke vergunningen tot het dragen van een verweerwapen (Europese vuurwapen-kaarten).

Naast de hierboven beschreven beslissingsbevoegdheid inzake wapens, brengt de Veiligheid van de Staat ook adviezen uit ten behoeve van andere instanties die belast zijn met de toepassing van de wapenwetgeving, namelijk de provinciegouverneurs, de gemeentelijke politiekorpsen en de Vreemdelingendienst.

Deze adviezen hebben in hoofdzaak betrekking op :

— vergunningen tot het dragen van een wapen voor het personeel van diplomatieke vertegenwoordigingen die niet zijn vrijgesteld van inschrijving in de gemeenteregisters;

— de erkenningen van wapenmakers (artikel 27 van de wet van 3 januari 1933 op de vervaardiging van, de handel in en het dragen van wapens, en op de handel in de munitie);

— vergunningen tot het dragen van een wapen voor de leden van bewakingsdiensten;

— genaturaliseerde Belgen van wie de activiteiten de Veiligheid van de Staat aanbelangen;

— aanvragen ingediend door vreemdelingen die in België wonen.

(1) Vast Comité I, jaarverslag 1998, blz. 113.

B. Enquêtes à l'initiative du Comité R

CHAPITRE 1er

RAPPORT RELATIF À L'ENQUÊTE SUR LE FONCTIONNEMENT DE LA SECTION « LÉGISLATION » EN MATIÈRE D'ARMES DE LA SURÊTÉ DE L'ÉTAT

1. Introduction

En 1998, le Comité R a mené une enquête relative aux compétences du service « législation en matière d'armes » de la Sûreté de l'État afin d'apprécier si cette matière devait bien relever de ce service de renseignement (1).

Pour rappel, la Sûreté de l'État est compétente pour délivrer les permis suivants aux étrangers sans résidence en Belgique, ainsi qu'aux Belges résidant à l'étranger :

— les autorisations de détention d'une arme à feu de défense ou de guerre;

— les permis de port d'arme de défense;

— les autorisations temporaires de détention d'une arme de défense ou de guerre;

— les permis temporaires de port d'arme de défense (cartes européennes d'armes à feu).

Outre ses compétences décisionnelles précitées en matière d'armes, la Sûreté de l'État rend des avis à l'intention d'autres instances chargées de l'application de la législation sur les armes, à savoir, les gouverneurs de province, les polices communales et l'Office des étrangers.

Ces avis concernent essentiellement :

— les permis de port d'arme pour les membres du personnel des représentations diplomatiques qui ne bénéficient pas de l'exonération d'inscription dans les registres communaux;

— les agréments d'armuriers (article 27 de la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions);

— les permis de port d'arme pour les membres des services de gardiennage;

— les Belges naturalisés dont les activités concernent la Sûreté de l'État;

— les demandes introduites par des étrangers résidant en Belgique.

(1) Comité R, rapport d'activités 1998, p. 103.

In de besluiten van zijn verslag had het Comité I de volgende aanbevelingen geformuleerd:

— aan de Veiligheid van de Staat elke beslissingsbevoegdheid te ontnemen die zij bezit op het gebied van de uitvoering van de wapenwetgeving;

— integendeel, aan deze dienst een algemene adviesbevoegdheid te verlenen, voorafgaand aan het uitreiken of intrekken van eender welke vergunning tot het voorhanden hebben van een verweer- en oorlogsvuurwapen, alsook van elke vergunning tot het dragen van verweerwapens, en dit ongeacht de woonplaats van de aanvrager (in België of in het buitenland).

In 1999 besliste het Comité I zijn onderzoek naar deze materie voort te zetten:

— enerzijds, door de werking van de dienst «wapenwetgeving» van de Veiligheid van de Staat aan een grondiger onderzoek te onderwerpen;

— anderzijds, door het kwantitatief belang van de uitoefening van deze opdracht te beoordelen.

2. Procédure

Krachtens een kantschrift van 13 juli 1999 heeft de voorzitter van het Comité I de Dienst Enquêtes belast bepaalde verificaties te doen met betrekking tot het jaar 1998 en de eerste zes maanden van het jaar 1999.

Overeenkomstig artikel 43, 1º, van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten heeft het hoofd van de Dienst Enquêtes de minister van Justitie bij brief van 27 juli 1999 kennis gegeven van de opening en van het voorwerp van het onderzoek.

Op 16 november 1999 heeft de Dienst Enquêtes zijn rapport aan het Vast Comité bezorgd.

Op 1 september 2000 stuurde het Comité I opnieuw een kantschrift naar de Dienst Enquêtes, met het verzoek enkele bijkomende controles te verrichten.

De Dienst Enquêtes heeft zijn aanvullend verslag op 24 oktober 2000 aan het Comité I bezorgd.

Op 29 december 2000 heeft het Comité I aanvullende informatie aan de Veiligheid van de Staat gevraagd. De Veiligheid van de Staat antwoordde op 6 februari 2001.

Het onderhavige verslag werd goedgekeurd op 15 februari 2001.

Op 6 april 2001 heeft het Comité I de opmerkingen ontvangen van de minister van Justitie. Deze opmerkingen, weergegeven in een nota geclassificeerd «Vertrouwelijk — wet van 11 december 1998», konden slechts meegedeeld worden aan de parlementaire begeleidingscommissies P en I na een declassificatie vanwege de Veiligheid van de Staat. Dit docu-

Dans les conclusions de son rapport, le Comité R avait recommandé:

— de retirer à la Sûreté de l'État toutes les compétences décisionnelles qu'elle détient en matière d'exécution de la législation sur les armes à feu;

— d'attribuer par contre à ce service une compétence d'avis générale et préalable à la délivrance ou au retrait de toute autorisation de détention d'une arme à feu de défense et de guerre ainsi que de tout permis de port d'arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

En 1999, le Comité R a décidé de poursuivre sa réflexion sur le sujet:

— en examinant de plus près le fonctionnement du service «législation en matière d'armes» de la Sûreté de l'État d'une part;

— en évaluant l'importance quantitative de l'exercice de cette mission d'autre part.

2. Procédure

Par apostille du 13 juillet 1999, le président du Comité R a dès lors chargé le Service d'enquêtes de procéder à certaines vérifications qui couvrent l'année 1998 et les six premiers mois de l'année 1999.

Par courrier du 27 juillet 1999, conformément à l'article 43, 1º, de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements, le ministre de la Justice a été averti de l'ouverture et de l'objet de l'enquête par les soins du chef du Service d'enquêtes.

Le Service d'enquêtes a remis son rapport au Comité R le 16 novembre 1999.

Le Comité R a adressé une nouvelle apostille au Service d'enquêtes le 1er septembre 2000 lui demandant de procéder à quelques vérifications complémentaires.

Le Service d'enquêtes a remis son rapport complémentaire au Comité R le 24 octobre 2000.

Le Comité R a demandé un complément d'information à la Sûreté de l'État le 29 décembre 2000. La Sûreté de l'État a communiqué sa réponse le 6 février 2001.

Le présent rapport a été approuvé le 15 février 2001.

Par courrier du 6 avril 2001, le ministre de la Justice a fait valoir ses observations. Celles-ci contenues dans une note classifiée «Confidentiel — loi du 11 décembre 1998» ont pu être transmises aux commissions de suivi P et R après avoir fait l'objet d'une déclassification de la part de la Sûreté de l'État. Ce document porte cependant la mention «Diffusion res-

ment draagt echter de vermelding «beperkte verspreiding»(1) en mag niet in *extenso* hernomen worden in het huidig verslag.

3. Vaststellingen

3.1. Analyse en verspreiding van de informatie door de Veiligheid van de Staat

3.1.1. De studiedienst «Wapenwetgeving»

Binnen de administratieve diensten van de Veiligheid van de Staat bestaat er een studiedienst Wapenwetgeving, die belast is met de toepassing van de wapenwetgeving.

Sinds 1997 is de dienst Wapenwetgeving ook belast met het onderzoeken van alle vormen van proliferatie die kunnen bijdragen tot de toepassing of de ontwikkeling van niet-conventionele of zeer geavanceerde wapensystemen; deze bevoegdheid strekt zich uit tot de vormen en de structuren van de georganiseerde misdaad die wezenlijk betrekking hebben op de proliferatie.

Deze nieuwe bevoegdheden vloeien voort uit de artikelen 7 en 8, *d)* en *f)*, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. De dienst «proliferatie en wapens» moet alle nuttige informatie bezorgen aan de diensten bevoegd voor de andere materies die de Veiligheid van de Staat behandelt. Ook het toesturen van nuttige informatie in omgekeerde richting moet worden verzekerd.

Aan het hoofd van de dienst Wapenwetgeving staat een statutair adjunct-adviseur (derde graad van niveau 1).

Op 1 december 2000 telde deze dienst zeven personen. Het hoofd van de dienst Wapenwetgeving vertegenwoordigt de Veiligheid van de Staat op de vergaderingen van het Interdepartementaal Coördinatiecomité ter bestrijding van illegale wapentransfers (ICIW).

3.1.2. Het Interdepartementaal Coördinatiecomité ter bestrijding van illegale wapentransfers (ICIW)

Dit comité werd opgericht bij koninklijk besluit van 9 februari 1999. Het heeft als opdracht «te komen

(1) Gezien bepaalde informaties, beperkt deze vermelding de verspreiding tot de personen die bevoegd zijn om er kennis van te nemen zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet (artikel 20 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen).

treinte»(1) et ne peut être reproduit in *extenso* dans le présent rapport.

3. Constatations

3.1. L'analyse et la diffusion de l'information par la Sûreté de l'État

3.1.1. Le service d'étude «législation armes»

Il existe au sein des services administratifs de la Sûreté de l'État, un service d'étude chargé de l'application de la législation en matière d'armes.

Depuis 1997, le service «législation armes» est également chargé d'examiner toutes les formes de prolifération qui peuvent contribuer à l'application ou au développement de systèmes d'armement non conventionnels ou très avancés; cette compétence s'étend aux formes et structures du crime organisé qui se rapportent intrinsèquement à la prolifération.

L'introduction de ces nouvelles compétences résulte des articles 7 et 8, *d)* et *f)*, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le service prolifération et armes est tenu de transmettre toutes les informations utiles aux services compétents pour les autres matières traitées par la Sûreté de l'État. La transmission inverse d'informations utiles doit également être assurée.

Le service «législation armes» est placé sous la direction d'un conseiller adjoint statutaire (troisième grade du niveau 1).

Au 1er décembre 2000, ce service comptait sept personnes. Le responsable du service «législation armes» représente la Sûreté de l'État aux réunions du Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes.

3.1.2. Le Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes (CITI)

Ce comité a été créé par un arrêté royal du 9 février 1999. Il a pour mission d'optimaliser la coordination

(1) Eu égard à certaines informations, cette mention limite la diffusion aux personnes qualifiées pour en connaître sans attacher à cette limitation les effets juridiques prévus par la loi (article 20 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité).

tot een betere coördinatie en informatie-uitwisseling in de strijd tegen illegale wapentransfers zodat alle diensten die bij de wapenhandel betrokken zijn de hen toegekende bevoegdheden beter kunnen uitoefenen(1)».

Het ICIW is samengesteld uit een nationaal magistraat en vertegenwoordigers van het ministerie van Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, het ministerie van Justitie, het ministerie van Economische Zaken, het ministerie van Binnenlandse Zaken, het ministerie van Financiën, het ministerie van Landsverdediging (de ADIV), de rijkswacht en de Proefbank voor vuurwapens.

De Veiligheid van de Staat heeft de opdracht gekregen, in samenwerking met de ADIV en de rijkswacht, een vragenlijst op te stellen teneinde zicht te krijgen op de respectievelijke bevoegdheden van elk lid van het ICIW inzake wapens, alsook op de behoeften aan informatie van de leden. Op basis van de antwoorden op deze vragenlijst zal het ICIW een ontwerp van protocolakkoord opmaken betreffende de uitwisseling van informatie tussen de leden.

Onderling maken de leden van het ICIW een onderscheid tussen de «overheden» enerzijds, en de «diensten» anderzijds.

— Met «overheden» wordt bedoeld: de leden van het ICIW die, op grond van de informatie waarover ze beschikken of die hun wordt verstrekt, beslissingen moeten nemen, deze beslissingen moeten toepassen en controleren, en die een administratief of gerechtelijk beleid moeten voeren.

— Met «diensten» wordt bedoeld: de verstrekkers van informatie (onder andere de politiediensten) en de uitvoerders (onder andere de controlediensten), die als opdracht hebben de beslissingen van de «overheden» voor te bereiden en op passende wijze uit te voeren. Tengevolge van haar bevoegdheid wordt de Veiligheid van de Staat als een «dienst» beschouwd.

In afwachting dat een protocolakkoord over het uitwisselen van informatie wordt gesloten, kan het ICIW reeds een belangrijke rol vervullen op het vlak van coördinatie. In de praktijk ontstaat de samenwerking tussen de Veiligheid van de Staat en de andere diensten in functie van concrete gevallen.

3.1.3. De Interdepartementale vergaderingen inzake proliferatie

Sinds 1999 neemt de Veiligheid van de Staat eveneens deel aan de interdepartementale vergaderingen (Buitenlandse Zaken, Financiën, Economische

(1) Artikel 3 van het koninklijk besluit van 9 februari 1999 tot oprichting van het Interdepartementaal Coördinatiecomité ter bestrijding van illegale wapentransfers.

et l'échange d'informations en matière de lutte contre les transferts illégaux d'armements, afin de permettre à tous les services concernés par le commerce des armes de mieux exercer les compétences qui leur ont été attribuées(1).

Le CITI réunit le magistrat national et des représentants des ministères des Affaires étrangères, du Commerce extérieur et de la Coopération au Développement, de la Justice, des Affaires économiques, de l'Intérieur, des Finances, de la Défense nationale (le SGR), de la gendarmerie et du Banc d'épreuves des armes à feu.

La Sûreté de l'État a été chargée, en collaboration avec le SGR et la gendarmerie d'élaborer un questionnaire destiné à connaître les compétences respectives de chacun des membres du CITI en matière d'armes, et d'identifier leurs besoins en informations. Selon les réponses apportées à ce questionnaire, le CITI élaborera un projet de protocole d'accord sur l'échange d'informations entre les membres.

Les membres du CITI distinguent parmi eux les «autorités» d'une part, les «services» d'autre part.

— Par «autorités» il faut entendre les membres du CITI qui, sur base de l'information dont ils disposent ou qui leur est fournie, doivent prendre des décisions, les faire appliquer et contrôler et qui doivent mener une politique administrative ou judiciaire.

— Par «services», on entend les fournisseurs d'information (entre autres les services de police) et les exécutants (entre autres les services de contrôle) qui ont pour mission de préparer et d'exécuter de manière adéquate les décisions prises par les «autorités». De par sa compétence, la Sûreté de l'État est considérée comme un «service».

En attendant la conclusion d'un protocole d'accord sur l'échange d'information, le CITI peut déjà jouer un rôle important de coordination. Dans la pratique, la collaboration entre la Sûreté de l'État et les autres services se construit en fonction de cas concrets.

3.1.3. Les réunions interdépartementales sur la prolifération

Depuis 1999, la Sûreté de l'État participe également à des réunions interdépartementales (Affaires étrangères, Finances, Affaires économiques, Justice,

(1) Article 3 de l'arrêté royal du 9 février 1999 instituant le Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes.

Zaken, Justitie, Landsverdediging, de strijdkrachten en de Koninklijke Militaire School), die tot doel hebben erop toe te zien dat de uitvoer van materieel en uitrustingen niet bijdraagt tot de verspreiding van chemische of biologische wapens.

Binnen dit kader heeft de Veiligheid van de Staat informatie verstrekt over de belangstelling die terroristische groeperingen betonen voor het vervaardigen van niet-conventionele wapens.

3.2. Toekennen van vergunningen tot het voorhanden hebben en het dragen van een wapen (verweer- of oorlogswapens)

Tussen 1 januari 1998 en 31 december 2000 heeft de dienst wapenwetgeving 5 003 vergunningen uitgereikt aan vreemdelingen en aan enkele Belgen zonder woonplaats in België.

	Vergunning tot het voorhanden hebben en dragen van wapens	Tijdelijke vergunningen (Europese vuurwapenskaarten)	Totaal
1998 .	1 175	210	1 385
1999 .	1 625	256	1 881
2000 .	1 481	256	1 737
Totaal .	4 281	722	5 003

De vreemdelingen die een vergunning kregen, zijn in hoofdzaak gendarmes en beschermingsagenten die belangrijke buitenlanders naar België vergezellen, maar ook gewone burgers, militairen die op de SHAPE werken, diplomaten van buitenlandse ambassades op post in België, politieambtenaren op doorreis in België, sportschutters die deelnemen aan competities georganiseerd door erkende Belgische schuttersverenigingen.

Binnen dit kader behandelt de Veiligheid van de Staat de Europese vuurwapenpassen met het oog op hun regularisatie.

Zelfverdediging, de sport en de jacht zijn de redenen die worden genoemd bij het indienen van een aanvraag. In uitzonderlijke gevallen werden tijdelijke vergunningen geweigerd aan beschermingsagenten die belangrijke buitenlanders vergezelden, alsook aan sportschutters. Dit gebeurde omdat de aanvragen onvolledig waren of te laat werden ingediend.

De Veiligheid van de Staat heeft geen aanvragen ontvangen van Belgen die in het buitenland wonen en wapens wilden uitvoeren naar een land dat het voorwerp is van een embargo.

Een dienstnota van 16 maart 1992 beschrijft de *modus operandi* toepasbaar op de aanvragen die buitenlanders indienen om een vergunning tot het voor-

Défense nationale, Forces armées et École royale militaire) chargées de veiller à ce que les exportations de matériels et d'équipements ne contribuent pas à la dissémination d'armes chimiques ou biologiques.

Dans ce cadre, la Sûreté de l'État a produit des informations relatives à l'intérêt porté par des groupes terroristes à la confection d'armes non-conventionnelles.

3.2. L'octroi des autorisations de détention et de port d'arme (armes de défense ou armes de guerre)

Pendant la période du 1er janvier 1998 au 31 décembre 2000, 5 003 autorisations ont été délivrées par le service « législation armes » à des étrangers et à quelques citoyens belges sans résidence en Belgique. Ce chiffre se répartit comme suit :

	Autorisations de détention et permis de port d'armes	Autorisations temporaires (cartes européennes d'armes à feu)	Totaux
1998 .	1 175	210	1 385
1999 .	1 625	256	1 881
2000 .	1 481	256	1 737
Totaux .	4 281	722	5 003

Les étrangers bénéficiaires sont principalement des gendarmes et des agents de protection qui accompagnent des personnalités étrangères en Belgique, mais aussi des citoyens ordinaires, des militaires employés au SHAPE, des diplomates d'ambassades étrangères en poste en Belgique, des policiers en transit en Belgique, des tireurs sportifs participant à des compétitions de tir organisées par des associations de tireurs belges reconnues.

C'est dans ce cadre que la Sûreté de l'État traite et régularise les cartes européennes d'armes à feu.

Les motifs invoqués lors de la requête relèvent de l'auto-défense, du sport et de la chasse. Dans des cas exceptionnels, des autorisations temporaires ont été refusées à des agents de protection qui accompagnaient des personnalités étrangères ainsi qu'à des tireurs sportifs. Les raisons étaient que ces demandes étaient incomplètes ou avaient été introduites tardivement.

Il n'y pas eu de demande adressée à la Sûreté de l'État émanant de citoyens belges résidant à l'étranger en vue d'exporter des armes vers des pays soumis à un embargo.

Une note de service du 16 mars 1992 indique le *modus operandi* applicable aux demandes introduites par des étrangers pour obtenir une autorisation de

handen hebben (van verweer- of oorlogswapens) of het dragen van een wapen te verkrijgen.

De Veiligheid van de Staat onderzoekt niet alleen de redenen van de aanvragen maar ook, indien het gaat om personen die niet in België wonen, of zij voldoen aan de wetgeving van het land waar ze verblijven.

De richtlijn (91/477/EEG) van de Raad van de Europese Gemeenschappen d.d. 18 juni 1991 inzake de controle op de verwerving en het voorhanden hebben van wapens, alsook het Akkoord van Schengen (artikel 91) voorzien respectievelijk een systeem van dubbele vergunning en een uitwisseling van inlichtingen over het verwerven van een vuurwapen door een ingezetene van een andere lidstaat.

Intern controleert de Veiligheid van de Staat het strafblad van de buitenlandse aanvrager en gaat ze na of de betrokkene voorkomt in haar bestanden. Het komt erop aan rekening te houden met de persoonlijkheid van de aanvrager, in het bijzonder met een mogelijke gewelddadige politieke activiteit. Is dit het geval, dan voert de Veiligheid van de Staat een diepgaander onderzoek.

In een nota van 14 mei 1986 aan de toenmalige administrateur-directeur-generaal meende de kabinetschef van de minister van Justitie echter dat «alleen het feit te weten of de betrokkene al dan niet bij uw diensten gekend is geen voldoende waarborgen» bood; bijgevolg gebood hij dat voortaan een onderzoek in het buitenland moest worden gevoerd.

Met betrekking tot particulieren die nu en dan naar België komen om te jagen of aan schietcompetities deel te nemen, gaat de Veiligheid van de Staat na of de aanvragers deze activiteiten wel degelijk op een eervolle wijze beoefenen.

Aanvragen met het oog op het verkrijgen van een vergunning tot het voorhanden hebben van een oorlogswapen, worden met heel wat omzichtigheid onderzocht. Niettemin vraagt men aan de aanvrager zelf het bewijs te leveren van de werkelijkheid van de reden die hij noemt ter staving van zijn aanvraag, bijvoorbeeld door het overleggen van zijn lidkaart van een erkende sportclub, een uitnodiging die hij heeft ontvangen van een erkende club in België, enz.

De Veiligheid van de Staat voert geen bijzonder onderzoek voor elk afzonderlijk geval. Ze raadpleegt haar permanente documentatie over schietclubs (statuten gepubliceerd in het *Belgisch Staatsblad*, enz.). In geval van twijfel kan ze aanverwante diensten in het buitenland raadplegen, maar er bestaat geen internationale procedure van wederzijdse raadpleging tussen inlichtingen- en veiligheidsdiensten. In 1998 en 1999 werd geen enkele vraag om inlichtingen verstuurd naar een buitenlandse dienst.

Tot op heden hebben de Veiligheid van de Staat en de SGR niet op specifieke en systematische wijze gege-

détention (d'armes de défense ou d'armes de guerre) ou un permis de port d'arme.

Outre les motifs des demandes, la Sûreté de l'État vérifie, s'agissant de personnes non domiciliées en Belgique, si elles sont en règle au regard de la législation de l'État où elles demeurent.

La directive (91/477 CEE) du Conseil des Communautés européennes du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes, ainsi que l'Accord de Schengen (article 91) prévoient respectivement un système de double autorisation et un échange de renseignements sur l'acquisition d'une arme à feu par un résident d'un autre État membre.

Au niveau interne, la Sûreté de l'État vérifie le casier judiciaire de l'étranger demandeur et examine s'il est connu dans ses fichiers. Il s'agit ici de tenir compte de la personnalité du demandeur et notamment d'une éventuelle activité politique violente. Si tel est le cas, la Sûreté procède alors à une enquête plus approfondie.

Par note du 14 mai 1986 adressée à l'administrateur directeur général de l'époque, le chef de cabinet du ministre de la Justice avait toutefois estimé que «le seul fait de savoir si la personne est connue ou non de vos services (n'offrait) pas les garanties suffisantes»; il prescrivait par conséquent qu'il soit désormais procédé à une enquête à l'étranger.

En ce qui concerne les particuliers qui viennent pratiquer le tir sportif ou la chasse occasionnellement en Belgique, la Sûreté de l'État vérifie si les demandeurs pratiquent vraiment ces disciplines de manière honorable.

Les demandes d'autorisation de détention d'une arme de guerre sont examinées avec beaucoup de circonspection. Cependant, c'est au demandeur lui-même qu'il est demandé de produire la preuve de la réalité du motif qu'il invoque à l'appui de sa demande, par exemple en produisant sa carte d'affiliation à un club sportif reconnu, une invitation reçue d'un club belge reconnu, etc.

La Sûreté de l'État ne procède pas à une enquête particulière pour chaque cas. Elle consulte sa documentation permanente sur les clubs sportifs de tirs (statuts parus au *Moniteur belge*, etc.). En cas de doute elle peut consulter des services correspondants étrangers mais il n'existe pas de procédure internationale de consultation réciproque entre services de renseignement et de sécurité. Aucune demande de renseignement n'a été adressée à un service étranger.

Jusqu'à présent il n'y a pas eu d'échange spécifique et systématique de données entre la Sûreté de l'État et

vens uitgewisseld met betrekking tot het toepassen van de Belgische wetgeving over vuurwapens, zoals ze wordt toegepast door de dienst « wapenwetgeving ».

De vergunning tot het voorhanden hebben en/of dragen van een wapen wordt getekend door ambtenaren van de Veiligheid van de Staat, allen van niveau 1 en aangeduid bij ministerieel besluit.

De wapenvergunning moet samen met het wapen worden gedragen en moet op elk verzoek van de overheden worden overgelegd. De houder moet het Bestuur van de Veiligheid van de Staat verwittigen in geval van verlies of diefstal van het wapen tijdens zijn verblijf in België.

De dienstnota van 16 maart 1992 bevat geen beschrijving van de *modus operandi* toepasbaar in geval van intrekking of schorsing van de vergunning tot het voorhanden hebben en dragen van een wapen.

Tussen 1 januari 1998 en 31 december 2000 werd geen enkele vergunning tot het voorhanden hebben of het dragen van een wapen geschorst of ingetrokken.

De procedures van schorsing en intrekking van vergunningen zijn natuurlijk alleen toepasbaar gedurende het verblijf in België van de houders van de genoemde documenten. Indien het om een kort verblijf gaat, lijkt de toepassing van deze procedures nogal van het toeval af te hangen.

De Veiligheid van de Staat verklaart dat ze, indien ze kennis zou hebben van gewelddadige activiteiten van de houder van een vergunning tot het dragen van een wapen, in de eerste plaats de gerechtelijke overheden zou verwittigen, wier beslissing vervolgens de basis voor de intrekking van de vergunning zou vormen.

3.3. Verzoeken om advies

Tussen 1 januari 1998 en 31 december 2000 ontving de dienst Wapenwetgeving slechts 164 verzoeken om schriftelijk advies (48 in 1998; 75 in 1999 en 41 in 2000) vanwege de provinciegouverneurs, de Dienst Vreemdelingenzaken of de gemeenten.

De Veiligheid van de Staat werd ook een paar keer geraadpleegd met betrekking tot het uitreiken van vergunningen tot het dragen van een wapen voor de leden van bewakingsdiensten, internationale organisaties of diplomatieke vertegenwoordigingen in België, ingevolge de aanbeveling van het Bestuur Strafzaken en Criminele Zaken in 1994.

Rekening houdend met het feit dat er in België gedurende drie jaar ongeveer 48 000 (1) vergunnin-

(1) Volgens de aan het Comité I overhandigde statistieken vanwege de centrale gegevensbank, het Nationaal Wapenregister.

le SGR concernant l'application de la législation belge sur les armes à feu telle qu'elle est appliquée par le service « législation armes ».

L'autorisation de détention et/ou de port d'arme est signée par des fonctionnaires de la Sûreté de l'État, tous de niveau 1 et désignés par arrêté ministériel.

Le permis de port d'arme doit accompagner l'arme autorisée et doit être présenté à toute réquisition des autorités. Son titulaire doit informer l'administration de la Sûreté de l'État en cas de perte ou de vol de l'arme durant son séjour en Belgique.

La note de service du 16 mars 1992 n'indique pas quel est le *modus operandi* applicable aux retraits ou aux suspensions d'autorisation de détention et de port d'arme.

Pendant la période du 1er janvier 1998 au 31 décembre 2000, aucune autorisation de détention, ni aucun permis de port d'arme n'a été suspendu ou retiré.

Les procédures de suspension et de retrait des autorisations ne peuvent bien sûr s'appliquer que pendant les séjours en Belgique des titulaires desdits documents. En cas de court séjour, l'application de ces procédures semble quelque peu aléatoire.

La Sûreté de l'État déclare que si elle avait connaissance d'activités violentes de la part d'un titulaire d'un port d'arme, elle en avertirait en premier lieu les autorités judiciaires dont la décision constituerait alors la base du retrait de l'autorisation.

3.3. Les demandes d'avis

Pour la période du 1er janvier 1998 au 31 décembre 2000, le service armes n'a reçu que 164 demandes d'avis écrits (48 en 1998, 75 en 1999, 41 en 2000) de la part des gouverneurs de provinces, de l'Office des étrangers ou des communes.

La Sûreté de l'État a également été consultée quelquefois en vue de la délivrance des permis de port d'arme pour les membres des services de gardiennage, des organisations internationales ou des représentations diplomatiques en Belgique, ainsi que l'a recommandé l'Administration des affaires criminelles et pénales en 1994.

Sachant qu'au cours de la même période, on a délivré en Belgique près de 48 000 autorisations de déten-

(1) Selon les statistiques fournies au Comité R par la direction de la banque de données nationale — registre central des armes.

gen tot het dragen van een wapen worden uitgereikt, wordt de Veiligheid van de Staat bijgevolg slechts geraadpleegd in minder dan 1% van de gevallen, waarin zij zelf niet bevoegd is om zulke vergunningen uit te reiken.

Gewoonlijk controleert de Veiligheid van de Staat of de aanvrager voorkomt in haar bestanden. Indien hij bekend staat om een gewelddadige politieke activiteit, brengt de bevoegde directie een met redenen omkleed negatief advies uit.

Met betrekking tot adviezen inzake vreemdelingen zonder woonplaats in België, neemt de Veiligheid van de Staat contact op met haar correspondent in het buitenland. Voor diplomaten worden de toekenningsvoorwaarden geval per geval bepaald.

Wat de wapenmakers betreft, verricht de Veiligheid van de Staat een snel onderzoek naar hun activiteiten. Ze raadpleegt haar algemene documentatie over wapentrafieken. Dit onderzoek verloopt minder grondig dan een veiligheidsonderzoek. Ook de gerechtelijke politie voert een onderzoek. Beide onderzoeken overlappen elkaar soms.

3.4. Informatie verstrekt aan de Veiligheid van de Staat door de provinciegouverneurs en de gemeentepolitie

Tijdens de beoogde periode kreeg de Veiligheid van de Staat geen kennis van de provinciegouverneurs over hun beslissingen inzake de aanvragen van een vergunning tot het dragen van een wapen voor het personeel van diplomatieke zendingen of gelijkwaardig personeel, hoewel de gouverneurs daartoe verplicht zijn krachtens de gecoördineerde omzendbrief van 30 oktober 1995 betreffende de toepassing van de wettelijke en reglementaire bepalingen inzake wapens (2).

Ook de gemeentepolitie moet aan de Veiligheid van de Staat, binnen de acht dagen, een kopie bezorgen van de vergunning tot het voorhanden hebben van een verweerwapen die wordt uitgereikt aan een lid van een diplomatieke vertegenwoordiging dat niet is vrijgesteld van inschrijving in het gemeenteregister of aan een genaturaliseerde Belg wiens activiteiten de Veiligheid van de Staat aanbelangen.

Tijdens de vermelde periode werd de Veiligheid van de Staat slechts één keer door een gemeentelijk politiekorps op de hoogte gebracht van het uitreiken van een vergunning aan een lid van een diplomatieke zending dat niet was vrijgesteld van inschrijving in het gemeenteregister.

(1) Volgens de aan het Comité I overhandigde statistieken vanwege de centrale gegevensbank, het Nationaal Wapenregister.

(2) *Belgisch Staatsblad* d.d. 28 november 1995 en 29 februari 1996.

tion d'arme à feu et permis de port d'arme (1), on constate que la Sûreté de l'État n'a été consultée que dans moins d'un pour cent des cas où elle-même n'est pas compétente pour délivrer ces autorisations de détention ou de port d'arme.

Lorsqu'elle est consultée, la Sûreté de l'État vérifie si le demandeur est connu dans ses fichiers. S'il est connu pour une activité politique violente, la direction compétente émet un avis négatif motivé.

Pour les avis à l'égard des étrangers non domiciliés en Belgique, la Sûreté de l'État consulte son correspondant étranger. En ce qui concerne les diplomates, les modalités d'octroi sont déterminées cas par cas.

En ce qui concerne les armuriers, la Sûreté de l'État procède à une enquête rapide sur les activités des intéressés. Elle consulte sa documentation générale relative aux trafics d'armes. Cette enquête n'est pas aussi approfondie qu'une enquête de sécurité. La police judiciaire procède aussi à une enquête. Ces deux enquêtes font parfois double emploi.

3.4. L'information de la Sûreté de l'État par les gouverneurs de province et par les polices communales

Au cours de la période visée, la Sûreté de l'État n'a pas été avisée par les gouverneurs de province de leurs décisions relatives aux demandes de permis de port d'arme pour le personnel des missions diplomatiques ou équivalent alors qu'ils sont requis de le faire par la circulaire coordonnée du 30 octobre 1995 relative à l'application des dispositions légales et réglementaires dans le domaine des armes (2).

De même, les polices communales doivent transmettre à la Sûreté de l'État, dans les huit jours, une copie de l'autorisation de détention d'une arme de défense délivrée à un membre d'une représentation diplomatique non exonéré d'inscription dans le registre communal ou à un belge naturalisé dont les activités concernent la Sûreté de l'État.

Au cours de la période visée, la Sûreté de l'État n'a été avertie qu'une seule fois par une police communale de la délivrance d'une autorisation à un membre d'une mission diplomatique non exempté d'inscription au registre communal.

(1) Selon les statistiques fournies au Comité R par la direction de la banque de données nationale — registre central des armes.

(2) *Moniteur belge* des 28 novembre 1995 et 29 février 1996.

Overigens heeft het Comité I vastgesteld dat het koninklijk besluit van 21 september 1991 de Veiligheid van de Staat opdraagt om haar gegevens over te maken aan het Nationaal Wapenregister, alhoewel dit register enkel beperkt toegankelijk is voor een aantal gerechtelijke-, administratieve- en politiediensten, waartoe de inlichtingendiensten niet behoren.

In de praktijk heeft de Veiligheid van de Staat dus geen enkel zicht op het geheel aan wapenvergunningen in België.

Alhoewel de Veiligheid van de Staat geen elektronische toegang heeft tot het Centraal wapenregister, heeft zij steeds een antwoord ontvangen op haar aanvragen per fax.

3.5. Opvolging van de dossiers

Het Comité I heeft aan de Veiligheid van de Staat gevraagd of en hoe een dossier eventueel werd opgevolgd nadat een vergunning is uitgereikt of nadat advies is verleend (bijvoorbeeld: wanneer nieuwe gegevens aan het licht komen die invloed kunnen hebben op de beslissing of het advies), of nadat de geldigheidstermijn van een vergunning is verstreken.

Het Bestuur van de Veiligheid van de Staat antwoordde dat de aanvraag, eens de vergunning is uitgereikt en het advies verleend, wordt bewaard door de dienst «wapenwetgeving».

Indien deze dienst kennis krijgt van ongunstige informatie betreffende de persoon aan wie een vergunning is uitgereikt of over wie om advies is gevraagd, zou deze dienst daaraan het passende gevolg geven op grond van de vigerende wetgeving.

Het Comité I heeft de toepassing van dit besluit niet kunnen controleren, aangezien de Veiligheid van de Staat verklaart dat ze sinds 1998 geen ongunstige inlichtingen heeft ontvangen betreffende een persoon aan wie een vergunning was uitgereikt.

4. De positie van de Veiligheid van de Staat

Op 2 februari 2000 stuurde de administrateur-generaal van de Veiligheid van de Staat een nota naar de minister van Justitie. Daarin verklaarde zij zich akkoord met de aanbeveling van het Comité I om elke beslissingsbevoegdheid inzake de uitvoering van de wapenwetgeving aan haar dienst te onttrekken.

De administrateur-generaal is er voorstander van dat aan haar dienst een algemene adviesbevoegdheid zou worden verleend, voorafgaand aan het uitreiken of intrekken van eender welke vergunning tot het voorhanden hebben van een verweer- en oorlogsvuurwapen en van elke vergunning tot het dragen van een verweerwapen, ongeacht de woonplaats van de aanvrager (in België of in het buitenland).

Par ailleurs, le Comité R constate que si l'arrêté royal du 21 septembre 1991 oblige la Sûreté de l'État à alimenter le registre central des armes en informations, celui-ci par contre ne reste accessible qu'à un nombre strictement limité d'autorités judiciaires, administratives et de police au nombre desquelles ne figurent pas les services de renseignement.

La Sûreté de l'État ne peut donc, en principe, avoir une vue globale sur l'ensemble des autorisations de ports d'arme délivrées en Belgique.

Il faut cependant savoir que si la Sûreté de l'État ne dispose pas d'un accès par voie électronique au registre central des armes, elle a toujours eu une réponse à ses demandes de renseignements par fax.

3.5. Le suivi des dossiers

Le Comité R a demandé à la Sûreté de l'État quel était le suivi éventuel du dossier une fois l'autorisation accordée ou l'avis donné (par exemple en cas de découverte d'éléments nouveaux susceptibles de modifier la décision ou l'avis), ou après l'expiration du délai d'autorisation.

L'administration de la Sûreté de l'État déclare qu'une fois l'autorisation délivrée et l'avis donné, la demande est conservée par le service «législation armes».

Si des informations défavorables lui parvenaient concernant la personne à laquelle une autorisation a été délivrée ou une personne au sujet de laquelle un avis a été demandé, ce service y donnerait une suite appropriée sur base de la législation en vigueur.

Le Comité R n'a pas été en mesure de vérifier un cas d'application de cette résolution vu que la Sûreté de l'État déclare n'avoir reçu depuis 1998 aucun renseignement défavorable concernant une personne à qui une autorisation a été délivrée.

4. La position de la Sûreté de l'État

Le 2 février 2000, l'administrateur général de la Sûreté de l'État a fait parvenir une note au ministre de la Justice dans laquelle elle se déclare d'accord avec la recommandation du Comité R de retirer à son service toutes les compétences décisionnelles qu'il détient en matière d'exécution de la législation sur les armes à feu.

L'administrateur général plaide aussi pour que soit attribuée à son service une compétence d'avis générale et préalable à la délivrance ou au retrait de toute autorisation de détention d'une arme à feu de défense et de guerre ainsi que de tout permis de port d'arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

In tegenstelling tot het Comité I is de administrateur-generaal niet van mening dat het toekennen van deze algemene adviesbevoegdheid aan de Veiligheid van de Staat een aanpassing vereist van het koninklijk besluit d.d. 20 september 1991 tot uitvoering van de wet van 3 januari 1933 op de vervaardiging van, de handel in en het dragen van wapens, en op de handel in munitie. Volgens haar zou een ministeriële omzendbrief volstaan.

5. Besluiten en aanbevelingen

De studiedienst Wapenwetgeving van de Veiligheid van de Staat oefent de beide bevoegdheden uit die deze dienst heeft inzake de uitvoering van de wapenwetgeving: een beslissingsbevoegdheid en een adviesbevoegdheid met betrekking tot vreemdelingen en Belgen zonder woonplaats in België.

Tussen 1 januari 1998 en 31 december 2000 heeft de dienst Wapenwetgeving 5 003 vergunningen uitgereikt aan vreemdelingen en aan enkele Belgen zonder woonplaats in België, terwijl deze dienst gedurende dezelfde periode slechts 164 schriftelijk verzoeken om advies ontving vanwege de provinciegouverneurs, de Vreemdelingendienst van het ministerie van Binnenlandse Zaken of vanwege de gemeenten.

Rekening houdend met het feit dat er in België gedurende drie jaar ongeveer 48 000 vergunningen tot het dragen van een wapen werden uitgereikt, wordt de Veiligheid van de Staat bijgevolg slechts geraadpleegd in minder dan 1% van de gevallen, waarin zij zelf niet bevoegd is om zulke vergunningen uit te reiken.

Niettemin blijft het Comité I van mening dat de beslissingsbevoegdheid van de Veiligheid van de Staat niet behoort tot de normale activiteiten van een inlichtingendienst. Deze activiteiten bestaan erin de overheid op de hoogte te brengen van zowel interne als externe bedreigingen waarvan België het voorwerp kan zijn. De adviesbevoegdheid van deze dienst past bijgevolg het best in het kader van de hierboven beschreven voorlichtingsopdracht.

Voorts stelt het Comité I vast dat in de praktijk de Veiligheid van de Staat geen enkel zicht heeft op het geheel aan wapenvergunningen in België.

Het Comité I beveelt aan hieraan te verhelpen door de Veiligheid van de Staat toegang te verlenen tot het nationaal wapenregister.

Voor het overige herhaalt het Comité I de aanbevelingen die het in 1998 heeft geformuleerd en die nog steeds actueel zijn, namelijk:

— aan de Veiligheid van de Staat elke beslissingsbevoegdheid te ontnemen die zij bezit op het gebied van de uitvoering van de wapenwetgeving;

Mais contrairement au Comité R, l'administrateur n'estime pas que l'octroi de cette compétence générale d'avis à la Sûreté de l'État nécessitera une adaptation de l'arrêté royal du 20 septembre 1991 exécutant la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions. Selon elle, une circulaire ministérielle suffirait.

5. Conclusions et recommandations

La section d'étude «législation armes» de la Sûreté de l'État exerce les deux compétences que ce service détient en matière d'exécution de la législation sur les armes à feu: une compétence décisionnelle et une compétence d'avis à l'égard des étrangers et des citoyens belges sans résidence en Belgique.

Pendant la période du 1er janvier 1998 au 31 décembre 2000, 5 003 autorisations de détention et ports d'armes ont été délivrées par le service «législation arme» à des étrangers et à quelques citoyens belges sans résidence en Belgique, alors que pour la même période, ce service n'a reçu que 164 demandes d'avis écrits de la part des gouverneurs de provinces, de l'Office des étrangers du ministère de l'Intérieur ou des communes.

Sachant qu'au cours de ces trois années, on a délivré en Belgique près de 48 000 autorisations et permis de port d'arme, on constate que la Sûreté de l'État n'a été consultée que dans moins d'un pour cent des cas où elle-même n'est pas compétente pour délivrer ces autorisations de détention ou port d'arme.

Le Comité R reste pourtant d'avis que les compétences décisionnelles de la Sûreté de l'État n'ont aucun lien avec les activités naturelles d'un service de renseignement qui consistent à informer les autorités des menaces tant internes qu'externes pouvant peser sur la Belgique. La compétence d'avis de ce service est par contre celle qui entre le mieux dans le cadre de la mission d'information précitée.

Le Comité R constate par ailleurs que dans la pratique, la Sûreté de l'État n'a pas une vue globale sur les autorisations de détention et port d'arme délivrées en Belgique.

Le Comité R recommande qu'il soit remédié à cette lacune, notamment en permettant l'accès de la Sûreté de l'État au registre central des armes.

Le Comité R réitère par ailleurs les recommandations qu'il a formulées en 1998 et qui restent d'actualité, à savoir:

— retirer à la Sûreté de l'État toutes les compétences décisionnelles qu'elle détient en matière d'exécution de la législation sur les armes à feu;

— integendeel, aan deze dienst een algemene adviesbevoegdheid te verlenen, voorafgaand aan het uitreiken of intrekken van eender welke vergunning tot het voorhanden hebben van een verweer- en oorlogsvuurwapen, alsook van elke vergunning tot het dragen van een verweerwapen, en dit ongeacht de woonplaats van de aanvrager (in België of in het buitenland).

HOOFDSTUK 2

DE WIJZE WAAROP DE INLICHTINGENDIENSTEN DE GEGEVENS OMTRENT ACTIVITEITEN VAN DE VOORMALIGE KGB IN BELGIË HEBBEN VERWERKT

1. Inleiding

1.1. Procedure

Volgend op het verschijnen van diverse persartikelen over de onthullingen in het boek «*The Mitrokhin Archive. The KGB in Europe and the West*»(1) van de historicus Christopher Andrew, en nadat in ons land drie geheime KGB-opslagplaatsen met zendapparatuur waren ontdekt, besliste het Comité I op 6 oktober 1999 een toezichtsonderzoek te openen. Dit onderzoek kreeg de titel «De wijze waarop de inlichtingendiensten de gegevens omtrent activiteiten van de voormalige KGB in België hebben verwerkt».

Overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten kreeg de voorzitter van de Senaat per brief van 13 oktober 1999 kennis van de opening van dit onderzoek.

Op 12 oktober 1999 stuurde de voorzitter van het Comité I een gedetailleerd kantschrift terzake naar het hoofd van de Dienst Enquêtes.

Overeenkomstig artikel 43.1 van de voornoemde organieke wet werden de ministers van Landsverdediging en Justitie per brief van 3 november 1999 op de hoogte gebracht van het begin van het toezichtsonderzoek.

Op 8 november 1999 vroeg de voorzitter van het Comité I aan de heer procureur-generaal bij het hof van beroep van Brussel om aan het hoofd van de Dienst Enquêtes van het Comité I toestemming te verlenen om kennis te nemen van het gerechtelijk dossier

(1) Gepubliceerd door Allen Lane — The Penguin Press.

— attribuer par contre à ce service une compétence d'avis générale et préalable à la délivrance ou au retrait de toute autorisation de détention d'une arme à feu de défense et de guerre ainsi que de tout permis de port d'arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

CHAPITRE 2

LA MANIÈRE DONT LES SERVICES DE RENSEIGNEMENT ONT TRAITÉ LES ACTIVITÉS DE L'ANCIEN KGB EN BELGIQUE

1. Introduction

1.1. Procédure

Suite aux nombreux articles de presse reprenant les révélations contenues dans le livre intitulé «*The Mitrokhin Archive The KGB in Europe and the West*»(1) de l'historien Christopher Andrew, et la découverte dans notre pays de trois dépôts clandestins du KGB contenant du matériel de transmission, le Comité R a décidé le 6 octobre 1999 d'ouvrir une enquête de contrôle intitulée: «La manière dont les services de la Sûreté de l'État et du SGR ont traité les informations relatives aux activités de l'ancien KGB en Belgique».

En application de l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le président du Sénat a été informé de l'ouverture de cette enquête par courrier du 13 octobre 1999.

Le président du Comité R a adressé le 12 octobre 1999 une apostille circonstanciée en la matière au chef du Service d'enquêtes.

Conformément à l'article 43.1 de la loi organique précitée, les ministres de la Défense nationale et de la Justice ont pour leur part été avertis, par lettre du 3 novembre 1999, du début de l'enquête de contrôle.

Le 8 novembre 1999, le président du Comité R a demandé à M. le procureur général près la cour d'appel de Bruxelles, l'autorisation pour le chef du Service d'enquêtes du Comité R de prendre connaissance et copies des pièces du dossier judiciaire relatif à

(1) Publié par Allen Lane — The Penguin Press.

betreffende de ontdekking van zendapparatuur die op diverse bergplaatsen was begraven, alsook om fotokopieën te nemen van stukken uit dat dossier.

Deze toestemming werd verleend op 21 december 1999(1).

Op 24 maart 2000 bezorgde de Dienst Enquêtes zijn rapport aan het Comité I.

Op 16 maart 2001 keurde het Comité I een versie van het rapport goed, die als «vertrouwelijk» was geclassificeerd krachtens de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen.

De huidige versie, die aan de voorzitter van de Senaat en aan de ministers van Justitie en Landsverdediging werd bezorgd, en die tevens voor het openbaar verslag is bestemd, werd op 16 maart 2001 door het Comité I goedgekeurd.

Op 11 april 2001 heeft het Comité I de opmerkingen ontvangen van de minister van Justitie. Deze werden hernomen in een nota geclassificeerd «vertrouwelijk — wet van 11 december 1998».

Op vraag van het Comité I werd deze nota gedeclassificeerd tot de vermelding «beperkte verspreiding»(2), teneinde te kunnen worden meegedeeld aan de parlementaire begeleidingscommissies van P en I.

Op 25 april 2001 heeft de minister van Landsverdediging schriftelijk laten weten dat hij geen bezwaren had tegen de publicatie van het huidig verslag.

1.2. Vragen gesteld aan de inlichtingendiensten

1. Welke zijn, in het algemeen, de mogelijkheden van toegang van de Veiligheid van de Staat en van de ADIV tot het «Mitrokhin-archief»?

2. Wanneer en hoe hebben onze diensten kennis gekregen van het bestaan van dit archief?

3. In welke mate hebben onze eigen inlichtingendiensten (sectie contraspionage) informatie verzameld over de activiteiten beschreven in het voornoemde archief?

(1) De gerechtelijke overheden hebben de zaak geseponeerd, nadat ze van de ADIV informatie hadden ontvangen en na de ontdekking van de bergplaatsen en van het materieel dat er was opgeslagen.

(2) Gezien bepaalde informaties, beperkt deze vermelding de verspreiding tot de personen die bevoegd zijn om er kennis van te nemen zonder aan deze beperking de juridische gevolgen te verbinden voorzien door de wet (artikel 20 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen).

la découverte du matériel de transmission enterré dans diverses caches.

Cette autorisation a été accordée le 21 décembre 1999(1).

Le rapport du Service d'enquêtes a été communiqué au Comité R le 24 mars 2000.

Une version du rapport classifiée «confidentielle» aux termes de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a été approuvée par le Comité R le 16 mars 2001.

La présente version adressée au Sénat, ainsi qu'aux ministres de la Justice et de la Défense nationale qui est également la version destinée au rapport public, a été approuvée par le Comité R le 16 mars 2001.

Par courrier du 11 avril 2001, M. le ministre de la Justice a fait valoir ses observations dans une note classifiée «Confidentiel — loi du 11 décembre 1998».

À la demande du Comité R, cette note a été déclassifiée pour être transmise aux commissions de suivi P et R avec la mention «Diffusion restreinte»(2).

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas de remarque à formuler quant à la publication de ce rapport.

1.2. Les questions posées aux services de renseignement

1. Quelles sont, de manière générale, les possibilités d'accès de la Sûreté de l'État et du SGR aux «archives Mitrokhin»?

2. Quand et comment nos services ont-il été informés de l'existence de ces archives?

3. Dans quelle mesure nos propres services de renseignements (section contre-espionnage) ont-ils recueilli des informations concernant les activités mentionnées dans ces archives?

(1) L'affaire a été classée sans suite par les autorités judiciaires après la transmission des informations à celles-ci par le SGR et la découverte des caches et du matériel s'y trouvant.

(2) Eu égard à certaines informations, cette mention limite la diffusion aux personnes qualifiées pour en connaître sans attacher à cette limitation les effets juridiques prévus par la loi (article 20 de l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité).

4. Hebben de aldus ingewonnen gegevens alleen betrekking op de bergplaatsen van apparatuur of bestaat er ook informatie betreffende personen of kopstukken die in België zouden hebben gewerkt voor rekening van de KGB of de GRU(1)?

5. Hoe werd de verkregen informatie geëxploiteerd? Werd ze volledig of gedeeltelijk aan derden bezorgd? Zo ja, aan wie en wanneer?

6. Is er nog informatie die nog niet werd geëxploiteerd en/of bezorgd, of die momenteel nog wordt verwerkt?

7. Hoe verloopt de samenwerking met andere binnenlandse en buitenlandse diensten (onder meer met de Belgische politiediensten en de gerechtelijke overheden)?

8. Moeten de feiten die in het archief worden beschreven uitsluitend in een historische context worden bekeken of kan men ervan uitgaan dat er vandaag reden is om te vrezen of zelfs zeker te zijn dat de SVR, de opvolger van de KGB, activiteiten inzake spionage verricht?

9. *Quid* met de relaties die zouden bestaan tussen voormalige KGB-leden, die vandaag een nieuwe carrière hebben gevonden in de zakenwereld en de georganiseerde misdaad?

10. Vinden de inlichtingendiensten dat ze vandaag over de noodzakelijke middelen beschikken om deze problemen doeltreffend aan te pakken? Welke zijn deze middelen? Indien niet, hoe gaan ze dan te werk in de praktijk?

11. Welke besluiten halen de Veiligheid van de Staat en de ADIV uit hun voorbije ervaringen om de bedreigingen inzake spionage doeltreffender te beperken? Bestaan er in verband hiermee documenten, richtlijnen of rapporten? Wie zijn in voorkomend geval de bestemmelingen daarvan, benevens de Veiligheid van de Staat en de ADIV zelf?

2. Algemene beschouwingen

Basisconcepten inzake het uitwisselen van informatie

De Veiligheid van de Staat is de dienst die specifiek is belast met de defensieve opdracht van contraspionage, krachtens de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (artikelen 7 en 8).

Met betrekking tot het precieze gegeven dat het voorwerp is van dit onderzoek, vond het Comité I het daarom nuttig wat meer algemene informatie te verstrekken, in het bijzonder over de Veiligheid van de Staat.

(1) Militaire equivalent van de KGB.

4. Les données ainsi recueillies concernent-elles uniquement les caches de matériel ou bien existe-t-il également des informations relatives à des personnes ou à des personnalités qui auraient travaillé en Belgique pour le compte du KGB ou du GRU(1)?

5. Comment les informations reçues ont-elles été exploitées? Ont-elles été transmises, en tout ou en partie, à des tiers? Le cas échéant, à qui et à quel moment?

6. Y-a-t-il encore des informations qui n'ont pas été exploitées et/ou transmises ou qui sont actuellement traitées?

7. Comment se passe la coopération avec d'autres services nationaux et étrangers (y compris les autorités policières et judiciaires belges)?

8. Les faits relatés dans les archives doivent-ils être uniquement considérés dans un contexte historique ou peut-on considérer qu'à l'heure actuelle, il y a lieu de craindre ou même d'être certain que le SVR qui a succédé au KGB poursuit des activités d'espionnage?

9. *Quid* des relations qui existeraient entre des anciens membres du KGB qui se sont reconvertis dans le monde des affaires et la criminalité organisée?

10. Les services de renseignements estiment-ils disposer aujourd'hui des moyens nécessaires pour aborder cette problématique de manière efficace et quels sont ces moyens? Si ce n'est pas le cas, comment vont-ils faire en pratique?

11. Quelles sont les conclusions que la Sûreté de l'État et le SGR tirent de leur expérience passée afin de mieux limiter les menaces d'espionnage? Existe-t-il des documents, directives ou rapports à ce sujet? Qui en sont, le cas échéant, les destinataires autres que la Sûreté de l'État et le SGR eux-mêmes?

2. Généralités

Les concepts de base de l'échange d'informations

La Sûreté de l'État est le service spécifiquement chargé de la mission défensive de contre-espionnage par la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (articles 7 et 8).

Il a donc semblé utile au Comité R de donner, dans la perspective du sujet précis concerné par l'enquête, quelques informations de nature plus générale concernant plus particulièrement la Sûreté de l'État.

(1) L'équivalent militaire du KGB.

Deze informatie werd verstrekt door de Dienst Enquêtes van het Comité I. Daarbij werd rekening gehouden met de ervaring van sommige leden van deze dienst op het specifieke gebied dat het voorwerp is van dit onderzoek.

2.1. Relaties met de correspondenten

2.1.1. Organisatie

De wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten geeft aan de Veiligheid van de Staat de opdracht rechtstreekse contacten te onderhouden met buitenlandse overheden en toe te zien op het verzekeren van een samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten (1).

Deze samenwerking moet de Veiligheid van de Staat tot nut zijn bij het vervullen van zijn opdrachten. Tot die opdrachten behoren het opsporen, analyseren en verwerken van inlichtingen betreffende eender welke activiteit die de fundamentele belangen van het land in het algemeen bedreigt (2).

Binnen de Veiligheid van de Staat is een van de diensten van algemeen belang belast met de internationale betrekkingen. Deze dienst is verantwoordelijk voor de bilaterale betrekkingen met de «correspondenten» (dit wil zeggen met de buitenlandse inlichtingen- en veiligheidsdiensten) en voor de multilaterale betrekkingen.

Deze dienst is belast met de dossiers van de «Club» en de «Mec» (zie punt 2.1.2 hierna). Daartoe staat hij in voor de opvolging van alle inkomende en uitgaande correspondentie in verband hiermee. Hij moet de ontvankelijkheid ervan nagaan en zich ervan vergewissen dat er gevolg aan wordt gegeven.

Deze dienst staat ook in voor de verspreiding van de informatie die aankomt in de vorm van nota's. Hij organiseert de diverse contacten en volgt de ontwikkeling van elke corresponderende dienst.

2.1.2. Internationale contacten

De Veiligheid van de Staat onderhoudt contacten met een zestigtal buitenlandse of internationale diensten op de vijf continenten.

Natuurlijk wordt voorrang gegeven aan de internationale betrekkingen die zich situeren binnen het kader van wat men gewoonlijk de «geallieerde landen» noemt, in het bijzonder de buurlanden van België.

(1) Artikel 20.

(2) Artikel 7, 1º, van dezelfde wet houdende regeling van de inlichtingendiensten.

Ces informations ont été fournies par le Service d'enquêtes du Comité R en tenant compte également de l'expérience de certains membres de ce service dans le domaine particulier abordé par la présente enquête.

2.1. Les relations avec les correspondants

2.1.1. Organisation

La loi organique des services de renseignement et de sécurité du 30 novembre 1998 charge la Sûreté de l'État d'entretenir des contacts directs avec des autorités étrangères et de veiller à assurer une coopération avec les services de renseignement et de sécurité étrangers (1).

Cette coopération doit être utile à la Sûreté de l'État pour remplir ses missions parmi lesquelles figure la recherche, l'analyse et le traitement des renseignements relatifs à toute activité qui menace notamment d'une manière générale les intérêts fondamentaux du pays (2).

Au sein de la Sûreté de l'État, le service chargé des relations internationales est un des services d'intérêt général, responsable des relations bilatérales avec les «correspondants», (c'est-à-dire avec les services étrangers de renseignement et de sécurité) et des relations multilatérales.

Ce service est chargé des dossiers du «Club» et de la «Mec» (voir point 2.1.2 ci-après). À cette fin, il assure le suivi de toute la correspondance reçue et transmise à ce sujet, il est chargé d'en vérifier la recevabilité et de s'assurer qu'une suite y est donnée.

Ce service assure également la répartition des informations qui arrivent sous la forme de notes; il organise les contacts et suit l'évolution de chaque service correspondant.

2.1.2. Les contacts internationaux

La Sûreté de l'État entretient des relations avec une soixantaine de services étrangers ou internationaux répartis sur les cinq continents.

Il va de soi que les relations internationales auxquelles la priorité est donnée sont celles qui se situent dans le cadre de ce qu'il est convenu d'appeler «les pays alliés», en particulier ceux qui sont voisins de la Belgique.

(1) Article 20.

(2) Article 7, 1º, de la même loi organique des services de renseignement.

De Veiligheid van de Staat maakt deel uit van een aantal informatienetwerken waaraan alle andere landen van de Europese Unie deelnemen. Voorts is deze dienst lid van twee samenwerkingsverbanden die hierboven al werden genoemd, te weten de «Club» en de «Mec».

De «Club van Bern»

Het gaat om een feitelijke vereniging van de hoofden van de veiligheidsdiensten van de West-Europese landen. Deze vereniging werd opgericht in 1965 en werkt volgens strikte procedureregels.

De vergaderingen van deze vereniging vinden plaats om de zes maanden. Alleen de diensthoofden — of hun vertegenwoordiger — zijn bevoegd om beslissingen te nemen; dit moet gebeuren met eenparigheid van stemmen.

Voor de andere leden van de diensten vinden eenmaal per jaar «Les Cours du Club» plaats. Het doel daarvan bestaat erin de opleidingen op elkaar af te stemmen en de contacten tussen de «middle-rank officers» te bevorderen.

Regelmatig worden werkgroepen georganiseerd. Diensten die geen deel uitmaken van de «Club» kunnen hier toegelaten worden. Dit gebeurt geval per geval, en de beslissing moet worden genomen met eenparigheid van stemmen.

De «Middle European Conference» (MEC)

De «Mec» is een feitelijke vereniging van de hoofden van de civiele inlichtingen- en veiligheidsdiensten van West- en Midden-Europa.

We leggen er de nadruk op dat beide verenigingen (waarvan de Veiligheid van de Staat deel uitmaakt, in tegenstelling tot de ADIV) *sensu stricto* niet de minste wettelijke bescherming bieden met betrekking tot de informatie die wordt uitgewisseld.

Dit wil echter niet zeggen dat er geen regels bestaan. In de praktijk wordt de classificatie gegeven door de partij die de informatie verstrekt nauwgezet gevolgd en verleent de dienst die de informatie ontvangt daaraan het overeenstemmende niveau van classificatie (1).

(1) Er kan een parallel worden gelegd met het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet d.d. 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen. De bijlage 1 daarvan bevat een overeenstemming tussen de classificatieniveaus in toepassing van internationale overeenkomsten of verdragen die België binden, en het Belgische classificatieniveau.

La Sûreté de l'État fait partie de certains réseaux d'information auxquels participent tous les autres pays de l'Union européenne. Elle fait partie également de deux associations de coopération, dont il a déjà été question ci-dessus, à savoir: le «Club» et la «Mec».

Le «Club de Berne»

Il s'agit d'une association de fait des chefs des services de sécurité des pays d'Europe de l'Ouest dont la création remonte à 1965 et qui fonctionne suivant des règles strictes de procédure.

Tous les six mois une réunion a lieu et seuls les chefs des services — ou leur représentant — peuvent prendre des décisions à l'unanimité.

Pour les autres membres des services, il est organisé une fois par an «Les Cours du Club» dont le but est d'harmoniser les procédures de formation et de promouvoir les contacts entre les «middle-rank officers».

Des groupes de travail sont régulièrement organisés. À l'occasion de ceux-ci des services qui n'appartiennent pas au «Club» peuvent également être admis. Cette admission se réalise au cas par cas moyennant une décision prise à l'unanimité.

La «Middle European Conference» (MEC)

La «Mec» est une association de fait entre les patrons des services civils de renseignements et de sécurité d'Europe de l'Ouest et d'Europe centrale

Il convient de souligner que les deux associations (dont la Sûreté de l'État est membre ce qui n'est pas le cas du SGR) n'offrent *sensu stricto* aucune protection légale en ce qui concerne les informations échangées.

Cela ne veut pas dire cependant qu'il n'existe aucune règle. Dans la pratique, la classification de la partie qui donne les informations est strictement respectée et le service qui les reçoit leur confère le degré de classification correspondant (1).

(1) Un parallèle peut être fait avec l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité qui contient en annexe 1 une correspondance entre les degrés de classification en application de conventions ou de traités internationaux qui lient la Belgique, et le degré de classification belge.

2.1.3. Het uitwisselen van informatie

In zijn rapport 1997-1998 gebruikt het Canadees Comité van toezicht op de inlichtingendiensten de volgende formule: «Het Comité is zich bewust van het belang van het principe «voor wat hoort wat» of van de tegenprestatie in de wereld van de inlichtingendiensten» (1).

Het is een algemeen erkend feit dat de inlichtingendiensten wereldwijd handelen volgens een ruilsysteem. Dit betekent dat elke dienst ernaar streeft exclusieve informatie te verkrijgen, die hij vervolgens kan uitwisselen met andere diensten die op hun beurt in het bezit zijn van informatie waartoe de eerste dienst geen toegang heeft.

Het principe van het uitwisselen brengt onvermijdelijk het principe van de reciprociteit met zich mee.

Indien een land waarmee men gemeenschappelijke belangen heeft wordt bedreigd, is het evident dat de partner, die over de informatie beschikt, verplicht is aan dat eerste land bijstand te verlenen.

De «regel van de derde» is het basisprincipe van de samenwerking tussen de diensten. Dit is een van de oudste en striktste regels, die haar grondslag vindt in een van de bekommeringen aan de basis van elke vorm van samenwerking tussen diensten: de bescherming van de bronnen.

Artikel 5, § 1, waarin de procedure betreffende het uitwisselen van informatie binnen de «Club» wordt beschreven, formuleert deze regel als volgt:

«Zonder het formeel akkoord van de dienst die de informatie verstrekt, mag de informatie die binnen de Club wordt uitgewisseld niet worden bezorgd aan een vreemde instantie die geen deel uitmaakt van de Club, en mag ze evenmin worden gebruikt met andere doelstellingen dan deze beschreven in de informatie.»

Het gaat hier niet alleen om de regel van de derde, maar ook om de regel van de derde dienst. De bezorgdheid die blijkt uit het lezen van dit artikel van het statuut van de «Club», werd ook vastgelegd in andere teksten waarvan er sommige kracht van wet hebben verworven.

Het gaat onder meer om de veiligheidsreglementen «C-M(55)15» van de NAVO en «VR 100» van de WEU, die expliciet bepalen dat informatie pas kan worden verspreid nadat degene die de informatie heeft verstrekt zijn akkoord heeft gegeven.

We vinden dezelfde logica terug in het Verdrag van 28 januari 1981 van de Raad van Europa betreffende de bescherming van de persoonlijke levenssfeer. Daarin wordt bepaald dat het gevaarlijk is om, via

(1) Jaarverslag van de CSARS - 1997-1998 blz. 7.

2.1.3. L'échange d'informations

Dans son rapport 1997-1998, le Comité canadien de contrôle des services de renseignement utilise la formule suivante: «Le Comité est conscient de l'importance de la politique du «donnant- donnant» ou de la contrepartie dans le milieu du renseignement (1)».

Il est un fait reconnu que les services de renseignement opèrent dans le monde entier sur la base d'un système de troc consistant pour chaque service à obtenir des informations exclusives qui pourront par la suite être échangées avec d'autres services qui détiennent eux des informations inaccessibles au premier service.

Le principe de l'échange implique celui de la réciprocité.

Lorsqu'un pays avec lequel sont partagés des intérêts communs est menacé, il est évident que le partenaire, qui dispose des informations, a l'obligation de lui prêter assistance.

La «règle du tiers» constitue la règle de base de la collaboration entre services. Il s'agit là d'une des règles les plus anciennes et les plus strictes qui trouve son fondement dans une des préoccupations à la base de toute coopération entre service: la protection des sources.

L'article 5, § 1er, qui régit la procédure d'échange de renseignements au sein du «Club» formule cette règle de la manière suivante:

«Les renseignements qui sont échangés au sein du Club ne peuvent être adressés à une instance étrangère au Club, ni être utilisés à d'autres fins que celles contenues dans l'information sans l'accord formel du service qui en est à l'origine.»

Il s'agit ici non seulement de la règle du tiers, mais également de la règle du service tiers. La préoccupation qui apparaît de la lecture de cet article du statut du «Club» a également été formalisée dans d'autres contextes dont certains ont force de loi.

Il faut ainsi mentionner les règlements de sécurité «C-M(55)15» de l'OTAN et «VR 100» de l'UEO qui prévoient explicitement qu'avant toute dissémination d'informations, l'accord préalable doit être donné par celui qui les a fournies.

On retrouve la même logique dans la Convention du 28 janvier 1981 du Conseil de l'Europe, relative à la protection de la vie privée dans laquelle il est stipulé qu'il est dangereux de fournir, par l'intermédiaire

(1) Rapport annuel du CSARS - 1997-1998, p. 7

een andere partij, informatie over personen te verstrekken aan een Staat die geen deel uitmaakt van de verdragsluitende partijen (1).

2.2. Samenwerking inzake contraspionage

Sinds de Koude Oorlog en de vestiging van het NAVO-hoofdkwartier in België (1967) werkten de geallieerden samen op het gebied van contraspionage. Deze samenwerking was in hoofdzaak gericht tegen het communistisch blok in het algemeen en tegen de landen van het Warschaupact in het bijzonder.

Zo wisselden de westerse inlichtingendiensten informatie uit, in het bijzonder over het personeel van de Sovjet-Russische ambassades (handels- en persattachés) en over de werknemers van luchtvaartmaatschappijen of van andere ondernemingen waar zowel de KGB als de GRU overal ter wereld hun inlichtingenofficieren plaatsten, onder de dekmantel van functies die speciaal daarvoor werden gecreëerd.

Gegevens over deze personen en over de evolutie van hun internationale carrière werden voortdurend bijgewerkt en onderling uitgewisseld door alle westerse inlichtingendiensten.

Naast dit permanente systeem voor het uitwisselen van gegevens, bestond de mogelijkheid informatie te vragen via de verbindingsofficieren van de diverse westerse inlichtingendiensten op de ambassades, alsook via het « Nato Office of Security » (NOS).

2.3. De KGB in België

Het Belgisch grondgebied, waar een groot aantal internationale instellingen gevestigd zijn (onder meer de toenmalige EG en de NAVO), was een belangrijk doelwit voor de inlichtingendiensten van de voormalige Sovjet-Unie.

Dit was de opdracht van enkele tientallen officieren van de inlichtingen- en veiligheidsdiensten van de USSR. Zij konden rekenen op de hulp van andere analoge diensten van de Oost-Europese landen.

Zoals in alle landen waar de KGB inlichtingen verzamelde, bestond er ook in België een zogenaamde « residentie ». De vertegenwoordigers van de bewuste diensten waren georganiseerd binnen deze residentie.

Ze werd geleid door de « resident » en zijn adjunct. Men vond er niet alleen technische specialisten (decodeurs, veiligheidspersoneel ...), maar ook officieren belast met het echte inlichtingenwerk, verdeeld over diverse « lijnen ».

(1) Artikel 12, § 3, *b)*.

d'une autre partie, des informations liées aux personnes à un État qui n'est pas partie à la convention (1).

2.2. Coopération en matière de contre-espionnage

Depuis la guerre froide et l'installation du quartier général de l'OTAN en Belgique (1967), il existait en matière de contre-espionnage une coopération entre les alliés qui était principalement dirigée contre le bloc communiste en général et les pays du pacte de Varsovie en particulier.

Des informations ont ainsi été échangées entre les services de renseignement occidentaux concernant notamment le personnel des ambassades soviétiques (attachés commerciaux, attachés de presse) et celui de sociétés de transport aérien ou d'autres entreprises dans lesquelles aussi bien le KGB que le GRU plaçaient, dans le monde entier, leurs officiers de renseignement sous le couvert de fonctions spécialement réservées à cet effet.

Des données concernant ces personnes, ainsi que celles en rapport avec l'évolution de leur carrière internationale, étaient constamment mises à jour par tous les services de l'ouest et faisaient l'objet d'un échange mutuel.

Outre ce système permanent d'échange de données, il existait également une possibilité de demander des informations par le canal des officiers de liaison des différents services de renseignements occidentaux présents dans les ambassades, ainsi que par l'intermédiaire du « NOS » (Nato Office of Security).

2.3. Le KGB en Belgique

Le territoire belge, lieu d'établissement de toute une série d'institutions internationales (entre autres la CEE et l'OTAN), représentait une cible importante pour les services de renseignement de l'ex-URSS.

C'était la mission de quelques dizaines d'officiers appartenant aux services de renseignement et de sécurité de l'URSS, qui pouvaient aussi compter sur l'aide des autres services analogues des pays de l'Europe de l'Est.

Comme dans tous les pays où le KGB était actif dans le domaine de la collecte du renseignement, il existait aussi en Belgique ce que l'on appelait une « résidence » au sein de laquelle les représentants de ces services étaient organisés.

Celle-ci était dirigée par le « résident » et son adjoint, et comprenait, à côté de spécialistes techniques (décodeurs, personnel de sécurité...), des officiers responsables du travail de renseignement qui étaient répartis en « lignes ».

(1) Article 12, § 3, *b)*.

De belangrijkste lijnen waren de lijnen «P», «X», «KR» en «N».

De lijn «P» bestond uit officieren die de opdracht hadden politieke informatie in te winnen (met inbegrip van militaire informatie en algemene economische informatie). In het algemeen werd ze beschouwd als de belangrijkste en productiefste lijn.

Teneinde hun opdracht zo doeltreffend mogelijk te vervullen, moesten deze officieren zo goed mogelijk op de hoogte blijven van de politieke situatie in het land waar ze verbleven. Daartoe raadpleegden ze open bronnen en onderhielden ze contacten met kopstukken of andere personen uit de politieke wereld.

Meestal maakten ze deel uit van het diplomatiek personeel of trof men ze aan op persagentschappen. Om meer vertrouwelijke informatie in te winnen, probeerden ze agenten te rekruteren, in hoofdzaak in politieke, journalistieke en literaire kringen.

Naast het verzamelen van informatie hield hun opdracht ook in dat ze gebruik maakten van methodes die men «actieve maatregelen» noemde. Dit betekent dat ze bijvoorbeeld probeerden de publieke opinie gunstig te stemmen jegens de USSR (of ongunstig jegens tegenstanders van de USSR).

Hiervoor deden ze ofwel een beroep op schrijvers of journalisten die in hun boeken of artikelen, eventueel in ruil voor een vergoeding, vooraf bepaalde standpunten verdedigden waarmee de KGB de publieke opinie probeerde te manipuleren (meestal en op subtiele wijze door het westers bondgenootschap aan te vallen), ofwel op beïnvloedingsagenten die bepaalde tendensen ingang deden vinden in de samenleving of binnen sommige drukkingsgroepen.

De lijn «X» was binnen de «residentie» de interface van het Directoraat NT van de KGB. Dit directoraat werd opgericht in 1963. Zijn voornaamste opdracht bestond erin informatie te verzamelen op de volgende gebieden: nucleaire technologie, wetenschappelijk onderzoek, ruimteonderzoek, strategische wetenschappen, cybernetica en bedrijfsprocédés.

Het Directoraat NT was betrokken bij de operaties en het coördineren van de activiteiten inzake wetenschappelijke, technische en bedrijfsspionage van alle andere departementen van de KGB.

Het besliste welke Russische wetenschappers de toelating kregen deel te nemen aan internationale conferenties. Het plaatste ook agenten in elke groep die naar het buitenland reisde.

Sinds zijn oprichting is dit Directoraat onophoudelijk gegroeid. In het begin van de jaren zeventig waren enkele honderden officieren werkzaam op het hoofdkwartier. Het was vertegenwoordigd op de ambassa-

Les plus importantes de celles-ci étaient les lignes «P», «X», «KR» et «N».

La ligne «P» composée d'officiers qui avaient pour tâche de collecter des informations politiques (en ce comprises des informations militaires et des informations économiques générales) était traditionnellement considérée comme la plus importante et la plus productive.

Pour pouvoir remplir leur mission avec efficacité, ces officiers devaient se tenir informés le mieux possible de la situation politique de leur pays de résidence par la consultation des sources ouvertes et leurs contacts avec des personnalités (ou des personnes) du monde politique.

On les retrouvait le plus souvent dans le personnel diplomatique ou au sein des agences de presse. Pour la récolte d'informations plus confidentielles, ils essayaient de recruter des agents, principalement dans les milieux politique, journalistique et littéraire.

En dehors de la collecte de l'information, leur mission comportait également le recours à des méthodes appelées «mesures actives», comme celle de chercher à influencer l'opinion publique en faveur de l'URSS (ou en défaveur des opposants à l'URSS).

Dans ce cas, ils avaient recours soit à des écrivains ou à des journalistes qui au travers de livres ou d'articles, éventuellement moyennant rémunération, défendaient des positions préétablies par lesquelles le KGB tentait de manipuler l'opinion publique (le plus souvent et de manière subtile par des attaques contre l'alliance occidentale), soit en ayant recours à des agents d'influence qui induisaient des tendances déterminées dans la société ou à l'intérieur de certains groupes de pression.

La ligne «X» était l'interface au sein de la «résidence» du Directorat NT du KGB qui fut constitué en 1963, avec comme tâche principale la collecte d'informations dans les domaines de la technologie nucléaire, de la recherche scientifique, de l'espace, des sciences stratégiques, de la cybernétique et des procédés industriels.

Le Directorat NT se trouvait impliqué dans les opérations et la coordination des activités d'espionnage scientifique, technique et industriel menées dans tous les autres départements du KGB.

Il décidait quel scientifique soviétique recevrait l'autorisation de participer à des conférences internationales et il plaçait également des agents dans chaque groupe quittant le pays.

Depuis sa création, ce Directorat a connu une croissance continue. Au début des années 70, son quartier général comptait quelques centaines d'officiers et il était représenté dans les ambassades des pays impor-

des van belangrijke landen. Bovendien beschikte het over een groot aantal specialisten op alle gebieden van de wetenschappen.

Halverwege de jaren zeventig beseften de leiders van de Sovjet-Unie dat hun economie achterop was geraakt tengevolge van de problemen om grondstoffen om te zetten in afgewerkte producten.

Daarom probeerden ze ondernemers ertoe over te halen vestigingen op te richten in de Sovjet-Unie en hun knowhow te leveren op het gebied van technologie en organisatie. Dit betekende echter niet dat ze hun inspanningen om wetenschappelijke en technologische informatie op andere wijze te verkrijgen terugschroefden.

In de jaren tachtig gaven ze absolute voorrang aan activiteiten inzake wetenschappelijke en technische spionage. Daarbij gaven ze blijk van een groeiende belangstelling voor een technologie die niet specifiek militair was.

Het ging om een gemeenschappelijke inspanning waartoe alle lidstaten van het Oostblok moesten bijdragen. Deze inspanning was in het bijzonder gericht op het inwinnen van informatie in de volgende sectoren: technologie, elektronica, wiskunde, genetica. Eigenlijk ging het om alle domeinen waartoe de lidstaten van het Warschaupact zo goed als geen toegang meer hadden, sinds de oprichting in 1949, in het kader van de NAVO, van een «Coordinating Committee for multilateral Export Controls» (COCOM). Dit comité had tot doel de toegang van de Sovjet-Unie en van de lidstaten van het Oostblok tot een moderne wapenindustrie te beletten of ten minste af te remmen.

De inspanningen van de KGB bleven echter niet beperkt tot het louter militaire aspect van de toepassingen op het gebied van wetenschappelijk onderzoek, maar richtten zich ook op alle industriële toepassingen.

De inlichtingenofficieren die in het buitenland voor het Directoraat NT werkten, behoorden tot de lijn X die geleidelijk aan belang won. In België telde deze lijn tussen de 4 en 6 officieren, die konden rekenen op de steun van de officieren van de andere lijnen. Ze behoorden voor het merendeel tot het personeel van de ambassades.

De functies van Sovjet-Russische handelsattachés alsook de activiteiten van sommige gemengde Belgisch-Sovjet-Russische bedrijven vormden uitstekende dekmantels en boden interessante kansen om contacten te leggen met de actoren van de economische en bedrijfswereld.

Zonder dat we hierover meer details kunnen geven, melden we nog dat dankzij de activiteiten van de Veiligheid van de Staat sommige van deze spionnen werden ontmaskerd in de periode tussen 1980 en 1990.

tants. De surcroît, il disposait d'un grand nombre de spécialistes dans tous les domaines scientifiques.

Au milieu des années 70, les responsables soviétiques ont réalisé que leur économie était handicapée par des problèmes de transformation des matières premières en produits finis.

Ils essayèrent alors de convaincre des entrepreneurs de créer des entités en Union-soviétique et de leur livrer leur «know-how» dans les domaines de la technologie et de l'organisation. Cela ne réduisait pas pour autant les efforts consentis pour obtenir par d'autres moyens des informations de nature scientifique et technologique.

Dans les années 80, ils donnèrent une priorité absolue à l'espionnage scientifique et technique en manifestant, dans ce contexte, un intérêt toujours croissant pour la technologie non spécifiquement militaire.

Il s'agissait d'un effort commun auquel tous les autres États du bloc de l'Est devaient participer. Cet effort était spécialement dirigé vers la collecte d'informations dans les secteurs de la technologie, de l'électronique, des mathématiques, de la génétique, en fait dans tous les domaines qui étaient devenus plus ou moins inaccessibles pour les membres du pacte de Varsovie, depuis la création en 1949 dans le cadre de l'Otan, d'un «Coordinating Committee for multilateral Export Controls» (COCOM). Ce comité avait comme objectif d'empêcher ou, du moins, de ralentir l'accès de l'Union soviétique et des États du bloc de l'Est à une industrie d'armement moderne.

Les efforts du KGB n'étaient toutefois pas limités au domaine purement militaire des applications de la recherche scientifique, mais visaient aussi toutes les applications industrielles.

Les officiers de renseignement qui travaillaient à l'étranger pour le Directorat NT appartenaient à la ligne X qui devenait graduellement la plus importante. En Belgique, cette ligne a compté entre 4 et 6 officiers, qui pouvaient compter sur l'appui des officiers des autres lignes. Ils appartenaient pour la plupart au personnel des ambassades.

Les fonctions d'attachés commerciaux soviétiques ainsi que les activités de certaines entreprises mixtes belgo-soviétiques constituaient d'excellentes couvertures et offraient des opportunités intéressantes pour entrer en relation avec les acteurs du monde économique et industriel.

Sans pouvoir entrer dans plus de détails, il faut mentionner que la Sûreté de l'État a permis d'intercepter certains de ces espions dans les années 80 à 90.

De derde lijn van KGB-residenten was de lijn «KR» (contraspionage).

De officieren van deze lijn waren niet alleen belast met het toezicht op en de bescherming van de ambassades en de «residentie», maar moesten er ook voor zorgen dat de Sovjet-Russische gemeenschap niet werd geïnfiltreerd door de inlichtingendienst van het gastland. Daartoe hielden ze alle Sovjet-Russische burgers nauwlettend in het oog, alsook hun collega's van de andere lijnen, met als gevolg dat ze niet erg populair waren.

Ze waren eveneens belast met het verzamelen van inlichtingen over de politie- en inlichtingendiensten van het gastland. Eventueel moesten ze deze diensten ook infiltreren.

Ze boden regelmatig operationele ondersteuning aan hun collega's van de andere lijnen, omdat ze werden beschouwd als specialisten inzake bewakings- en schaduwoperaties.

De 4e belangrijke lijn van de KGB-residentie was de lijn «N», die ressorteerde onder het «Directoraat S».

Naast de officiële residentie waar de inlichtingenofficieren werkten en inlichtingen verzamelden via informanten of met behulp van andere middelen, bestond er in de meeste landen die de KGB belangrijk genoeg achtte ook een zogenaamde «illegale residentie».

Ze bestond uit agenten die een valse identiteit hadden aangenomen en elk contact met de ambassade vermeden.

Deze agenten waren KGB-leden die in de USSR een speciale opleiding hadden genoten en die, voorzien van een rijkelijk gestoffeerd en zorgvuldig samengesteld persoonlijk verleden («de legende») en uitgerust met de nodige papieren, een inlichtingennet vormden.

In de periode tussen de twee wereldoorlogen waren deze illegale netwerken vaak belangrijker dan de legale netwerken. Dit was het gevolg van het feit dat de mogelijkheden om in sommige landen over officiële vertegenwoordigers te beschikken heel beperkt waren en dat voor KGB-officieren weinig dekmantelfuncties konden worden voorzien. Na de Tweede Wereldoorlog namen de Sovjet-Russische vertegenwoordigingen in aantal toe en kwam er meer plaats vrij voor de steeds talrijker legale residenten.

Vóór de jaren tachtig waren er in België nog enkele illegale residenten aanwezig, die vooral tot taak hadden een clandestien inlichtingennet op te bouwen dat de KGB had kunnen gebruiken indien het diplomatiek personeel in geval van conflict het grondgebied had moeten verlaten.

Binnen het kader van de legale residentie waren er ook nog enkele KGB-officieren die het «Directoraat

La troisième ligne importante des résidents du KGB était la ligne « KR « (contre- espionnage).

Les officiers de cette ligne n'étaient pas seulement responsables de la surveillance et de la protection des ambassades et de la «résidence», mais ils devaient aussi veiller à ce que la communauté soviétique ne soit pas infiltrée par les services de renseignement du pays d'accueil. À cette fin ils surveillaient étroitement tous les ressortissants soviétiques, ainsi d'ailleurs que leurs collègues des autres lignes, ce qui ne les rendait pas très populaires.

Leur mission comportait également la collecte d'informations concernant les services de police et de renseignement du pays d'accueil et éventuellement l'infiltration de ces services.

Puisqu'ils étaient considérés comme des spécialistes en matière de surveillance et de filatures, ils apportaient aussi régulièrement un appui opérationnel à leurs collègues des autres lignes.

La 4e ligne importante de la résidence du KGB était la ligne «N», dépendante du «Directorat S».

À côté de la résidence officielle au sein de laquelle les officiers de renseignement œuvraient et collectaient des informations via des informateurs ou par d'autres moyens, se trouvait dans la plupart des pays que le KGB considérait comme suffisamment important, ce que l'on appelait la «résidence illégale».

Elle était composée d'agents qui vivaient sous une fausse identité et qui évitaient les contacts avec l'ambassade.

Il s'agissait de membres du KGB qui étaient spécialement formés en URSS et qui, nantis d'un passé personnel étoffé et soigneusement élaboré («la légende») ainsi que des papiers nécessaires, constituaient un réseau de renseignements.

Entre les deux guerres, ces réseaux illégaux étaient souvent plus importants que les légaux. Ceci résultait du fait que les possibilités d'avoir des représentants officiels étaient très limitées dans certains pays et que peu de fonctions de couvertures pouvaient être prévues pour des officiers du KGB. Après la deuxième guerre mondiale, les représentations soviétiques augmentèrent et l'on a pu offrir davantage de place à des résidents légaux de plus en plus nombreux.

Avant les années 80, on peut dire qu'il subsistait encore en Belgique quelques résidents illégaux dont le rôle consistait principalement à préparer un réseau clandestin de renseignements sur lequel le KGB aurait pu compter dans l'éventualité où, en cas de conflit, le personnel diplomatique aurait dû quitter le territoire.

Dans le cadre de la résidence légale, il y avait également encore quelques officiers du KGB qui représen-

S» vormden en die logistieke ondersteuning moesten bieden aan de «illegale» officieren.

Naast de belangrijkste lijnen (P, X , KR en N) omvatte «de residentie» ook de lijn «EM» (controle van emigranten), de lijn «SK» (controle van de Sovjet-Russische gemeenschap in de gastlanden) en de lijn «I» (informatica).

Benevens haar eigen officieren kon de KGB-residentie rekenen op de medewerking van zogenaamde «gecoöpteerde agenten», dit is Sovjetburgers (ambassadepersoneel, maar ook zakenlieden of wetenschappers die regelmatig naar het Westen reisden) die, zonder dat ze lid waren van de KGB, niettemin bereid waren voor deze dienst te werken en daarbij meer te doen dan het werk van een gewone informant.

Voorts kon de KGB rekenen op de inspanningen van de inlichtingendiensten van de andere leden van het Warschaupact (met uitzondering van Roemenië), die onder controle van de KGB stonden.

In totaal kunnen we ervan uitgaan dat tijdens de jaren tachtig permanent een dertigtal inlichtingenofficieren van de KGB en een vijftiental officieren van de GRU (militaire inlichtingen) in België actief waren.

Rekening houdend met het feit dat ze meer dan de andere lijnen werden gevolgd, alsook met het feit dat hun activiteiten gemakkelijker konden worden gevolgd, mogen we er eveneens van uitgaan dat vooral de lijnen «P» en «X» actief waren inzake het verzamelen van inlichtingen met behulp van menselijke bronnen.

2.4. Contraspionage bij de Veiligheid van de Staat

De Belgische contraspionage werd georganiseerd vanaf het einde van de oorlog en werd verder ontwikkeld tijdens de jaren van de Koude Oorlog waarin de spanningen het grootst waren.

Na de overbrenging van het hoofdkwartier van de NAVO naar België in 1967, werd ons land een doelwit voor de inlichtingendiensten van de landen van het Oostblok, waartegen de Alliantie werd opgericht.

Op verzoek van de partners van de Noord-Atlantische Verdragsorganisatie werd van de Belgische inlichtingendiensten een grote inspanning gevraagd, niet alleen op het vlak van het personeel dat werd ingezet, maar ook inzake de organisatie van de secties die de taak kregen de activiteiten van de inlichtingendiensten van potentiële tegenstanders te «counteren».

Er bestond een goede samenwerking met het ministerie van Buitenlandse Zaken en de Dienst Vreemdelingenzaken, de NAVO en de EG. Met de correspon-

taient le «Directorat S» et qui devaient offrir un support logistique aux officiers «illégaux».

À côté des lignes les plus importantes (P, X, KR, et N) on trouvait aussi, au sein de « la résidence», la ligne «EM» (contrôle des émigrés), la ligne «SK» (contrôle de la communauté soviétique dans le pays d'accueil) et la ligne «I» (informatique).

Outre ses propres officiers, la résidence du KGB pouvait compter sur la collaboration d'«agents cooptés», c'est-à-dire de ressortissants soviétiques (du personnel d'ambassade, mais aussi des hommes d'affaires ou des scientifiques qui voyageaient régulièrement à l'Ouest) qui, sans appartenir au KGB, étaient cependant disposés à travailler pour ce service en étant davantage impliqués qu'un simple informateur.

Le KGB pouvait compter également sur les efforts des autres services de renseignement des membres du pacte de Varsovie (à l'exclusion de la Roumanie) sur lesquels il avait le contrôle.

Au total, on peut ainsi estimer que durant les années 80, il y avait en permanence une trentaine d'officiers de renseignement du KGB et une quinzaine d'officiers du GRU (renseignement militaire) actifs en Belgique.

En tenant compte du fait qu'ils étaient davantage suivis que les autres lignes et aussi que leurs activités pouvaient être mieux suivies, on peut estimer également que c'était surtout les lignes «P» et «X» qui étaient actives en matière de collecte du renseignement en utilisant des sources humaines.

2.4. Le contre-espionnage à la Sûreté de l'État

L'organisation du contre-espionnage belge a débuté après les années de guerre et s'est développée durant les années les plus tendues de la guerre froide.

Depuis le déplacement du quartier général de l'Otan en Belgique en 1967, notre pays fut une cible désignée pour les services de renseignement des pays du bloc de l'Est contre lesquels l'Alliance était constituée.

À la demande des partenaires du Traité de l'Atlantique Nord, un effort considérable fut demandé aux services de renseignement belges, tant sur le plan du personnel engagé que sur celui de l'organisation des sections qui auraient à «contrer» les activités des services de renseignement des adversaires potentiels.

Il existait une bonne collaboration avec le ministère des Affaires étrangères et l'Office des étrangers, l'OTAN et la CEE. Un échange suivi d'informations

denten van de NAVO-leden werd een permanente uitwisseling van informatie op touw gezet.

Tot aan de val van de Berlijnse Muur in 1990 bleven de inspanningen van de Veiligheid van de Staat inzake contraspionage op hetzelfde niveau staan. Deze inspanningen kregen concrete vorm door de regelmatige interceptie van diplomaten uit het Oostblok die schuldig werden bevonden aan spionage en in de meeste gevallen werden teruggestuurd. Tussen 1982 en 1986 werden 7 gevallen geïdentificeerd (waarvan 3 alleen al in 1983).

De sectie die zich specifiek met de USSR bezighield, behandelde tussen 1967 en 1986 in totaal 13 gevallen. Telkens werden de Sovjet-Russische diplomaten verklaard tot *persona non grata*.

Op het einde van de jaren tachtig werd deze sectie geleidelijk ontmanteld, omdat nieuwe materies (ideologisch extremisme, terrorisme, proliferatie) steeds meer energie opslorpten en een steeds groter menselijk potentieel vergden.

In weerwil van deze situatie bleek het nog mogelijk om in 1990, dankzij de ingewonnen inlichtingen, een voorlopig einde te stellen aan de activiteiten van de lijn P in ons land.

De Veiligheid van de Staat interpelleerde diverse personen. Tegen een van hen werden gerechtelijke vervolgingen aangespannen.

Na 1990 ging men verder met het ontmantelen van de sectie, rekening houdend met de gewijzigde internationale situatie.

In 1992 kon de lijn X gedurende enige tijd worden geneutraliseerd, na de bekendmaking van de namen van agenten die tot deze lijn behoorden (operatie «Glasnost»).

Hoewel deze zaak aanleiding gaf tot huiszoekingen en sommige personen in voorlopige hechtenis werden genomen, werd geen van de betrokkenen gerechtelijk vervolgd.

Er werd bewezen dat sommige bedrijven in het verleden dekmantelfuncties ter beschikking hadden gesteld van KGB-officieren (in hoofdzaak officieren van de lijn «X»).

Voorts is gebleken dat sommige van die bedrijven banden hadden met de Russische maffia. Vandaag houdt een nieuwe sectie van de Veiligheid van de Staat zich bezig met criminele organisaties in Midden- en Oost-Europa.

Uit gesprekken die de Dienst Enquêtes van het Comité I heeft gevoerd met leden van de Veiligheid van de Staat, alsook uit de verklaringen die de administrateur-generaal van de Veiligheid van de Staat in oktober 1999 aan de pers heeft afgelegd met betrekfut instauré avec les correspondants des membres de l'OTAN.

Jusqu'à la chute du Mur de Berlin en 1990, les efforts de la Sûreté de l'État en matière de contre-espionnage restèrent au même niveau. Ces efforts se sont concrétisés par l'interception régulière de diplomates du bloc de l'Est convaincus d'espionnage et qui furent dans la plupart des cas renvoyés. Au cours de la période allant de 1982 à 1986, 7 cas furent identifiés (dont 3 pour la seule année 1983).

En ce qui concerne la section qui s'occupait spécifiquement de l'URSS, 13 affaires au total furent traitées de 1967 à 1986, qui chaque fois conduisirent à faire déclarer des diplomates soviétiques *persona non grata*.

À la fin des années 80, cette section fut progressivement démantelée parce que de nouvelles matières (l'extrémisme idéologique, le terrorisme, la prolifération) absorbaient de plus en plus d'énergie et demandaient davantage de potentiel humain.

Nonobstant cette situation, il fut encore possible, en 1990, grâce aux renseignements recueillis, de mettre un terme provisoire aux activités de la ligne P dans notre pays.

Plusieurs personnes furent interpellées par la Sûreté de l'État. Une de celles-ci fut poursuivie judiciairement.

Après 1990, et compte tenu du changement de la situation internationale, le démantèlement de la section fut poursuivi.

En 1992, la révélation des noms des agents actifs dans la ligne X a également permis de la neutraliser pendant quelque temps (opération «Glasnost»).

Bien que cette affaire ait donné lieu à des perquisitions et à des mises en détention préventive, aucun des intervenants ne fut poursuivi devant les tribunaux.

Il fut établi que des entreprises avaient fourni, dans le passé, des fonctions de couvertures pour des officiers du KGB (principalement ceux de la ligne «X»).

Il est apparu également que certaines d'entre elles avaient des liens avec la maffia russe. Une nouvelle section de la Sûreté de l'État s'occupe aujourd'hui des organisations criminelles et de l'Europe centrale et orientale.

Il ressort d'entretiens que le service d'enquêtes du Comité R a eus avec des membres de la Sûreté de l'État, ainsi que de déclarations de l'administrateur général de la Sûreté de l'État à la presse en octobre 1999, qu'en ce qui concerne la Russie, un effort allait

king tot Rusland, blijkt dat er een inspanning zou worden geleverd inzake de gemengde bedrijven, in hoofdzaak in het kader van de strijd tegen de Russische maffia.

Tengevolge van de reacties in de Belgische pers op de zaak « Mitrokhin », liet de Veiligheid van de Staat weten dat er opnieuw voorrang zou worden gegeven aan de strijd tegen de activiteiten van de SVR(1), voornamelijk in het kader van de wettelijke opdracht inzake de bescherming van het economisch en wetenschappelijk potentieel van het land.

In de krant *La Dernière Heure* van 16 september 1999 verklaarde de woordvoerster van de Veiligheid van de Staat :

« Na de val van de Berlijnse Muur ging men ervan uit dat spionage zou afnemen. Dat is gedurende een paar jaar inderdaad het geval geweest, maar het is duidelijk dat de activiteiten opnieuw toenemen... De Veiligheid van de Staat had de onderzoeken inzake contraspionage geleidelijk verminderd in het voordeel van de strijd tegen het terrorisme en de georganiseerde misdaad, die de voornaamste prioriteiten zijn geworden. Vandaag stellen we echter vast dat we rechtsomkeer moeten maken en opnieuw de nadruk moeten gaan leggen op contraspionage. »

3. Resultaten van het onderzoek

3.1. Antwoorden op de vragenlijst

Het Comité I stelt vast dat de zo goed als identieke antwoorden die beide diensten hebben gegeven op de vragen in punt 1.2. hierboven, door de ADIV als « vertrouwelijk » werden geclassificeerd, terwijl de Veiligheid van de Staat geen enkel niveau van classificatie heeft toegekend.

Op 8 maart 2001 werd een brief verstuurd naar het hoofd van de ADIV met de vraag of deze classificatie werd behouden dan wel volledig of gedeeltelijk kon worden opgeheven, teneinde het Comité I toe te laten overeenkomstig de wet een rapport op te stellen voor de begeleidingscommissies en voor de betrokken ministers.

Het Comité I had nog geen antwoord gekregen op deze vraag op het ogenblik waarop dit rapport werd goedgekeurd.

Bijgevolg kan het Comité I, rekening houdend met de bepalingen van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, onmogelijk de inhoud van deze antwoorden bekendmaken aan personen die geen houder zijn van een veiligheidsmachtiging van het vereiste niveau.

(1) Een van de Russische inlichtingendiensten die de activiteiten van de ex-KGB op dit vlak heeft overgenomen.

être fait au niveau des entreprises mixtes principalement dans le cadre de la lutte contre la mafia russe.

Suite aux échos donnés par la presse belge à l'affaire « Mitrokhin », la Sûreté de l'État a fait savoir que la priorité serait à nouveau donnée à la lutte contre les activités du SVR(1), principalement dans le cadre de la mission légale de la protection du potentiel économique et scientifique du pays.

Le quotidien *La Dernière Heure* du 16 septembre 1999, rapporte ainsi les propos de la porte-parole de la Sûreté de l'État :

« Avec la chute du mur de Berlin, on imaginait que l'espionnage allait diminuer. Cela a été le cas durant quelques années, mais les faits ont manifestement repris... La Sûreté avait progressivement diminué les enquêtes de contre-espionnage au profit de la lutte contre le terrorisme et le crime organisé, qui sont devenus les premières priorités. Aujourd'hui on constate qu'il faut faire marche arrière et remettre l'accent sur le contre-espionnage. »

3. Les résultats de l'enquête

3.1. Les réponses au questionnaire

Le Comité R se doit de signaler qu'il constate que les réponses quasi-identiques fournies par les deux services aux questions dont l'énoncé est repris au point 1.2. ci-avant ont été classifiées « confidentiel » par le SGR et n'ont fait l'objet d'aucune classification par la Sûreté de l'État.

Un courrier a été adressé au chef du SGR en date du 8 mars 2001 lui demandant si cette classification était maintenue ou si elle pouvait être levée en tout ou en partie, afin de permettre au Comité R de faire rapport, comme la loi le prévoit à sa commission de suivi ainsi qu'aux ministres concernés.

Au moment d'approuver le présent rapport aucune réponse définitive n'est encore parvenue au Comité R.

Celui-ci n'est donc pas en mesure actuellement, compte tenu des dispositions de la loi sur la classification et les habilitations de sécurité du 11 décembre 1998 de reproduire le contenu de ces réponses à destination de personnes ne disposant pas d'une habilitation de sécurité du niveau requis.

(1) Un des services de renseignements russe qui a repris dans ce domaine les activités de l'ex-KGB.

3.2. Vaststellingen en commentaar van het Comité I

3.2.1. Vertraging bij het bezorgen van informatie aan de Veiligheid van de Staat en aan de ADIV

In het boek van Professor Christopher Andrew en Vasili Mitrokhin (1) lezen we dat deze laatste op 7 september 1992 in Engeland was aangekomen. In augustus 1993 maakte een Amerikaans schrijver reeds melding van deze zaak in een boek met de titel *«Federal Bureau of Investigation (FBI)»*.

Hij schreef onder meer dat de informatie die een voormalig KGB-medewerker over honderden Amerikanen had verstrekt zo specifiek was dat reeds in de zomer van 1993 in de meeste grote Amerikaanse steden FBI-agenten waren gemobiliseerd om een onderzoek te voeren naar deze feiten.

Een anoniem informant van de nationale inlichtingendiensten had dit verhaal bevestigd aan de Amerikaanse krant *The Washington Post*. Het tijdschrift *Time* had de overloper van de KGB geïdentificeerd als een ex-medewerker van het Eerste Directoraat-generaal.

In oktober 1996 onthulde de Franse krant *Le Monde* dat de Britse inlichtingendiensten aan de DST een lijst hadden bezorgd met ongeveer 300 namen van diplomaten en ambtenaren die voor de Sovjet-Russische inlichtingendiensten zouden hebben gewerkt.

In december van hetzelfde jaar publiceerde de Duitse pers soortgelijke berichten. Hier werd beweerd dat de Britten hun inlichtingen hadden bezorgd aan de Duitse inlichtingendienst BfV, het *Bundesamt für Verfassungsschutz*.

In juli 1997 verscheen het verhaal van Mitrokhin in de Oostenrijkse pers, dit keer in verband met het bestaan van geheime bergplaatsen van explosieven.

In juli 1998 publiceerde het Duitse tijdschrift *Focus* het verhaal van de Russische ex-kolonel die in 1992 naar het Westen was overgelopen en handgeschreven informatie aan de Britse inlichtingendiensten had bezorgd.

Uit het antwoord van de Veiligheid van de Staat blijkt dat deze dienst pas op 11 juli 1995 kennis kreeg

(1) The Mitrokhin Archive, p. 19 en 20.

3.2. Les constatations et les commentaires du Comité R

3.2.1. Le retard dans la transmission des informations à la Sûreté de l'État et au SGR

On peut lire en substance dans l'ouvrage du professeur Christopher Andrew et de Vasili Mitrokhin (1) que ce dernier était arrivé en Angleterre le 7 septembre 1992. En août 1993 un auteur américain faisait déjà mention de l'affaire dans un livre intitulé *Federal Bureau of Investigation (FBI)*.

Il mentionnait le fait que les informations transmises par un ancien collaborateur du KGB concernant des centaines d'américains étaient tellement spécifiques que dès l'été 1993 dans la plupart des grandes villes américaines des agents du FBI avaient été mobilisés pour enquêter sur ces faits.

Le quotidien américain *The Washington Post* avait obtenu confirmation de ce récit par un informateur anonyme des services de renseignement nationaux et le périodique *Time* avait pour sa part identifié le transfuge du KGB comme étant un ex-collaborateur du premier directorat général.

En octobre 1996, le journal français *Le Monde* révélait que les services de renseignement britanniques avaient transmis à la DST une liste d'environ 300 noms de diplomates et de fonctionnaires qui auraient travaillé pour les services de renseignement soviétiques.

En décembre de la même année, des informations similaires paraissaient dans la presse allemande. Dans celles-ci, on situait la transmission de données par les britanniques au service de renseignement allemand, le BfV *Bundesamt für Verfassungsschutz*.

En juillet 1997, le récit de Mitrokhin paraissait à son tour dans la presse autrichienne et cette fois-ci en relation avec l'existence de caches d'explosifs.

En juillet 1998, le magazine allemand *Focus* publiait l'histoire de l'ex-colonel russe qui en 1992 passait à l'Ouest tout en transmettant aux services de renseignement britanniques des informations manuscrites.

Selon la réponse de la Sûreté de l'État, ce service ne fut informé que le 11 juillet 1995 de l'existence d'un

(1) The Mitrokhin Archive, pp. 19 et 20.

van het bestaan van een overloper, «die later werd vereenzelvigd als zijnde Mitrokhin.»

We stellen dus vast dat de Veiligheid van de Staat kennis kreeg van de feiten meer dan twee jaar nadat de Amerikanen (en volgens de krant *Le Monde* ook de Fransen) op de hoogte waren gebracht, en nadat daarvan melding werd gemaakt in een boek dat in 1993 in de Verenigde Staten verscheen.

De algemene context van de zaak was echter voor de Veiligheid van de Staat reeds duidelijk vanaf 1996. De identiteit van Mitrokhin daarentegen werd slechts vernomen door deze dienst via de Belgische pers waar de eerste artikelen pas verschenen in 1999, na de ontdekking van geheime bergplaatsen waarin zendapparatuur was opgeslagen.

Tijdens het onderhoud dat de leden van de Dienst Enquêtes hebben gehad met de aangestelde verantwoordelijke van de studiedienst van de Veiligheid van de Staat, is gebleken dat de betrokkene geen weet had van de eerklank die deze zaak vanaf 1993 in andere landen had gevonden in de media, en vanaf 1996 in de internationale pers.

Uit het bovenstaande kunnen we afleiden dat de Veiligheid van de Staat met vertraging en blijkbaar op beknopte wijze kennis kreeg van het bestaan van een overloper van de KGB.

Voorbijgaand aan de redenen die aan de basis zouden kunnen liggen van een dergelijke situatie en zonder vandaag kennis te hebben van de inhoud van de meegedeelde informatie en bijgevolg van het grote of minder grote belang ervan(1), kan het Comité I niet anders dan vaststellen dat de leden van de dienst contraspionage van de Veiligheid van de Staat heel weinig belangstelling voor deze zaak lijken te hebben getoond, in de veronderstelling dat ze pas na de interventie van de Belgische media kennis hebben gekregen van de precieze context van de zaak.

Uit de contacten van de Dienst Enquêtes van het Comité I met de persoon die bij de ADIV werd aangesteld om dit onderzoek te volgen, is gebleken, op één uitzondering na, dat de vertraging in het meedelen van interessante informatie in de praktijk geen negatieve gevolgen heeft gehad op militair vlak.

We benadrukken dat de Veiligheid van de Staat en de ADIV in staat zijn geweest een stand van zaken betreffende deze situatie op te maken in het kader van de uitvoering van het protocolakkoord dat deze

(1) Uit een eerste evaluatie door de Veiligheid van de Staat van een verzoek van het Comité I om toegang te krijgen tot de inhoud van deze informatie blijkt dat de «regel van de derde» ook van toepassing zou zijn jegens leden van het Comité I en zijn Dienst Enquêtes, hoewel ze een veiligheidsmachtiging van het niveau «heel geheim» bezitten. In deze context zou het Comité ook het bewijs moeten leveren van zijn «Need to Know».

transfuge «qui plus tard a été identifié comme étant Mitrokhin.»

Cette information intervient donc plus de deux ans après que les Américains (et selon le journal *Le Monde*, les français) furent mis au courant et après qu'un livre paru en août 1993 aux États-Unis en ait fait mention.

Si le contexte intégral de l'affaire était déjà connu de la Sûreté de l'État dès 1996, l'identité de Mitrokhin ne serait arrivée à la connaissance de ce service que par la presse belge dans laquelle les premiers articles ne sont apparus qu'en 1999, à la suite de la découverte des caches contenant des appareils émetteurs récepteurs.

Durant l'entretien que les membres du Service d'enquêtes ont eu avec le responsable désigné du service d'étude de la Sûreté de l'État, il est apparu que celui-ci n'était pas au courant des échos que cette affaire avait eus dans la presse des autres pays dès 1993 et dans la presse internationale à partir de 1996.

On peut déduire de ce qui précède que la Sûreté de l'État a été informée avec retard et d'une manière apparemment sommaire de l'existence d'un transfuge du KGB.

Au-delà des raisons qui pourraient être à la base d'une telle situation et sans avoir à ce jour connaissance du contenu des informations communiquées et donc de leur plus ou moins grand degré d'intérêt(1), force est de constater pour le Comité R que les membres du service contre-espionnage de la Sûreté de l'État semblent avoir montré un intérêt fort limité pour cette affaire, dans l'hypothèse où il a fallu attendre l'intervention des médias belges pour qu'ils soient mis au courant du contexte précis de celle-ci.

Il est apparu des contacts du Service d'enquêtes du Comité R avec le responsable désigné au SGR pour suivre cette enquête, qu'à une exception près, le retard dans la transmission d'informations intéressantes sur le plan militaire n'avait pas eu de conséquences négatives en pratique.

Il faut souligner que la Sûreté de l'État et le SGR ont été en mesure de faire le point sur cette situation dans le cadre de l'exécution du protocole d'accord qui les lie depuis 1997. Ils ont ainsi pu confronter et mettre à

(1) D'après une première évaluation par la Sûreté de l'État d'une demande du Comité R d'avoir accès au contenu de ces informations, il ressort que la «règle du tiers» s'appliquerait également à l'égard des membres du Comité R et de son Service d'enquêtes, malgré la possession par ceux-ci d'une habilitation de sécurité du niveau «très secret». Le Comité aurait également dans ce contexte à justifier de son «Need to Know».

diensten in 1997 hebben gesloten. Op die manier konden ze de onvolledige en verschillende informatie die ze hadden ontvangen, vergelijken en aanvullen.

3.2.2. Inhoud, waarde en exploitatie van de informatie

Uit de antwoorden die we van beide nationale inlichtingendiensten hebben ontvangen, blijkt dat de meegedeelde informatie niet uitsluitend betrekking had op de zaak van de geheime bergplaatsen van zendapparatuur, die de media in 1999 in ons land aan het licht brachten.

We moeten vaststellen dat, in strikte toepassing van de regel van de derde dienst, alleen de informatie die de ADIV als relevant beschouwt met betrekking tot de bergplaatsen van communicatietoestellen kon worden bezorgd aan de gerechtelijke overheden(1), na het voorafgaand akkoord van de dienst die deze informatie had verstrekt. De ADIV en de Veiligheid van de Staat zelf konden de informatie die ze respectievelijk van dezelfde derde dienst hadden ontvangen pas uitwisselen na hetzelfde soort voorafgaande toestemming te hebben verkregen.

De overige inlichtingen, waarvan het belang, gelet op hun ouderdom (ouder dan 1985), door de ADIV en de Veiligheid van de Staat historisch(2) wordt genoemd, werden of worden momenteel niet meer geëxploiteerd. Ze werden evenmin meegedeeld aan Belgische of buitenlandse bestemmelingen, met uitzondering van de inlichtingendiensten die bij deze zaak betrokken zijn.

We preciseren echter dat de Veiligheid van de Staat in sommige gevallen een onderzoek heeft verricht en dat deze dienst de resultaten daarvan aan een geallieerde inlichtingendienst heeft bezorgd.

4. Besluiten en aanbevelingen

In de eerste plaats maakt dit onderzoek duidelijk hoe complex het probleem van de uitwisseling van informatie binnen de nationale en internationale

(1) Er moest inderdaad rekening worden gehouden met de eventuele aanwezigheid van explosieven die een gevaar vormden voor de openbare veiligheid.

(2) In verband hiermee benadrukt het Comité I dat in deze veronderstelling de bepalingen van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten eventueel hadden moeten worden toegepast. Dit artikel bepaalt: «Persoonsgegevens verwerkt in het kader van de toepassing van huidige wet worden bewaard voor een duur die niet langer mag zijn dan die welke noodzakelijk is om de doeleinden waarvoor ze worden opgeslagen, met uitzondering van de gegevens die een door het Rijksarchief erkend historisch karakter hebben.»

Zie in verband hiermee ook de jaarverslagen van het Comité I van 1996, p. 97, 1997, p. 11 en 1999, p. 97 betreffende de bestemming van de archieven van onze inlichtingendiensten.

jour les informations partielles et différentes qu'ils avaient réciproquement reçues.

3.2.2. Le contenu, la valeur et l'exploitation des informations

Il ressort des réponses apportées par les deux services de renseignement nationaux que les informations transmises ne concernaient pas uniquement l'affaire des caches de matériel de transmission révélée dans notre pays par les médias en 1999.

Il convient de constater qu'en application stricte de la règle du service tiers, seules les informations qualifiées de pertinentes par le SGR concernant les caches d'appareils de communications ont pu être communiquées aux autorités judiciaires(1) après avoir reçu l'accord préalable du service qui avait fourni les informations. Le SGR et la Sûreté de l'État n'ont eux-mêmes pu échanger les informations qu'ils avaient respectivement reçues du même service tiers qu'après avoir obtenu le même type d'autorisation préalable.

Aucune des autres informations, pour lesquelles, vu leur ancienneté (antérieures à 1985), l'intérêt est qualifié d'historique(2) par le SGR et la Sûreté de l'État, n'a été, ni n'est encore exploitée actuellement. Celles-ci n'ont pas davantage fait l'objet de communication à des destinataires belges ou étrangers, autres que les services de renseignement concernés par la présente affaire.

Il convient toutefois de noter que des enquêtes ont été faites par la Sûreté de l'État dans quelques cas et que les résultats en ont été communiqués à un service de renseignement allié.

4. Conclusions et recommandations

Sous différents aspects, c'est la complexité de la problématique de l'échange des informations au sein de la communauté nationale et internationale du

(1) Il fallait en effet tenir compte de la présence éventuelle d'explosifs présentant un danger pour la sécurité publique.

(2) À ce sujet, le Comité R souligne que dans cette hypothèse les dispositions de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité trouveraient éventuellement à s'appliquer. Cet article dispose que: «Les données à caractère personnel traitées dans le cadre de l'application de la présente loi sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées, à l'exception de celles présentant un caractère historique, reconnu par les archives de l'État. .. »

Voir également à ce sujet les rapports annuels du Comité R de 1996, p. 97, 1997, p. 11 et 1999, p. 97 concernant la destruction des archives par nos services de renseignements.

inlichtingengemeenschap is; hetzelfde geldt voor het meedelen van gegevens, onbewerkt of na analyse, aan andere autoriteiten en andere overheden (in het bijzonder aan de gerechtelijke en de politieke overheid)(1).

Dit onderzoekt toont aan dat de toepassing van «de regel van de derde of van de derde dienst», die aan de basis ligt van de internationale samenwerking tussen de inlichtingendiensten, verbiedt dat inlichtingen zonder het voorafgaand akkoord van de dienst die deze inlichtingen heeft verstrekt, worden meegedeeld aan de nationale politieke en gerechtelijke overheden van het land dat de inlichtingen ontvangt(2).

In het huidige geval zal men deze situatie wellicht rechtvaardigen met het feit dat deze inlichtingen niet langer actueel waren (ouder dan 1985), dat eventuele inbreuken — voor zover ze al konden worden bewezen — verjaard waren, dat ze dus enkel historische waarde hadden en dat er in de praktijk dan ook geen enkel bezwaar was om op deze manier te handelen. Waarom echter wordt het embargo op deze inlichtingen zoveel later nog steeds gerechtvaardigd?

Kan men er zeker van zijn, rekening houdend met het belang van de bovengenoemde regel, dat er anders zou worden gehandeld indien bepaalde inlichtingen grotere actuele waarde zouden hebben?

(1) Blijkbaar gaat het niet om een typisch Belgisch probleem. De krant *«Le Monde»* van 15 september 1999 schreef met betrekking tot de zaak-Mitrokhin: «De conservatieve oppositie in het Verenigd Koninkrijk stelde de vraag waarom de contraspionagediensten het niet nodig vonden beide regeringen kennis te geven van dit heel bijzonder geval, en waarom het Parlement pas op de hoogte werd gebracht na de publieke onthullingen van een professor in Cambridge». Nog steeds in verband met het niet meedelen van informatie door de Britse inlichtingendiensten aan de politieke overheden in deze context, lezen we in hetzelfde artikel: «Heeft de MI5 (Britse dienst voor contraspionage) in de zaak-Norwood misbruik gemaakt van zijn rechten? Kan deze dienst zijn rechten behouden zonder een strengere controle op zijn activiteiten vanwege het Parlement? Dit is de inzet van het debat dat onlangs werd geopend, en het is tevens de reden waarom de parlementaire commissie belast met het toezicht op de inlichtingendiensten zopas de opdracht kreeg een grondiger onderzoek te voeren naar alle raadsels van deze Koude Oorlog, die opnieuw komt rondspoken in het Groot-Brittannië van het jaar 2000.»

(2) Het is interessant vast te stellen dat de regel van de «derde» dienst een expliciete toepassing vindt in de formulering van het 2e lid van artikel 5, § 3 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen:
«Op verzoek van de inlichtingen- en veiligheidsdienst kan het beroepsorgaan beslissen dat sommige inlichtingen uit de verklaring van een lid van de in § 2 bedoelde inlichtingendienst, uit het onderzoeksverslag of het onderzoeksdossier, om een van de in § 2 vierde lid, genoemde redenen, geheim zijn en dat de eiser noch zijn advocaat er inzage van krijgen.
Wanneer die inlichtingen afkomstig zijn van een buitenlandse inlichtingendienst, wordt de beslissing tot niet-inzage genomen door de inlichtingen- en veiligheidsdienst».

renseignement, ainsi que la communication des données soit sous une forme brute, soit après analyse à d'autres autorités et à d'autres pouvoirs (notamment le pouvoir judiciaire et le pouvoir politique) qui est en premier lieu mise en évidence par la présente enquête(1).

Celle-ci montre que l'application de «la règle du tiers ou du service tiers» qui fonde la collaboration internationale entre les services de renseignement interdit, que sans autorisation préalable du service qui a donné les informations, celles-ci soient communiquées aux autorités politiques et judiciaires nationales du pays qui les reçoit(2).

Dans le cas d'espèce, on justifiera sans doute cette situation par le fait que ces informations n'étaient plus d'actualité (antérieures à 1985), que d'éventuelles infractions — pour autant qu'elles eussent pu être prouvées — étaient prescrites, qu'elles n'avaient donc qu'un intérêt historique et qu'il n'y a donc eu en pratique aucun inconvénient à agir de la sorte. Mais pourquoi l'embargo sur ces informations se justifie-t-il encore aussi longtemps après?

Compte tenu de l'importance de la règle précitée, peut-on être assuré qu'il en serait autrement dans le cas d'informations présentant un plus grand intérêt actuel?

(1) Le problème n'est semble-t-il pas propre à la Belgique, puisque d'après le journal *«Le Monde»* du 15 septembre 1999 se penchant sur l'affaire Mitrokhin: «l'opposition conservatrice au Royaume-Uni a demandé pourquoi les services de contre-espionnage n'ont pas cru devoir informer les deux gouvernements de ce cas très particulier et pourquoi le Parlement n'est-il informé qu'après les révélations publiques d'un professeur de Cambridge.» Parlant d'informations non communiquées par les services de renseignement britanniques aux autorités politiques dans ce contexte, le même article mentionne encore: «Dans l'affaire Norwood, le MI 5 (service de contre-espionnage britannique) a-t-il abusé de ses droits? Doit-il les conserver sans un contrôle plus étroit de ses activités par les élus? C'est tout l'enjeu du débat qui vient de s'ouvrir et c'est pourquoi la commission parlementaire en charge de la surveillance des services de renseignement vient de se voir confier mission d'enquêter plus à fond sur tous les mystères de cette guerre froide qui revient hanter la Grande-Bretagne de l'an 2000.»

(2) Il est intéressant de noter que la règle du service «tiers» trouve une application explicite dans le libellé du 2e alinéa de l'article 5, § 3 de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité:
À la demande du service de renseignement et de sécurité, l'organe de recours peut décider que certaines informations figurant dans la déposition d'un membre du service de renseignement visé au § 2, dans le rapport d'enquête ou dans le dossier d'enquête sont secrètes pour un des motifs visés au § 2, alinéa 4, et qu'elles ne pourront être consultées ni par le requérant ni par son avocat.
Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité.»

Anderzijds kan men niet ontkennen dat de samenwerking met internationale inlichtingendiensten absoluut noodzakelijk is om bij te dragen tot het garanderen van de doeltreffendheid waarmee de Veiligheid van de Staat en de ADIV hun wettelijke opdrachten moeten vervullen, en dat «de regel van de derde», die niet meer dan een voorbeeld is van de bescherming die aan informatiebronnen moet worden geboden, op dit vlak een beginsel is waar men niet omheen kan.

Er moet echter rekening worden gehouden met de nationale wetsbepalingen, die vandaag het principe bekrachtigen van het meedelen van gegevens door de inlichtingen- en veiligheidsdiensten aan andere diensten en overheden, alsook het principe van de bescherming van deze gegevens door de classificatie en het principe van de samenwerking tussen de diensten.

Artikel 19, eerste lid, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten bepaalt: «De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten, alsook aan de instanties en personen die het voorwerp zijn van een bedreiging bedoeld in de artikelen 7 en 11».

Het principe van de samenwerking tussen de diensten, niet alleen op nationaal maar ook op internationaal niveau, wordt dan weer geregeld door artikel 20, § 1 van dezelfde wet: «De inlichtingen- en veiligheidsdiensten, de politiediensten, de administratieve en gerechtelijke overheden zorgen voor een zo doeltreffend mogelijke wederzijdse samenwerking. De inlichtingen- en veiligheidsdiensten zorgen er eveneens voor dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten.»

En § 3 van artikel 20 bepaalt: «Het Ministerieel Comité bepaalt de in artikel 19, eerste lid, bedoelde voorwaarden waaronder de inlichtingen worden meegedeeld en de voorwaarden van de in §1 van dit artikel bedoelde samenwerking.»

Met betrekking tot de bescherming van de inlichtingen vaardigt de wet betreffende de classificatie, in haar artikel 8, het verbod uit «betreffende de toegang tot geclassificeerde informatie, documenten of gegevens, materieel, materialen of stoffen» voor de persoon die «geen houder is van een overeenstemmende veiligheidsmachtiging» en die «er geen behoefte aan heeft er kennis van te nemen en er toegang toe te hebben voor de uitoefening van zijn functie of zijn opdracht, onverminderd de eigen bevoegdheden van de gerechtelijke overheden».

Het Comité I meent dat deze nieuwe bepalingen van aard zijn in de praktijk oplossingen aan te reiken

Il est indéniable d'autre part que la collaboration avec les services de renseignement internationaux est indispensable pour contribuer à assurer l'efficacité avec laquelle la Sûreté de l'État et le SGR doivent remplir leurs missions légales et que «la règle du tiers» qui n'est qu'un exemple de la protection à accorder aux sources d'informations, constitue dans ce domaine un principe incontournable.

Il convient toutefois de tenir compte des dispositions légales nationales qui consacrent aujourd'hui le principe de la communication des données par les services de renseignement et de sécurité à d'autres services et autorités, celui de la protection de ces données par la voie de la classification, ainsi que le principe de la coopération entre les services.

C'est ainsi que la loi du 30 novembre 1998 organique des services de renseignement et de sécurité prévoit en son article 19 alinéa 1er que: «Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes, conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11».

Le principe de la coopération entre les services, aussi bien au niveau national qu'international, est prévu quant à lui par l'article 20, § 1er de la même loi: « Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une collaboration avec les services de renseignement et de sécurité étrangers.»

Le § 3 de l'article 20 précité édicte que: «Le Comité ministériel du renseignement définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article.»

En ce qui concerne la protection des informations, la loi relative à la classification édicte en son article 8 l'interdiction «à l'accès aux informations, documents ou données, au matériel, aux matériaux ou matières classifiées» à la personne qui «n'est pas titulaire d'une habilitation de sécurité correspondante» et qui «n'a pas besoin d'en connaître et d'y avoir accès pour l'exercice de sa fonction ou de sa mission, sans préjudice des compétences propres des autorités judiciaires».

Le Comité R estime que ces nouvelles dispositions sont de nature à apporter dans la pratique des solu-

voor meer en wellicht ook voor een betere communicatie tussen de nationale inlichtingendiensten en andere diensten en overheden, voor zover de natuurlijke bestemmelingen van geclassificeerde informatie zo nodig de passende maatregelen nemen om aan de wettelijke vereisten te voldoen, en op die manier toegang kunnen krijgen tot deze gegevens om de beslissingen te nemen die eigen zijn aan hun domein van bevoegdheid en soevereiniteit, waarbij ze indien dat past de bescherming van deze gegevens blijven verzekeren.

Het principe van het meedelen van gegevens, dat door de wetgever wordt bekrachtigd, leidt immers niet automatisch tot het gebruik daarvan in de staat waarin ze zich bevinden (bijvoorbeeld in het kader van een gerechtelijke procedure) of tot hun openbare verspreiding.

In deze optiek, en in het kader van de hierboven aangehaalde principes die de wetgever heeft ontwikkeld, vraagt het Comité I zich af, gelet op een praktijk zoals die naar voren komt uit het huidige onderzoek en uit de algemene context beschreven in punt 2.1.3. hierboven, of er niet alleen op nationaal maar wellicht ook op Europees en internationaal vlak moet worden nagedacht, in het bijzonder over de toepassing van «de regel van de derde» en het toezicht daarop. In sommige opzichten zou deze toepassing immers kunnen leiden tot een verkeerde interpretatie die samenhangt met een bepaalde cultuur van het geheim of zelfs, in extreme gevallen, tot een verkeerd gebruik.

Al vormt een vergelijking nog geen reden, het Comité I kan niet anders dan verwijzen naar de recente ongelukkige ervaring met bepaalde gerechtelijke zaken. Daaruit is gebleken hoe belangrijk het is dat de informatie goed wordt beheerd. Dit betekent onder meer dat de gegevens optimaal en tijdig worden meegedeeld. Moeten we herinneren aan de nadelige en soms tragische gevolgen waartoe disfuncties in deze sector aanleiding kunnen geven?

Het tweede punt dat het Comité I uit het huidige onderzoek onthoudt, is dat uit de verklaringen van de verantwoordelijken van de Veiligheid van de Staat zelf blijkt (zie punt 2.4 hierboven) dat er sprake was van een neerwaartse evaluatie van de activiteiten inzake spionage, die tot gevolg heeft gehad dat minder middelen werden ingezet op het vlak van contraspionage. Uiteindelijk hebben de feiten deze evaluatie tegengesproken.

Om het belang van deze vaststelling te benadrukken, herinneren we eraan dat de gewezen administrateur van de Veiligheid van de Staat op 9 oktober 1999 aan de *«Financieel Economische Tijd»* verklaarde: «De Staatsveiligheid beschikt over aanwijzingen dat de voorbije jaren buitenlandse inlichtingendiensten in België aan economische en industriële spionage deden».

tions à une plus grande et sans doute à une meilleure communication entre les services de renseignement et les autres services et autorités nationales, pour autant que les destinataires naturels d'informations classifiées prennent, si nécessaire, les mesures appropriées pour répondre aux exigences de la loi, et puissent ainsi avoir accès à ces données pour prendre les décisions propres à leur domaine de compétence et de souveraineté tout en continuant, s'il échet, à assurer la protection de ces données.

Le principe de la communication des données consacré par le législateur n'implique pas en effet automatiquement l'usage en l'état de celles-ci (par exemple dans une procédure judiciaire) ou leur diffusion publique.

Dans cette optique, et dans le cadre des principes dégagés par le législateur qui viennent d'être rappelés, le Comité R se demande si, au vu d'une pratique telle qu'elle apparaît de la présente enquête et du contexte général décrit ci-dessus au point 2.1.3., une réflexion, tant sur le plan national que peut être aussi sur le plan européen et international, ne devrait pas être mise en ouvre, concernant notamment l'application de «la règle du tiers» et de son contrôle, dans la mesure où cette application pourrait, à certains égards, être susceptible d'une mauvaise interprétation liée à une certaine culture du secret ou même, dans des cas extrêmes, d'un mauvais usage.

Si comparaison n'est pas raison, le Comité R ne peut rester sans rappeler l'expérience malheureuse récente de certaines affaires judiciaires, qui a mis en évidence l'importance d'une bonne gestion des informations comprenant entre autres une communication optimale et en temps utile des données. Faut-il rappeler les conséquences dommageables et parfois dramatiques qui peuvent résulter de dysfonctionnements dans ce secteur?

Le second point que le Comité R retient de la présente enquête est qu'il y a eu de l'aveu même des responsables de la Sûreté de l'État (voir point 2.4 ci-dessus p. 84 *in fine*) une évaluation à la baisse de l'évolution des activités d'espionnage qui a entraîné une diminution des moyens consacrés au contre-espionnage. Cette évaluation a été finalement démentie dans les faits.

Pour souligner l'importance de ce constat, rappelons que l'ancien administrateur de la Sûreté de l'État déclarait le 9 octobre 1999 au *«Financieel Economische Tijd»* que: «La Sûreté de l'État disposait d'indices selon lesquels au cours des années précédentes des services de renseignement étrangers se livraient en Belgique à de l'espionnage économique et industriel.»

Hij voegde eraan toe :

« Over deze economische oorlog, ook wel de vergeten oorlog genoemd, zwijgt iedereen. In de zes jaar dat ik aan het hoofd van de Staatsveiligheid stond, stelde geen enkele buitenlandse mogendheid voor om over dit onderwerp een werkvergadering te organiseren. »

Hij voegde er verder nog aan toe, met betrekking tot dit specifieke gebied :

« Ook in het Europa van het jaar 2000 blijven nationale belangen een belangrijke rol spelen, en men moet niet verwachten dat dit de komende jaren verandert... »

In een artikel dat op 8 maart 2001 verscheen in de Franse krant *« Le Monde »* schreef Jacques Isnard :

« Het einde van de Koude Oorlog tussen het Oosten en het Westen heeft geen einde gesteld aan de activiteiten van spionnen op onze planeet... Na 1989 en de val van de Berlijnse Muur is er een — heel tijdelijke — vertraging geweest op het vlak van spionage. Het uiteenvallen van de Sovjet-Unie, vanaf 1991, en de aantrekking die de landen van het voormalige Oostblok op de NAVO uitoefenen, hebben de machine opnieuw aan het rollen gebracht, zoals blijkt uit de zaken die zich momenteel afspelen in Rusland en de Verenigde Staten » (1)

Dezelfde auteur vat de huidige situatie als volgt samen :

« Vandaag geeft eender welke Staat aan zijn inlichtingendiensten de opdracht niet zozeer militaire of zelfs operationele inlichtingen te verzamelen, maar wel informatie op het vlak van de politiek, van internationale financiën, handel, industrie en, vooral, geavanceerde technologie. Het komt erop aan, op clandestiene wijze, door het stelen van documenten, het intercepteren van communicatie of door middel van corruptie technologisch voordeel te behalen, met civiele en strategische doeleinden, tegen een zo laag mogelijke prijs, dat wil zeggen zonder buitensporige

(1) Het is interessant vast te stellen dat de regel van de « derde » dienst een expliciete toepassing vindt in de formulering van het 2e lid van artikel 5, § 3 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen :
« Op verzoek van de inlichtingen- en veiligheidsdienst kan het beroepsorgaan beslissen dat sommige inlichtingen uit de verklaring van een lid van de in § 2 bedoelde inlichtingendienst, uit het onderzoeksverslag of het onderzoeksdossier, om een van de in § 2 vierde lid, genoemde redenen, geheim zijn en dat de eiser noch zijn advocaat er inzage van krijgen.
Wanneer die inlichtingen afkomstig zijn van een buitenlandse inlichtingendienst, wordt de beslissing tot niet-inzage genomen door de inlichtingen- en veiligheidsdienst ».

Il ajoutait même :

« Concernant cette guerre économique, appelée également la guerre oubliée, tout le monde se tait. Durant les six années passées à la tête de la Sûreté de l'État, jamais aucune puissance étrangère n'a proposé d'organiser à ce sujet une réunion de travail. »

Il ajoutait concernant ce domaine particulier :

« Dans l'Europe de l'an 2000 les intérêts nationaux continuent à jouer un rôle important et l'on ne doit pas s'attendre à ce que cela change dans les années à venir... »

Dans un article paru dans le journal français *« Le Monde »* du 8 mars 2001, Jacques Isnard rappelle que :

« La fin de la guerre froide Est-Ouest n'a pas mis un terme aux activités des espions de tout poil sur la planète... Après 1989 et la chute du mur de Berlin, l'espionnage s'est — très momentanément — ralenti. L'implosion de l'ex-URSS, à partir de 1991, et l'attrait des pays de l'ancien « bloc » de l'Est pour l'Otan ont relancé la machine comme en témoignent les affaires en cours qui ont la Russie et les États-Unis pour théâtre » (1).

Le même auteur résume encore ainsi la situation actuelle :

« Tous États confondus, les services partent aujourd'hui en quête d'informations qui relèvent moins du militaire, voire de l'opérationnel que du politique, de la finance internationale, du commerce, de l'industrie et, surtout, de la haute technologie. Il s'agit d'assurer, de façon clandestine, par le vol de documents, l'interception des communications ou par la corruption, des gains technologiques, à des fins civiles et stratégiques, au moindre prix, c'est-à-dire sans devoir débourser des sommes excessives dans l'ordre des études de la recherche ou d'une technique

(1) Il est intéressant de noter que la règle du service « tiers » trouve une application explicite dans le libellé du 2e alinéa de l'article 5, § 3 de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité :
À la demande du service de renseignement et de sécurité, l'organe de recours peut décider que certaines informations figurant dans la déposition d'un membre du service de renseignement visé au § 2, dans le rapport d'enquête ou dans le dossier d'enquête sont secrètes pour un des motifs visés au § 2, alinéa 4, et qu'elles ne pourront être consultées ni par le requérant ni par son avocat.
Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité. »

bedragen te moeten uitgeven aan zogeheten «spits-technologische» studies, onderzoek of technieken. De ideologie is niet langer een reden om aan spionage te doen, zoals ten tijde van de Koude Oorlog. Men spioneert om tijd en geld te besparen, door zich de ontdekkingen toe te eigenen van landen waarvan men meent dat ze al verder staan op het vlak van technologische ontwikkelingen» (1).

Het Comité I beveelt aan om in het bijzonder in deze materie de vereiste middelen toe te kennen aan de Veiligheid van de Staat, teneinde deze dienst toe te laten zo doeltreffend mogelijk te werken in het kader van een voor deze dienst specifieke opdracht: contraspionage op economisch en industrieel gebied.

Deze aanbeveling steunt op de vaststelling dat, voortgaand op de verklaringen van de gewezen administrateur-generaal van de Veiligheid van de Staat en op de bovengenoemde analyse, de nationale diensten op het vlak van de bescherming van het economisch potentieel blijkbaar niet kunnen rekenen, zoals dat wel het geval lijkt te zijn op andere gebieden (terrorisme, proliferatie, enz.), op het uitwisselen van inlichtingen met andere buitenlandse diensten, zelfs indien het gaat om geallieerde diensten, in Europa of elders.

Het derde en laatste punt dat het Comité I wil aanhalen in het kader van de vaststellingen van het huidige onderzoek, heeft betrekking op het belang van open bronnen. Uit de vaststellingen van de Dienst Enquêtes van het Comité I blijkt niet dat de Veiligheid van de Staat de open bronnen op behoorlijke wijze exploiteert. Het Comité I herhaalt wat het reeds verklaarde in zijn activiteitenverslag 1996, naar aanleiding van de conclusies van een congres te Brussel over open bronnen: Nu een einde is gekomen aan de Koude Oorlog, worden de diensten geconfronteerd met nieuwe prioriteiten, zoals het delicate probleem van economische spionage.

Met betrekking tot de werking van de inlichtingendiensten op dit vlak stelde het Comité I vast:

«Steeds meer inlichtingen zijn in het openbaar beschikbaar, en bijgevolg heeft het geen enkele zin om bepaalde documenten bijvoorbeeld als «geheim» te classificeren. Veel deelnemers aan het congres zijn voorstander van het declassificeren van informatie en van een grotere transparantie van de werking van de inlichtingendiensten. De beste manier om de voorsprong op zijn tegenstander te behouden bestaat erin snel te handelen, want alleen de informatie die wordt geanalyseerd en verwerkt is nuttig.»

(1) Vrije vertaling.

dits de «pointe». L'idéologie n'est plus guère un motif d'espionner, comme du temps de la guerre froide. On espionne pour économiser du temps et de l'argent, en s'appropriant des découvertes des pays censés être les plus avancés» (1).

Le Comité R recommande qu'en cette matière particulièrement les moyens nécessaires soient donnés à la Sûreté de l'État pour lui permettre d'assurer un maximum d'efficacité dans le cadre d'une mission qui lui est spécifique: le contre-espionnage en matière économique et industrielle.

Cette recommandation est appuyée par la constatation qu'apparemment, si l'on se base sur les propos de l'ancien administrateur-général de la Sûreté de l'État, ainsi que sur l'analyse citée ci-dessus, en matière de défense du potentiel économique les services nationaux ne peuvent pas compter, comme cela semble être le cas dans les autres domaines (terrorisme, prolifération, etc..), sur un échange d'informations avec les autres services étrangers, même si ce sont d'autre part des services alliés, européens ou non.

Le troisième et dernier point que le Comité R tient à mettre en évidence au vu des constatations de la présente enquête est celui de l'importance des sources ouvertes. Une bonne exploitation de celles-ci par la Sûreté de l'État n'apparaît pas des constatations faites par le Service d'enquêtes du Comité R. Celui-ci rappelle ce qu'il mentionnait déjà dans son rapport d'activités de 1996 lorsqu'il rapportait les conclusions d'un congrès organisé à Bruxelles sur les sources ouvertes: À l'heure où la guerre froide a pris fin, les services se voient confrontés à de nouvelles priorités, tel que le problème délicat de l'espionnage économique.

Concernant à ce sujet le fonctionnement des services de renseignement le Comité R notait:

«De plus en plus d'informations sont publiquement disponibles, et en conséquence la tendance à classifier des documents «secrets» par exemple, est dépourvue de sens. Nombreux sont ceux qui, parmi les participants à ce congrès, prônent la déclassification d'informations et une plus grande transparence du fonctionnement des services de renseignement. Le meilleur moyen pour garder l'avantage sur son adversaire est de réagir vite, car seule l'information faisant l'objet d'une analyse et d'un traitement est utile.»

(1) Traduction libre.

HOOFDSTUK 3

VERSLAG VAN HET ONDERZOEK NAAR DE WIJZE WAAROP DE ADIV IS OMGEGAAN MET DE INFORMATIE OVER DE MILITAIRE SITUATIE IN KOSOVO

1. Inleiding

In haar editie van 22 oktober 1999 («België beducht voor Servische invasie in Kosovo») berichtte de krant *De Morgen* over een mededeling van de minister van Landsverdediging aan de Ministerraad van 24 september 1999.

In het artikel stond te lezen dat de minister over inlichtingen beschikte van het KFOR-opperbevel, dat rekening hield met een nakende inval van het Servische leger en de Servische politie in Kosovo.

Bijgevolg had hij gevraagd een *worst case scenario* te voorzien voor de 1 100 Belgische soldaten op missie in deze regio. Nog steeds volgens *De Morgen* leek de woordvoerder van de Belgische strijdkrachten in Kosovo deze informatie echter niet ernstig te nemen.

Bovendien kon men zich afvragen, gelet op de opeenvolgende tegenstrijdige berichten in de pers, of de NAVO, het ministerie van Landsverdediging en het bevel van de Belgische troepen in Kosovo over dezelfde informatie beschikten met betrekking tot de militaire situatie in deze regio.

In het kader van haar opdracht van toezicht op de coördinatie en de doeltreffendheid van de inlichtingendiensten, heeft het Comité I zich afgevraagd hoe de ADIV omging met de informatie over de militaire situatie in Kosovo, en hoe deze dienst op dit vlak samenwerkte met de Veiligheid van de Staat.

2. Procedure

Op maandag 8 november 1999 besliste het Comité I een onderzoek te openen naar de manier waarop de ADIV de informatie over de militaire situatie in Kosovo had beheerd.

Op 10 november 1999 richtte de voorzitter van het Comité I een kantschrift aan het hoofd van de Dienst Enquêtes.

Overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten werd de voorzitter van de Senaat op 18 november 1999 op de hoogte gebracht van de opening van dit onderzoek.

Overeenkomstig artikel 43.1 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten werd de minister van Landsverdedi-

CHAPITRE 3

RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LE SGR A GÉRÉ L'INFORMATION SUR LA SITUATION MILITAIRE AU KOSOVO

1. Introduction

Le journal «*De Morgen*» du 22 octobre 1999 («België beducht voor Servische invasie in Kosovo») a fait état d'une communication du ministre de la Défense nationale, André Flahaut, au Conseil des ministres du 24 septembre 1999.

Selon l'article, le ministre possédait des informations du commandement de la KFOR qui n'excluaient pas une prochaine invasion du Kosovo par l'armée et la police serbes.

En conséquence de quoi, il avait demandé de mettre en place un *worst case scenario* à l'intention des 1 100 soldats belges en mission dans cette région. Toujours selon «*De Morgen*», le porte-parole des forces belges au Kosovo ne semblait toutefois pas prendre cette information au sérieux.

Par ailleurs, une succession de communiqués contradictoires dans la presse posait la question de savoir si l'OTAN, le ministre de la Défense nationale et le commandement des troupes belges au Kosovo disposaient des mêmes informations sur la situation militaire dans cette région.

Dans le cadre de sa mission de contrôle portant sur la coordination et l'efficacité des services de renseignement, le Comité permanent R s'est demandé comment le SGR gérait l'information sur la situation militaire au Kosovo et comment il collaborait avec la Sûreté de l'État sur ce sujet.

2. Procédure

Le Comité permanent R a donc décidé le lundi 8 novembre 1999 d'ouvrir une enquête sur la manière dont le SGR avait géré l'information sur la situation militaire au Kosovo.

Le 10 novembre 1999, le président du Comité R a adressé une apostille au chef du Service d'enquêtes.

Le président du Sénat a été informé de l'ouverture de cette enquête le 18 novembre 1999 conformément à l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le ministre de la Défense nationale a été informé de l'ouverture de cette enquête le 24 novembre 1999 conformément à l'article 43.1 de la loi du 18 juillet

ging op 24 november 1999 op de hoogte gebracht van de opening van dit onderzoek.

In februari 2000 heeft de Dienst Enquêtes van het Comité I een aantal verhoren afgenomen bij de ADIV. Op 27 maart 2000 heeft deze dienst zijn verslag aan het Comité I bezorgd.

Op 29 mei 2000 richtte het Comité I opnieuw een kantschrift aan de Dienst Enquêtes met het verzoek bij de Veiligheid van de Staat na te gaan hoe deze dienst met de ADIV had samengewerkt in het kader van de problematiek in Kosovo.

Op 30 mei 2000 werd de minister van Justitie, overeenkomstig artikel 43.1 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, op de hoogte gebracht van het feit dat het onderzoek was uitgebreid tot de Veiligheid van de Staat.

In juni 2000 heeft de Dienst Enquêtes van het Comité I een aantal verhoren afgenomen bij de Veiligheid van de Staat. Op 26 juni 2000 heeft deze dienst zijn verslag aan het Comité I bezorgd.

Het onderhavige rapport werd goedgekeurd op 26 september 2000.

De minister van Landsverdediging liet op 11 januari 2001 schriftelijk weten dat het huidig verslag als dusdanig kon opgenomen worden in het activiteitenverslag 2000 van het Comité I.

3. Vaststellingen en besluiten

Gelet op de bijzonder geheime aard van de inlichtingenoperaties met betrekking tot de opdracht van KFOR in Kosovo, is het voor het Comité I onmogelijk om operationele informatie hierover openbaar te maken.

Uit de vaststellingen van de Dienst Enquêtes blijkt dat de ADIV, gedurende de periode die het voorwerp is van het onderhavige onderzoek, met de hulp van geallieerde diensten, het risico van een inval van het Joegoslavische leger in Kosovo concreet heeft kunnen beoordelen. Er werd rekening gehouden met dit risico, ook al oordeelde men dat het risico klein was.

De situatie werd onafgebroken geëvalueerd en de ADIV heeft nauwlettend toegekeken op eender welk element teneinde op dit risico te kunnen anticiperen en aldus de Belgische strijdkrachten en de geallieerden toe te laten om tijdig te reageren.

De Veiligheid van de Staat en de ADIV hebben elkaar voortdurend informatie hierover bezorgd. Overeenkomstig het bestaande protocol tussen beide diensten hebben ze gemeenschappelijke vergaderingen georganiseerd waarop de risico's werden geanalyseerd.

Regelmatig werden ook informatienota's bezorgd aan de politieke verantwoordelijken van het land,

1991 organique du contrôle des services de police et de renseignements.

Le Service d'enquêtes du Comité permanent R a procédé à des auditions au SGR dans le courant du mois de février 2000. Il a remis son rapport au Comité le 27 mars 2000.

Le 29 mai 2000, le Comité permanent R a adressé une nouvelle apostille au Service d'enquêtes pour lui demander de vérifier auprès de la Sûreté de l'État comment ce service avait collaboré avec le SGR dans le cadre de la problématique du Kosovo.

Le 30 mai 2000, conformément à l'article 43.1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le ministre de la Justice a été informé que l'enquête était étendue à la Sûreté de l'État.

Le Service d'enquêtes du Comité permanent R a procédé à des auditions à la Sûreté de l'État dans le courant du mois de juin 2000. Il a remis son rapport au Comité le 26 juin 2000.

Le présent rapport a été approuvé le 26 septembre 2000.

Par lettre du 11 janvier 2001, le ministre de la Défense nationale a fait savoir au Comité R que le présent rapport pouvait figurer tel quel dans le rapport annuel.

3. Constatations et conclusions

La nature particulièrement secrète des opérations de renseignements en rapport avec la mission de la KFOR au Kosovo ne permet pas au Comité permanent R de rendre publique la moindre information opérationnelle à ce sujet.

Il ressort des constatations du Service d'enquêtes que, pendant la période couverte par la présente enquête, le SGR a été en mesure, avec l'aide de services alliés, d'évaluer concrètement le risque d'invasion du Kosovo par l'armée yougoslave. Bien que considéré comme faible, le risque a été pris en compte.

L'évaluation de la situation était permanente et le SGR est resté attentif à tout élément de nature à anticiper ce risque, de manière à permettre aux forces armées belges et aux alliés de réagir en temps utile.

La circulation d'informations sur ce sujet a été fournie et constante entre la Sûreté de l'État et le SGR. Des réunions communes d'analyse des risques ont été organisées entre ces deux services conformément à ce qui est prévu dans leur protocole d'accord.

Des notes d'informations ont été régulièrement adressées aux responsables politiques du Royaume

teneinde hen toe te laten hun verantwoordelijkheid op te nemen met kennis van zaken.

HOOFDSTUK 4

VERSLAG VAN HET ONDERZOEK NAAR DE WIJZE WAAROP DE ADIV IS OMGEGAAN MET DE INFORMATIE OVER DE ALGEMENE SITUATIE IN KOSOVO

1. Inleiding

Het Comité I nam kennis van een artikel dat verscheen in de krant «*Le Soir*» van vrijdag 12 november 1999, met als titel: «Au Kosovo, les belges surveillent sans punir.»

De aandacht van het Comité I werd vooral getrokken door een passage in het artikel over de manier waarop een inlichtingenofficier, «alias James Bond», te werk gaat: «Chargé du renseignement, le militaire surveille de loin les criminels en tout genre qui, la plupart du temps, se baladent en grosses limousines allemandes. Le capitaine échange des informations avec ses équivalents français, danois et autres. Nous avons une image précise de la situation», verzekert hij.

Naar aanleiding van dit artikel stelde het Comité I zich een aantal vragen over de wijze waarop de ADIV was omgegaan met de informatie over de algemene situatie in Kosovo.

Het Comité I vroeg zich af of de in het artikel genoemde officier wel deel uitmaakte van de ADIV, dan wel of hij met deze dienst samenwerkte in het kader van een opdracht inzake inlichtingen binnen de operatie «Belkos 1».

Het Comité I had ook vragen over de verhoudingen die kunnen bestaan tussen leden van de ADIV die in opdracht zijn, en journalisten:

— is het gebruikelijk dat een officier die met een inlichtingenopdracht is belast, benaderd kan worden door een journalist, en dat niet alleen zijn identiteit, maar ook het voorwerp van zijn opdracht én de contacten die hij onderhoudt met zijn buitenlandse collega's, worden onthuld?

— indien ja, is dit conform de veiligheidsregels van de strijdkrachten, de staande orders van de ADIV of de bijzondere instructies uitgevaardigd in het kader van de operatie «Belkos 1»?

Indien neen:

— is er een inbreuk begaan tegen een van de bovengenoemde regels?

— is er schade berokkend aan het goede verloop van de opdracht? Is het mogelijk er de gevolgen van in te schatten?

afin de leur permettre d'assumer leurs responsabilités en pleine connaissance de cause.

CHAPITRE 4

RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LE SGR A GÉRÉ L'INFORMATION SUR LA SITUATION GÉNÉRALE AU KOSOVO

1. Introduction

Le Comité R a pris connaissance d'un article paru dans le journal *Le Soir* du vendredi 12 novembre 1999 intitulé «Au Kosovo, les belges surveillent sans punir».

Un passage de cet article relatant les déclarations d'un officier de renseignement «alias James Bond» a particulièrement retenu l'attention du Comité: «Chargé du renseignement, le militaire surveille de loin les criminels en tout genre qui, la plupart du temps, se baladent en grosses limousines allemandes. Le capitaine échange des informations avec ses équivalents français, danois et autres. «Nous avons une image précise de la situation», assure-t-il.»

Suite à cet article, le Comité R s'est posé quelques questions sur la manière dont le SGR avait géré l'information sur la situation générale au Kosovo.

Le Comité R s'est demandé si l'officier cité dans l'article faisait bien partie du SGR ou s'il collaborait avec ce service dans le cadre d'une mission de renseignement au sein de l'opération Belkos 1.

Le Comité R s'est aussi interrogé sur les rapports qui peuvent exister entre des membres du SGR en mission et des journalistes:

— Est-il d'usage qu'un officier chargé d'une mission de renseignement puisse être approché par un journaliste, voir son identité révélée ainsi que l'objet de sa mission et les contacts qu'il entretient avec ses équivalents étrangers?

— Si oui, est-ce conforme aux règles de sécurité des forces armées, aux ordres permanents du SGR ou aux instructions particulières délivrées dans le cadre de l'opération Belkos 1?

Si non:

— une infraction a-t-elle donc été commise à l'encontre d'une de ces règles?

— un préjudice a-t-il été causé au bon déroulement de la mission? Peut-on en évaluer les conséquences?

— zijn er maatregelen genomen om een einde te maken aan dit incident en om het hoofd te bieden aan de mogelijke nadelige gevolgen?

2. Procedure

Op 2 december 1999 besliste het Comité I een onderzoek te openen naar de wijze waarop de ADIV de informatie over de algemene situatie in Kosovo had beheerd.

Overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten werd de voorzitter van de Senaat op 15 december 1999 op de hoogte gebracht van de opening van dit onderzoek.

Op 16 december 1999 richtte de voorzitter van het Comité I een kantschrift aan het hoofd van de Dienst Enquêtes.

Overeenkomstig artikel 43.1 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten werd de minister van Landsverdediging op 17 december 1999 op de hoogte gebracht van de opening van dit onderzoek.

In februari 2000 heeft de Dienst Enquêtes van het Comité I een aantal verhoren afgenomen bij de ADIV. Op 27 maart 2000 heeft deze dienst zijn rapport aan het Comité I bezorgd.

Uit dit rapport blijkt dat de officier die in het krantenartikel wordt genoemd, niet behoort tot de ADIV: hij was de officier S2 (inlichtingenofficier) van het Belgisch bataljon in Kosovo (Belkos).

Artikel 3 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingen-diensten omschrijft de controleopdracht van het Comité I bij de Veiligheid van de Staat en bij de Algemene Dienst Inlichtingen en Veiligheid van de strijdkrachten.

Bijgevolg geniet het Comité I geen enkele bevoegdheid *rationae materiae* om een onderzoek te voeren naar de contacten tussen de voornoemde officier S2 en de pers, ook al werkte de betrokkene nauw samen met de ADIV.

Het Comité I besliste dan ook zijn vaststellingen te beperken tot de algemene bepalingen die ter zake toepasbaar zijn, en tot het standpunt van de ADIV over de mogelijke gevolgen van het bewuste artikel voor de veiligheid van de Belgische missie in Kosovo.

Het Comité I heeft het onderhavige rapport op 24 oktober 2000 goedgekeurd.

Het Comité I heeft rekening gehouden met een opmerking van de minister van Landsverdediging, vervat in zijn schrijven van 7 december 2000.

Met dit schrijven liet de minister het Comité I tevens laten weten dat het huidig verslag als dusdanig kon opgenomen worden in zijn activiteitenverslag.

— des mesures ont-elles été prises pour remédier à l'incident et parer à ses éventuelles conséquences dommageables?

2. Procédure

Le Comité R a décidé le 2 décembre 1999 d'ouvrir une enquête sur la manière dont le SGR avait géré l'information sur la situation générale au Kosovo.

Le président du Sénat a été informé de l'ouverture de cette enquête le 15 décembre 1999 conformément à l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le 16 décembre 1999, le président du Comité R a adressé une apostille au chef du Service d'enquêtes.

Le ministre de la Défense nationale a été informé de l'ouverture de cette enquête le 17 décembre 1999 conformément à l'article 43.1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le Service d'enquêtes du Comité R a procédé à des auditions au SGR dans le courant du mois de février 2000. Il a remis son rapport au Comité R le 27 mars 2000.

Il ressort de ce rapport que l'officier cité par l'article de presse n'appartient pas au SGR: il était l'officier S2 (l'officier de renseignement) du bataillon belge au Kosovo (Belkos).

L'article 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements circonscrit la mission de contrôle du Comité R à la Sûreté de l'État et au Service général du renseignement et de la sécurité des Forces armées.

Le Comité R n'a donc aucune compétence *rationae materiae* pour enquêter sur les contacts que l'officier S2 précité a entretenu avec la presse bien que celui-ci ait étroitement collaboré avec le SGR.

Le Comité R a donc décidé de limiter ses constatations aux règles générales applicables en la matière et au point de vue du SGR sur les répercussions éventuelles de l'article précité en matière de sécurité de la mission belge au Kosovo.

Le présent rapport a été approuvé par le Comité R le 24 octobre 2000.

Le Comité R a tenu compte d'une précision apportée par le ministre de la Défense nationale dans un courrier du 7 décembre 2000.

Par ce même courrier, le ministre a fait savoir au Comité que le présent rapport pouvait figurer tel quel dans son rapport annuel.

3. Vaststellingen

Het verspreiden van informatie door het leger en de relaties tussen de militairen en de pers zijn het voorwerp van de algemene orders J/813 en J/108. Voorts bevat instructie IF5 over de militaire veiligheid eveneens richtlijnen in verband hiermee.

Algemeen kunnen we stellen dat de relaties tussen de militairen en de pers tot voor kort onderworpen waren aan een voorafgaande machtiging.

Niettemin stelt het algemeen order J/108 F van 9 augustus 1994 dat elke militair, ongeacht zijn graad, de vrijheid heeft zijn mening te uiten op de wijze die hij het meest passend acht, net zoals alle burgers in België. Bijgevolg heeft hij het recht zich in eigen naam uit te drukken in de pers, zonder dat hij daarvoor eerst de toelating moet vragen.

Het is militairen echter verboden geclassificeerde informatie te onthullen aan niet gemachtigde personen, alsook verklaringen af te leggen die nadelig kunnen zijn voor 's lands veiligheid, die de openbare orde verstoren of die het voorkomen van delicten in het gedrang brengen. Evenmin mogen ze de eer en de waardigheid van de staatsinstellingen of van de strijdkrachten in gevaar brengen.

Binnen deze beperkingen geniet ook een inlichtingenofficier het recht in eigen naam verklaringen af te leggen aan de pers.

Desondanks de bepaling in artikel 19 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, die voorziet dat de chef van de ADIV een persoon kan aanwijzen die inlichtingen aan de pers mag meedelen, werd overeengekomen dat in praktijk enkel de woordvoerder van het kabinet van de minister van Landsverdediging bevoegd is om officiële verklaringen met betrekking tot de ADIV af te leggen tegenover de pers.

Vanuit het standpunt van de ADIV is er geen enkele inbreuk begaan op een van de bovengenoemde regels en hebben de verklaringen die door «*Le Soir*» van vrijdag 12 november 1999 in de mond van een inlichtingenofficier worden gelegd de veiligheid van de opdracht van de Belgische strijdkrachten in Kosovo niet in gevaar gebracht.

HOOFDSTUK 5

VERSLAG VAN HET ONDERZOEK NAAR DE ROL VAN DE ADIV BIJ HET TOEKENNEN VAN TOELATINGEN TOT HET MAKEN VAN LUCHTFOTO'S (EN ONDERWERPEN VAN MILITAIRE AARD)

1. Inleiding

Overeenkomstig het Belgisch intern recht is het verboden foto's te maken van militaire installaties zon-

3. Constatations

La diffusion d'informations par l'armée et les relations des militaires avec la presse font l'objet des ordres généraux J/813 et J/108. L'instruction IF5 sur la sécurité militaire contient également des instructions à ce sujet.

D'une manière générale, les relations des militaires avec la presse étaient jusqu'il y a peu soumises à autorisation préalable.

L'ordre général J/108 F du 9 août 1994 reconnaît cependant que chaque militaire, quel que soit son grade, dispose de la liberté d'exprimer ses opinions de la manière qu'il estime la plus appropriée, comme tout citoyen belge. Il a donc le droit de s'exprimer, en son propre nom, dans la presse sans autorisation préalable.

Il est cependant interdit aux militaires de révéler des informations classifiées à des personnes non habilitées et de faire des déclarations qui nuisent à la sécurité du pays, qui perturbent l'ordre public ou qui mettent en péril la prévention de faits délictueux. Ils ne peuvent également pas mettre l'honneur et la dignité des institutions de l'État ou celles des Forces armées en danger.

Dans ces limites, un officier de renseignement a lui aussi le droit de faire des déclarations à titre personnel à la presse.

L'information officielle des Forces armées n'est délivrée que par des porte-parole désignés par les autorités militaires. Nonobstant la disposition de l'article 19 de la loi du 30 novembre 1998 organique des services de renseignements qui prévoit que le chef du SGR peut désigner une personne qui peut communiquer des informations à la presse, il a été convenu que, dans la pratique, seul le porte-parole du ministre de la Défense nationale peut délivrer une information officielle à la presse en ce qui concerne le SGR.

Du point de vue du SGR, aucune infraction n'a été commise à l'encontre d'une des règles précitées et les propos attribués à un officier de renseignement par le journal *Le Soir* du vendredi 12 novembre 1999 n'ont pas compromis la sécurité de la mission des Forces armées belges au Kosovo.

CHAPITRE 5

RAPPORT DE L'ENQUÊTE MENÉE SUR LE RÔLE DU SGR DANS L'OCTROI DES AUTORISATIONS DE PRISES DE VUES AÉRIENNES (ET DE SUJETS MILITAIRES)

1. Introduction

En droit interne belge, il est défendu de prendre des photographies d'installations militaires sans l'autori-

der verlof van de militaire overheid (artikel 120*ter* van het Strafwetboek)(1).

Een ministerieel besluit van 28 februari 1940 bepaalt nog steeds de «voorwaarden onder welke de toelatingen tot het nemen of publiceren van fotographieën van militaire aard kunnen worden verleend.»

Het nemen van luchtfoto's boven het nationale grondgebied (ongeacht de plaats die men fotografeert) en «het vervoer van fototoestellen aan boord van luchtvaartuigen» zijn enkel toegelaten aan de houders van een bijzondere toelating, die wordt uitgereikt door de minister belast met het bestuur van de Luchtvaart, met voorafgaand akkoord van de minister van Landsverdediging (koninklijk besluit van 21 februari 1939).

Ook voor het publiceren van luchtfoto's is het voorafgaand akkoord van het ministerie van Landsverdediging vereist. Het koninklijk besluit van 1939 stelt ook de procedure vast die men moet volgen om deze toelatingen te verkrijgen. Inbreuken op deze bepalingen worden met strafsancties bestraft.

Hoewel deze stelsels van voorafgaande toelating werden ingevoerd in een periode waar oorlogvoorbereidingen aan de orde van de dag waren, zijn ze vandaag nog steeds van kracht. Aanvragen tot het verkrijgen van een toelating om foto's te maken, vanuit de lucht of van op de grond, moeten in principe nog steeds voorafgaandelijk worden onderzocht door de ADIV.

Nochtans ziet de situatie er vandaag heel anders uit. Het verschijnen van satellieten om de aarde te observeren enerzijds, het einde van de koude oorlog en de ondertekening van het verdrag van Helsinki van 24 maart 1992 inzake het open-luchtruim anderzijds, hebben respectievelijk geleid tot een ware revolutie van de technologische middelen om foto's te maken en tot een ingrijpende wijziging van de internationale juridische context.

Men kan zich dan ook afvragen of het ontstaan van deze nieuwe toestand geen gegronde reden vormt om de relevantie van de in 1939 genomen maatregelen opnieuw te onderzoeken, in het bijzonder betreffende het maken van luchtfoto's boven het nationale grondgebied.

(1) «Met gevangenisstraf van acht dagen tot één jaar en met geldboete van 26 tot 100 frank wordt gestraft: 1º Hij die, zonder verlof van de militaire, zeevaart- of luchtvaartoverheid, binnen een afstand van een myriameter of binnen enige andere door de minister van Landsverdediging later te bepalen afstand van een versterkte plaats, van een verdedigingswerk, van een post, van een militaire of zeevaartinrichting, van een luchtvaartinrichting, die niet een vliegveld of luchtvaartstation is, van een militair depot, magazijn of park, welke afstand gerekend wordt vanaf de buitenwerken, door enig procédé topografische opmetingen of verrichtingen doet of fotografische opnamen maakt van een van die plaatsen, werken of inrichtingen, of reproducties van die opnamen uitgeeft, tentoonstelt, verkoopt of verspreidt; 2º (...)».

sation de l'autorité militaire (article 120*ter* du Code pénal)(1).

C'est toujours un arrêté ministériel du 28 février 1940 qui détermine les conditions dans lesquelles peuvent être accordées les autorisations de prendre ou de publier des photographies de sujets militaires.

Toute prise de vue aérienne au-dessus du territoire national (quel que soit l'endroit photographié) ainsi que «le transport d'appareils photographiques à bord d'aéronefs» sont encore soumis à une autorisation spéciale du ministre chargé de l'administration de l'Aéronautique, avec l'accord préalable du ministre de la Défense nationale (arrêté royal du 21 février 1939).

La publication de photographies aériennes est également soumise à l'accord préalable du ministère de la Défense nationale. L'arrêté royal de 1939 fixe aussi la procédure à suivre en vue d'obtenir lesdites autorisations. Les infractions à ces dispositions sont passibles de sanctions pénales.

Ces régimes d'autorisation préalable, mis en place à une époque où des préparatifs de guerre étaient à l'ordre du jour, sont encore en vigueur de nos jours. Les demandes d'autorisation de photographies, qu'elles soient aériennes ou au sol, doivent toujours, en principe, être soumises à l'examen préalable du SGR.

La situation a pourtant bien changé depuis cette époque. L'apparition des satellites d'observation de la terre d'une part, la fin de la guerre froide et la signature du traité d'Helsinki du 24 mars 1992 sur le régime «ciel ouvert» d'autre part, ont bouleversé les moyens technologiques de prise de vue, de même que l'environnement juridique international.

Cette situation nouvelle ne justifie-t-elle pas que soit réexaminée la pertinence des dispositions prises en 1939, notamment à l'égard de la photographie aérienne au dessus du territoire national.

(1) «Sera puni d'un emprisonnement de huit jours à un an et d'une amende de 26 à 100 francs: 1º quiconque, sans l'autorisation de l'autorité militaire, maritime ou aéronautique, aura exécuté par un procédé quelconque des levés ou opérations de topographie dans un rayon d'un myriamètre ou dans tout autre rayon qui sera ultérieurement fixé par le ministre de la Défense nationale, autour d'une place forte, d'un ouvrage de défense, d'un poste d'un établissement aéronautique autre qu'un aérodrome ou aérogare, d'un dépôt, magasin ou parc militaires, à partir des ouvrages avancés, ou aura pris des photographies d'un de ces lieux, ouvrages ou établissements, édité, exposé, vendu ou distribué des reproductions de ces vues; 2º (...).»

Heeft het toezicht dat de ADIV uitoefent op het fotograferen van militaire onderwerpen (vanuit de lucht of van op de grond) nog enige reden van bestaan? Is dit toezicht nog langer mogelijk en nuttig? Hoeveel aanvragen van toelatingen moet de ADIV jaarlijks onderzoeken? Hoe gaat deze dienst daarbij te werk? Welke rol vervult de ADIV bij het toepassen van de inspectiemaatregelen vervat in het verdrag inzake het open-luchtruim?

Het zijn maar enkele van de vragen die het Comité I zich stelde met betrekking tot deze materie.

2. Procedure

Het Comité I besliste dit onderzoek te openen op 2 december 1999.

Met een kantschrift van 3 december 1999 gaf de voorzitter van het Comité I aan de Dienst Enquêtes de opdracht aan de ADIV de in de inleiding vermelde vragen te stellen.

Op 3 december 1999 werd voorzitter van de Senaat, op de hoogte gebracht van de opening van dit onderzoek.

Overeenkomstig artikel 43-1º van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten heeft het hoofd van de Dienst Enquêtes de minister van Landsverdediging, per brief van 6 december 1999, kennis gegeven van de opening van dit onderzoek.

Tussen 1 februari 2000 en 26 juni 2000, dat is de datum waarop de Dienst Enquêtes van het Comité I zijn verslag aan het Vast Comité I heeft bezorgd, heeft de Dienst Enquêtes diverse controles verricht.

Het Vast Comité I heeft een briefwisseling gevoerd met de directeur-generaal van het bestuur der Luchtvaart en het hoofd van de ADIV.

Het Comité I heeft het onderhavige verslag goedgekeurd op 23 januari 2001.

Dit verslag werd op 2 februari 2001 voorgelegd aan de minister van Landsverdediging.

3. De belangstelling van het Parlement

Op 16 september 1999 stelde de heer Yves Leterme, CVP-volksvertegenwoordiger, twee parlementaire vragen, de ene aan de vice-eerste minister en minister van Mobiliteit en Vervoer, de andere aan de minister van Landsverdediging.

Deze vragen hadden betrekking op de toepassing van de «reglementering inzake luchtfoto's en het vervoer van fototoestellen aan boord van luchtvaartuigen».

De volksvertegenwoordiger vroeg aan beide ministers of het koninklijk besluit van 21 februari 1939

Quelle est donc encore la raison d'être du contrôle des photographies de sujets militaires (aériennes ou au sol) par le SGR? Ce contrôle est-il encore possible et utile? Combien de demandes d'autorisations le SGR doit-il traiter chaque année? Comment procède-t-il pour instruire ces demandes? Quel rôle joue le SGR dans l'application des mesures d'inspection prévues par le traité «ciel ouvert»?

Telles sont quelques-unes des questions que le Comité R s'est posé sur cette matière.

2. Procédure

Le Comité «R» a décidé d'ouvrir cette enquête le 2 décembre 1999.

Par apostille du 3 décembre 1999, le président du Comité R a chargé le Service d'enquêtes de poser les questions reprises en introduction au SGR.

Le 3 décembre 1999, le président du Sénat a été averti de l'ouverture de cette enquête.

Par lettre du 6 décembre 1999, conformément à l'article 43-1º de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le chef du Service d'enquêtes a averti le ministre de la Défense nationale de l'ouverture de cette enquête.

Le Service d'enquêtes du Comité R a procédé à diverses vérifications entre le 1er février 2000 et le 26 juin 2000, date à laquelle il a déposé son rapport au Comité R.

Le Comité R a procédé à divers échanges de courriers avec le directeur général de l'administration de l'Aéronautique et le chef du SGR.

Le présent rapport a été approuvé par le Comité R le 23 janvier 2001.

Le rapport a été transmis au ministre de la Défense nationale le 2 février 2001.

3. L'intérêt parlementaire

Le 16 septembre 1999, M. Yves Leterme, député CVP a posé deux questions parlementaires, l'une au vice-premier ministre et ministre de la Mobilité et des transports, l'autre au ministre de la Défense nationale.

Ces question concernent l'application de la «réglementation relative à la prise de vues aériennes et au transport d'appareils photographiques à bord d'aéronefs».

Le député demande aux ministres si l'arrêté royal du 21 février 1939 est encore d'application à l'heure

vandaag nog steeds van toepassing is, en op welke gronden de toepassing ervan berust.

Het antwoord van de minister van Landsverdediging:

1. «Dit koninklijk besluit is tot op heden niet opgeheven en blijft dus van toepassing. De procedure voor het verkrijgen van zulke toelating werd echter gevoelig verlicht.

2. De bedoeling van het in stand houden van dit koninklijk besluit is om te beschikken over een wettelijk middel in geval van crisis en in het bijzonder in de strijd tegen het terrorisme.

3. *a)* De jaarlijkse aanvragen die ingediend worden bij de administratie van het Luchtverkeer bedragen ongeveer 500 (1999).

b) In normale omstandigheden wordt er tegenwoordig geen voorafgaandelijk akkoord meer geëist vanwege het ministerie van Landsverdediging.

4. Gezien er tegenwoordig op geen enkel militair objectief een verbod van publicatie van luchtfoto's rust, wordt artikel 6 niet toegepast(1).

4. Het commercialiseren van satellietbeelden op internationaal niveau

Meer dan veertig jaar na het lanceren van de eerste satelliet — de «Spoetnik» in 1957 —, is het ontginnen van de ruimte een belangrijke prioriteit geworden voor de hele internationale gemeenschap, niet alleen op burgerlijk maar ook op militair gebied evenals op het vlak van de inlichtingen. Ook België neemt deel aan burgerlijke programma's die tot doel hebben de aarde te observeren.

De eerste militaire observatiesatellieten werden in 1959 door de Verenigde Staten en in 1962 door de USSR gelanceerd. De informatie die men dankzij de satellieten verkreeg, heeft een niet te veronachtzamen rol gespeeld in het uitdenken van militaire strategieën: ze maakten het mogelijk nauwkeurige topografische kaarten te maken, doelwitten op te sporen en de uitbouw van het vijandelijk arsenaal van nabij te volgen.

Burgerlijke en militaire observatiesatellieten worden ook gebruikt om toe te zien op de naleving van internationale ontwapeningsverdragen of van straf- en ontwapeningsmaatregelen opgelegd door de VN.

(1) Artikel 6. Onmiddellijk na den uitvoering van een fotografische opname of een programma van fotografische opnamen waarvoor toelating is verleend, moeten van al de genomen clichés den minister van Landsverdediging (generalen staf van het leger, 2e sectie) twee van een volgnummer voorziene afdrukken voor onderzoek voorgelegd worden.

actuelle et sur quels motifs repose encore son application.

Réponse du ministre de la Défense nationale:

1. «Cet arrêté royal (du 21 février 1939) n'est pas abrogé et est donc toujours d'application. La procédure pour l'octroi d'une telle autorisation est cependant fortement allégée.

2. Le but de la conservation de cet arrêté royal est de disposer d'un outil en cas de crise en particulier dans la lutte contre le terrorisme.

3. *a)* les demandes annuelles introduites auprès de l'administration de l'Aéronautique sont de l'ordre de 500 (1999).

b) en temps normal, il n'est actuellement plus exigé un accord préalable du ministère de la Défense nationale.

4. Étant donné qu'actuellement aucun objectif militaire n'est interdit de publication de photo aérienne, l'article 6(1) n'est pas appliqué.

4. La commercialisation des images satellitaires au niveau international

Plus de quarante ans après le lancement du premier satellite «Spoutnik» en 1957, l'exploitation de l'espace est devenue un enjeu de première importance pour la communauté internationale dans son ensemble et ce, tant dans le domaine civil que dans le domaine militaire et celui du renseignement. La Belgique elle-même se trouve engagée dans des programmes civils d'observation de la Terre.

Les premiers satellites d'observation militaire ont été lancés par les États-Unis en 1959 et par l'URSS en 1962. L'information fournie par les satellites a joué un rôle non négligeable dans l'élaboration des stratégies militaires: en permettant de réaliser des cartes topographiques précises, en détectant des objectifs et en permettant de suivre l'évolution de l'arsenal de l'adversaire.

Les satellites d'observation, civils et militaires, connaissent aussi des applications dans le cadre de la surveillance de la mise en œuvre des traités internationaux de désarmement ou des mesures de sanctions et de désarmement imposées par l'ONU.

(1) Article 6. Aussitôt après l'exécution d'une prise de vues autorisée ou d'un programme de prises de vues autorisé, deux épreuves, munies d'un numéro d'ordre, de tous les clichés pris doivent être soumises à l'examen du ministre de la Défense nationale (état-major général de l'armée, 2e section).

Deze situatie wordt echter in toenemende mate gekenmerkt door de steeds grotere commerciële concurrentie tussen ruimtediensten.

Foto's genomen door burgerlijke satellieten worden vandaag aan het grote publiek aangeboden in resoluties die bijna even hoog zijn als die van militaire satellieten en tegen prijzen die steeds meer betaalbaar worden naarmate commerciële bedrijven elkaar in deze sector gaan beconcurreren.

Momenteel levert de Amerikaanse satelliet Ikonos de beste commerciële beelden; ze worden gecommercialiseerd door de Amerikaanse firma Space Imaging. Concurrenten zoals Orbital Imaging (USA), Kiberso (Rusland) en Spot Image (Europa) leveren beelden met een lagere resolutie.

Natuurlijk leidt deze situatie tot heel wat wantrouwen en discussies binnen de overheid van de Verenigde Staten, die beducht is voor het verspreiden van dergelijke beelden aan oorlogszuchtige staten of vijandige elementen.

Zo eist de regering van de Verenigde Staten dat Amerikaanse constructeurs de sluiter kunnen controleren van elke observatiesatelliet die aan vreemde landen wordt verkocht of voor vreemde landen wordt geëxploiteerd.

De industriëlen, die in het algemeen kunnen rekenen op de steun van het ministerie van Handel, zijn voorstander van een liberalisering van de markt, in tegenstelling tot het ministerie van Buitenlandse Zaken en het Pentagon.

De voorbije jaren hebben de industriëlen belangrijke resultaten behaald, maar het staat vast dat de Amerikaanse regering steeds de mogelijkheid zal bewaren om de verkoop te verbieden van beelden van bepaalde gevoelige zones in de Verenigde Staten of op het grondgebied van zijn bondgenoten, alsook om technische beperkingen op te leggen (in het bijzonder betreffende de hoek waarin de foto's worden gemaakt) of om de beeldenstroom te allen tijde te kunnen onderbreken.

Tot op heden zou alleen het grondgebied van Israël het voorwerp zijn van een dergelijke beperking vanwege de Amerikanen.

De vrees blijft dus bestaan dat om het even welke Staat, met vreedzame of oorlogszuchtige intenties, en zelfs om het even welke criminele onderneming of vijandige organisatie binnen afzienbare tijd de middelen kan verwerven om vanuit de ruimte de verdedigings- en veiligheidssystemen van democratische rechtsstaten te observeren.

Luchtfoto's en satellietfoto's

De mogelijkheden die satellieten bieden om de aarde te observeren, doen niets af aan het nut van het

Mais cette situation est de plus en plus marquée par l'intensification de la commercialisation concurrentielle des services spatiaux.

Des photos prises par satellites civils deviennent actuellement disponibles pour le grand public avec des degrés de résolution presque aussi élevés que ceux des satellites militaires et à des prix qui deviendront de plus en plus abordables au fur et à mesure que la concurrence commerciale s'installera dans ce secteur.

Les images commerciales les plus performantes sont actuellement celles fournies par le satellite américain Ikonos; elles sont commercialisées par la société américaine Space Imaging. Des sociétés concurrentes telles que Orbital Imaging (USA), Kiberso (Russie) et Spot Image (Europe) fournissent des images d'une résolution plus basse.

Ceci ne manque pas bien sûr de susciter des réticences et des débats au sein du gouvernement américain qui craint la diffusion de pareilles images à des pays belliqueux ou à des éléments hostiles.

Ainsi, celui-ci exige que les constructeurs américains puissent contrôler l'obturateur de tout satellite d'observation vendu à des pays étrangers ou exploité pour eux.

Les industriels, globalement soutenus par le département du Commerce sont favorables à une libéralisation du marché; le département d'État et le Pentagone y sont hostiles.

Au cours de ces dernières années, les industriels n'ont cessé de marquer des points mais il est certain que le gouvernement américain conserva toujours la possibilité d'interdire la vente d'images de certaines zones sensibles des États-Unis ou de ses alliés, de poser des limitations techniques (notamment sur les angles de prises de vues) ou de couper à tout moment le flot d'images.

Jusqu'à présent, seul le territoire d'Israël ferait l'objet d'une telle restriction de la part des américains.

La crainte demeure donc que n'importe quel État, qu'il soit pacifique ou belliqueux, et même que n'importe quelle entreprise criminelle ou organisation hostile, puisse bientôt se procurer les moyens d'observer depuis l'espace les systèmes de défense et de sécurité des États de droit démocratiques.

Photos aériennes et photos satellitaires

Les possibilités d'observation de la Terre par satellites ne diminuent en rien l'utilité de l'observation

observeren uit de lucht. Vooreerst omdat nog niet alle landen beschikken over de observatiecapaciteiten die satellieten bieden.

Vervolgens omdat een luchtfoto voorlopig gemakkelijker en sneller te verkrijgen blijft dan een satellietfoto. Tot slot omdat het observeren van de aarde met behulp van satellieten zijn geheim en onverwacht karakter aan het verliezen is.

Een satelliet verplaatst zich rond de aarde tegen een gemiddelde snelheid van 7 km per seconde. De duur van de observatiecyclus, hetzij het «terugkeerinterval», is de tijd tussen twee ogenblikken waarop de satelliet zich boven een geobserveerd punt bevindt.

Als gevolg van deze «terugkeertijd» (tussen 24 en 72 uur) is het niet altijd mogelijk op het gewenste ogenblik beelden te krijgen die informatie verstrekken over de evolutie van een bepaalde situatie («current intelligence»).

Hoe hoger de baan van de satelliet, hoe groter de gedekte observatieoppervlakte en hoe korter de «terugkeertijd». De resolutie van de beelden daarentegen is minder groot.

Wanneer de satelliet zich eenmaal in de geschikte positie bevindt om beelden te maken van een gewenste zone, dan moeten ook de weersomstandigheden of de voorwaarden van helderheid zich daartoe lenen. Satellieten die niet met radarsensoren zijn uitgerust, kunnen geen foto's maken door de wolken heen en evenmin gedurende de nacht.

Satellieten met een lange observatiecyclus hebben ook nog het nadeel dat de periodes tijdens dewelke de gegevens naar de grond worden doorgestuurd beperkt zijn, dat wil zeggen beperkt tot de ogenblikken waarop de satellieten zich in het zicht van een ontvangstation bevinden.

Tot slot zijn satellieten operationeel gezien vrij beperkt in hun gebruik; sommige satellieten laten zich manoeuvreren, maar binnen nogal nauwe grenzen en vaak ten nadele van hun levensduur, aangezien elk manoeuvre gepaard gaat met een aanzienlijke toename van het brandstofverbruik.

We merken nog op dat de grote mogendheden ruimtebewakingssystemen hebben ontwikkeld teneinde de inventaris bij te houden van de ongeveer 8 000 satellieten en diverse tuigen die in een baan rond de aarde draaien.

Deze netwerken, die informatie verzamelen uit open bronnen, afbeeldingen en elektronische afluisteroperaties, kunnen de bewegingen volgen van alle vreemde satellieten en hun opdrachten analyseren.

Deze gegevensstroom maakt het in het bijzonder mogelijk bewakingsberichten van het type SATRAN (Satellite Reconnaissance Advanced Notice) te versturen naar de strijdkrachten, die op die manier weten wanneer een bepaalde verkenningssatelliet een

aérienne. Tout d'abord, parce que les capacités d'observation par satellites ne sont pas encore à la portée de tous les pays.

D'autre part, parce qu'une photographie aérienne s'obtient encore plus facilement et plus rapidement qu'une photographie par satellite. Enfin, l'observation de la terre par satellites est en passe de perdre son caractère secret et impromptu.

La vitesse moyenne de déplacement d'un satellite autour de la terre est de 7 km par seconde. La durée du cycle d'observation, soit l'intervalle de «revisite», est l'intervalle de temps qui sépare chaque passage du satellite au dessus d'un point observé.

Ces temps de «revisite» (entre 24 et 72 heures) ne permettent pas toujours d'obtenir en temps voulu des images donnant des informations sur l'évolution d'une situation («current intelligence»).

Plus haute se situe l'orbite, plus grande est la surface d'observation couverte et plus l'intervalle de «revisite» est court. Par contre, la résolution est alors moins grande.

Le satellite étant en position de photographier une zone cible, encore faut-il que les conditions météorologiques ou de luminosité s'y prêtent. À moins d'être équipés de senseurs radars, il n'est pas possible de photographier à travers les nuages ou la nuit.

Les satellites dont le cycle d'observation est long présentent aussi le désavantage de n'offrir que des périodes limitées de transmission des données au sol, c'est-à-dire qu'elles sont limitées aux moments où les satellites sont en vue d'une station réceptrice.

Enfin, les satellites sont relativement rigides d'emploi sur le plan opérationnel; certains sont manouvrables, mais dans des limites assez étroites et, souvent au détriment de leur durée de vie puisque chaque manœuvre nécessite une grosse consommation de carburant.

Notons enfin que des systèmes de surveillance spatiale ont été déployés par les grandes puissances en vue de tenir à jour l'inventaire des quelques 8 000 satellites et objets divers en orbite autour de la terre.

En rassemblant l'information de sources ouvertes, l'imagerie et les écoutes électroniques, ces réseaux sont en mesure de suivre les mouvements et d'analyser les missions de tous les satellites étrangers.

Ce flux de données permet notamment de lancer des avis de surveillance SATRAN (Satellite Reconnaissance Advanced Notice) aux forces armées, qui savent ainsi quand tel ou tel satellite de reconnaissance étranger est en mesure d'observer une aire

geclassificeerd gebied van militaire activiteiten kan observeren. Voorts kan dit netwerk worden gebruikt om communicaties en signalen van vreemde satellieten, burgerlijke of militaire, te intercepteren.

Sinds kort publiceert een internationaal netwerk van astronomen de positie van elke satelliet op een website die Heavens-Above.com heet. Deze site heeft vooral de bedoeling om al wie geboeid is door wat er in de ruimte gebeurt de kans te bieden het voorbijkomen van een satelliet gedurende een bepaalde periode 's nachts te observeren.

Het Vast Comité I vroeg zich af of deze site het voor terroristische of criminele organisaties niet mogelijk maakte vast te stellen, net zoals voor militaire overheden, gedurende welke periodes er reden zou zijn om bepaalde activiteiten, verplaatsingen of wapensystemen te camoufleren voor observatie vanuit de ruimte. Het Comité heeft de ADIV en de Veiligheid van de Staat hierover ondervraagd.

In een gedetailleerde analyse die de ADIV op 23 januari 2001 aan het Vast Comité I heeft bezorgd, meent deze dienst, samengevat, dat de bewuste site geen enkele veiligheidsregel schendt en bijgevolg geen risico's inhoudt(1). De site maakt het voor de bezoeker immers niet mogelijk na te gaan of hij zich bevindt binnen de visualisatiekegel van een militaire observatiesatelliet. Overigens behoort de baan van de militaire satelliet Helios, die op de site beknopt wordt beschreven, tot het publiek domein.

Dit neemt niet weg dat de technische beperkingen en ongemakken van satellietobservatie tot gevolg hebben dat de luchtfotografie een nuttig en doeltreffend inlichtingeninstrument is en dat ook nog lange tijd zal blijven.

5. Het internationaal juridisch kader

Het observeren van de aarde met behulp van satellieten is conform het internationaal recht. Het «ruimteverdrag» van 1967 onderscheidt immers twee belangrijke principes: de vrijheid van verkeer en het vrij gebruik van hulpbronnen in de ruimte rond de aarde.

Het ontbreken van elke vorm van territoriale soevereiniteit in de ruimte buiten de dampkring, alsook het gevolg daarvan, namelijk de toepassing van het vlaggenrecht op ruimtetuigen, vestigen bijgevolg de internationale wettelijkheid van strategische waarnemingen in en vanuit de ruimte.

Bijgevolg is het koninklijk besluit van 1939 niet toepasbaar op het observeren van het nationaal grondgebied met behulp van satellieten, en evenmin

(1) Op het ogenblik waarop het onderhavige rapport werd goedgekeurd, had de Veiligheid van de Staat haar standpunt nog niet ter kennis gebracht van het Comité.

d'activités militaires classifiée. Ce réseau est également en mesure de procéder à l'interception des communications et signaux des satellites étrangers, qu'ils soient civils ou militaires.

Depuis peu, un réseau international d'astronomes diffuse sur un site web intitulé Heavens-Above.com la position de chaque satellite. Ce site est principalement destiné à permettre aux passionnés de l'espace d'observer le passage d'un satellite dans une période déterminée de la nuit.

Le Comité R s'est demandé si ce site ne permettait pas à des organisations terroristes ou criminelles d'être en état de prévoir, au même titre que les puissances militaires, les périodes au cours desquelles il y aurait lieu de camoufler les activités, mouvements ou systèmes d'armes qu'elles désireraient soustraire à la surveillance spatiale. Le Comité R a questionné le SGR et la Sûreté de l'État à ce sujet.

Dans une analyse détaillée transmise au Comité R le 23 janvier 2001, le SGR estime en résumé que le site en question ne viole aucune règle de sécurité et ne présente donc aucun danger(1). Le site ne donne pas en effet la possibilité au consultant de vérifier s'il se trouve dans le cône de visualisation d'un satellite d'observation militaire. Par ailleurs, l'orbite du satellite militaire Hélios, sommairement décrite sur le site, est du domaine public.

Il n'en demeure pas moins que les limites et inconvénients techniques de l'observation satellitaire font en sorte que la photographie aérienne reste et restera encore longtemps un outil utile et efficace de renseignement.

5. Le cadre juridique international

L'observation de la terre par satellites est conforme au droit international. Le «traité de l'espace» de 1967 énonce en effet deux grands principes, la liberté de circulation et la liberté d'utilisation des ressources de l'espace circumterrestre.

L'absence de toute souveraineté territoriale dans l'espace extra-atmosphérique et son corrolaire, l'application de la loi du pavillon aux engins spatiaux, fondent donc la légalité internationale des observations stratégiques dans et à partir de l'espace.

L'arrêté royal de 1939 n'est donc pas applicable à l'observation du territoire national à partir de satellites, ni d'ailleurs aux observations aériennes effectuées

(1) La Sûreté de l'État n'a pas encore fait connaître son point de vue au Comité R au moment de l'approbation du présent rapport.

op luchtwaarnemingen in het luchtruim in het kader van het verdrag van Helsinki van 24 maart 1992 inzake het open luchtruim.

Dit verdrag is een verlengstuk van de verbintenissen die de partijen zijn aangegaan in het kader van de Conferentie over veiligheid en samenwerking in Europa (CVSE), met het oog op het bevorderen van de openheid en de transparantie betreffende hun militaire activiteiten en het versterken van de veiligheid met maatregelen van vertrouwen en veiligheid.

De partijen zijn van mening dat het creëren van een open luchtruim, toepasbaar op luchtwaarnemingen, van aard is de openheid en transparantie te vergroten en bijgevolg het toezicht op de naleving van de bestaande en toekomstige akkoorden inzake wapenbeperking te vergemakkelijken, alsook het vermogen tot het voorkomen van conflicten en het beheren van crisissen te vergroten.

Het verdrag voert dus een aantal erkende procedures in om de ondertekenaars toe te laten op billijke basis het grondgebied van alle verdragsluitende partijen te observeren, met inbegrip van hun onderlinge strijdkrachten en militaire activiteiten.

De partijen hebben het recht een aantal ongewapende vluchten boven het grondgebied van alle andere deelnemers uit te voeren, op voorwaarde dat ze daarbij erkende vliegtuigen en observatietechnieken gebruiken en dit doen op grond van vooraf overeengekomen en gecontroleerde missie- en vluchtplannen.

De ondertekenaars van dit verdrag zijn de lidstaten van de NAVO, Rusland, Oekraïne, Wit-Rusland, Georgië, Kirgizië en nog andere ex-leden van het Warschaupact. Ook andere landen mogen toetreden tot het verdrag. Het Belgisch Parlement heeft dit verdrag goedgekeurd door de wet van 15 mei 1995 (*Belgisch Staatsblad*, 12 december 1995).

6. Vaststellingen van het Comité I

Met betrekking tot de toepassing van artikel 120*ter* van het Strafwetboek enerzijds en van het koninklijk besluit van 21 februari 1939 «tot het reglementeren van luchtfoto-opnamen boven het nationaal grondgebied en het vervoeren van fototoestellen aan boord van luchtvaartuigen» anderzijds, bestaan bij de ADIV diverse interne nota's:

— de instructie TVR 62: «veiligheid van de fotografische opnamen — grondfotografie — luchtfotografie», die echter niet meer van toepassing is;

— sectie 5 van verordening IF5: «veiligheid van de beeldopnamen — grondopnamen — luchtopnamen» (versie van 8 januari 1997);

— de lijst van tegen luchtopnamen te beschermen onderwerpen (versie van 30 september 1997 en versie van 14 december 1998).

dans l'espace aérien dans le cadre du traité d'Helsinki du 24 mars 1992 sur le régime «ciel ouvert».

Ce traité prolonge les engagements que les parties ont pris dans le cadre de la Conférence sur la sécurité et la coopération en Europe (CSCE) de promouvoir une ouverture et une transparence accrues de leurs activités militaires et de renforcer la sécurité par des mesures de confiance et de sécurité.

Les parties considèrent que la création d'un régime «ciel ouvert» applicable à l'observation aérienne est de nature à accroître l'ouverture et la transparence pour faciliter le contrôle du respect des accords existants et futurs de limitation des armements et pour renforcer la capacité de prévention des conflits et de gestion de crises.

Le traité instaure donc des procédures agréées pour permettre aux signataires d'observer sur une base équitable tous les territoires des États parties ainsi que leurs forces et activités militaires réciproques.

Les parties ont le droit d'effectuer un certain nombre de vols non armés sur l'ensemble des territoires des autres participants, à condition d'utiliser des avions et des techniques d'observation agréés, suivant des plans de mission et de vol préalablement convenus et contrôlés.

Les pays ayant signé ce traité sont les membres de l'OTAN, la Russie, l'Ukraine, la Biélorussie, la Géorgie, le Kirghistan ainsi que d'autres pays ex-membres du Pacte de Varsovie. Les autres pays sont admis à se joindre au traité. Le Parlement belge a ratifié ce traité par la loi du 15 mai 1995 (*Moniteur belge*, 12 décembre 1995).

6. Les constatations du Comité R

L'application de l'article 120*ter* du Code pénal et celle de l'arrêté royal du 21 février 1939 «réglementant la prise de vues aériennes au-dessus du territoire national et le transport d'appareils photographiques à bord d'aéronefs» font l'objet de plusieurs notes internes émanant du SGR:

— l'instruction TVR 62: «sécurité des prises de vues — prises de vues terrestres — prises de vues aériennes» qui n'est cependant plus d'application;

— la section 5 du règlement IF5: «sécurité des prises de vues — prises de vues terrestres — prises de vues aériennes» (version du 8 janvier 1997);

— la liste des objectifs à protéger contre la prise de vues aériennes (version du 30 septembre 1997 et version du 14 décembre 1998).

Deze documenten voorzien twee afzonderlijke procedures naargelang het gaat om het maken van land- of luchtopnamen.

6.1. Grondopnamen

Met betrekking tot grondopnamen mag geen enkel foto-, film- of televisiedocument van militaire onderwerpen worden gemaakt of uitgezonden zonder toelating van de bevoegde militaire overheid.

Naargelang het geval is de bevoegde militaire overheid de kamp- of kwartiercommandant, de korpschef, de provinciecommandant, het kabinet van de minister van Landsverdediging, de SID of de ADIV (SGR/S).

Deze laatste dienst is bevoegd inzake toelatingen tot het maken van film- of televisiereportages van de troepen met oefening, de militaire installaties en het militair materieel.

De richtlijn TVR 62 beschreef de veiligheidsmaatregelen die de bevoegde overheden moesten nemen wanneer ze toelating verleenden tot het maken van opnamen. Dit document bepaalde onder meer dat alle aanvragen tot het verkrijgen van een toelating (ongeacht de bevoegde overheid) ter kennisgeving moesten worden bezorgd aan SDRA.

De houder van een toelating tot het fotograferen van militaire installaties moest bovendien door een officier worden vergezeld, om te voorkomen dat foto's werden gemaakt van een onderwerp dat een vreemde mogendheid kon interesseren. Deze instructies werden niet overgenomen in het document IF5, dat deze materie momenteel regelt.

6.2. Luchtopnamen

In principe bezorgt het bestuur der Luchtvaart elke aanvraag tot het maken van luchtfoto's met betrekking tot het nationaal grondgebied aan de ADIV, ongeacht of de aanvrager een burger of een militair is.

Tot voor kort raadpleegde de ADIV, telkens wanneer deze dienst een aanvraag tot toelating ontving, een vertrouwelijke lijst van te beschermen onderwerpen.

Deze lijst vermeldde, per provincie, de burgerlijke (bijvoorbeeld: kerncentrales) en militaire (bijvoorbeeld: luchthavens) installaties waarvan geen luchtopnamen mochten worden gemaakt. Na de aanvraag te hebben onderzocht, deelde de ADIV zijn advies mee aan het bestuur der Luchtvaart, die vervolgens al dan niet een toelating uitreikte.

Met betrekking tot het publiceren van luchtopnamen moesten, onmiddellijk na de uitvoering van de opnamen waarvoor toelating was verleend, twee van een volgnummer voorziene afdrukken van al de geno-

Ces documents prévoient deux procédures distinctes selon qu'il s'agit de prises de vues terrestres ou de prises de vues aériennes.

6.1. Prises de vues terrestres

Pour les prises de vues terrestres, aucun document photographique, filmé ou télévisé de sujets militaires ne peut être pris ou diffusé sans l'autorisation de l'autorité militaire compétente.

Selon le cas, l'autorité militaire compétente est le commandant de camp, de quartier, le chef de corps, le commandant de province, le cabinet du ministre de la Défense nationale, le SID ou le SGR/S.

Le SGR/S est compétent pour les autorisations de reportages filmés ou télévisés sur les troupes à l'exercice, les installations militaires et le matériel militaire.

La directive TVR 62 indiquait les mesures de sécurité que les autorités compétentes devaient prendre en matière d'autorisation de prises de vues. Ce document prévoyait ainsi que toutes les demandes d'autorisations (quelle que soit l'autorité compétente) devaient être adressées pour information à SDRA.

Une personne en possession d'une autorisation de photographier des installations militaires devait aussi être accompagnée d'un officier pour vérifier qu'aucun objectif susceptible d'intéresser une puissance étrangère ne soit photographié. Ces instructions ne furent pas reprises dans le document IF5 qui règle actuellement la matière.

6.2. Prises de vues aériennes

En principe, l'administration de l'Aéronautique transmet au SGR toute demande de prise de vues aériennes concernant le territoire national, qu'elle émane de civils ou de militaires.

Jusqu'il y a peu, lorsqu'il recevait une telle demande d'autorisation, le SGR consultait une liste confidentielle d'objectifs qu'il convenait de protéger.

Cette liste reprenait, par provinces, les installations civiles (exemple: les centrales nucléaires) et militaires (exemple: les aérodromes) qui ne pouvaient être photographiées par voie aérienne. Après examen, le SGR renvoyait son avis à l'administration de l'Aéronautique qui octroyait ou non l'autorisation.

En ce qui concerne la publication de photos aériennes, aussitôt après l'exécution des prises de vues autorisées, deux épreuves, munies d'un numéro d'ordre, de tous les clichés pris devaient être soumises à

men clichés voor onderzoek aan de ADIV worden overgelegd.

De foto's die mochten worden gepubliceerd, kregen een stempel met de vermelding « publicatie toegelaten ». Eén exemplaar van deze foto's bleef in het bezit van Landsverdediging, de andere foto werd teruggestuurd naar de eigenaar. Foto's waarvan de publicatie niet werd toegestaan, bleven definitief eigendom van Landsverdediging en bleven in het bezit van de ADIV.

In 1992 heeft de ADIV met het bestuur der Luchtvaart gesprekken aangeknoopt over de toepassing van het koninklijk besluit van 1939. Het bestuur der Luchtvaart, dat bevoegd is in het kader van de materies die worden geregeld door het Verdrag van Chicago van 7 december 1944, stelde de militaire overheden voor om het koninklijk besluit van 1939 op te heffen of ten minste de toepassing ervan afhankelijk te maken van het afkondigen van de staat van oorlog.

Hoewel de ADIV goed besefte dat de reglementering op bepaalde punten was achterhaald, weigerden de militaire overheden in te stemmen met het voorstel van het bestuur der Luchtvaart.

In september 1998 vond bij de ADIV een vergadering plaats die werd bijgewoond door vertegenwoordigers van de generale staf, de ADIV, het Agentschap voor nucleaire veiligheid en van het Nationaal Geografisch Instituut (NGI); de vergadering had tot doel na te gaan of het opportuun was de regels betreffende de toelatingen tot het nemen en publiceren van luchtfoto's te wijzigen.

Alle deelnemers aan de vergadering waren het eens met de gegrondheid van de opmerkingen van het NGI, volgens dewelke de huidige commercialisering van satellietfoto's met hoge resolutie, die van even goede kwaliteit zijn als klassieke luchtfoto's, niet langer toelaat dat nog enige controle wordt uitgeoefend op het nemen of verspreiden ervan.

Bijgevolg meende men dat de beperkende maatregelen die nog steeds toepasbaar zijn op de publicatie van luchtfoto's van militaire onderwerpen enigszins waren achterhaald.

Niettemin vond de ADIV ook dat het volledig intrekken van alle wetgeving ter zake een handicap zou betekenen in crisissituaties en Landsverdediging zou beroven van toereikende middelen om personen met slechte bedoelingen te vervolgen, of het nu ging om echte spionage of om het zoeken naar inlichtingen door subversieve of terroristische organisaties.

De ADIV stelde ook vast dat een luchtfoto veel sneller verkrijgbaar was dan een satellietbeeld.

Er werd dan ook beslist de huidige wetgeving te behouden, maar de toepassing ervan te verlichten, in

l'examen du SGR. Les photos autorisées de publication recevaient un cachet avec la mention « publication autorisée ».

Un exemplaire de ces photos demeurait la propriété de la Défense nationale, l'autre était renvoyé à son propriétaire. Les photos dont la publication n'était pas autorisée appartenaient définitivement à la Défense nationale et restaient en la possession du SGR.

En 1992, le SGR a entrepris des discussions sur l'application de l'arrêté royal de 1939 avec l'administration de l'Aéronautique. Celle-ci, qui est compétente dans le cadre des matières réglées par la Convention de Chicago du 7 décembre 1944, a proposé aux autorités militaires d'abroger, ou tout au moins de conditionner, l'application de l'arrêté royal de 1939 à la promulgation de l'état de guerre.

Les autorités militaires n'ont cependant pas souscrit à cette proposition bien que le SGR était tout à fait conscient que cette réglementation était dépassée sur certains points.

En septembre 1998, une réunion s'est tenue au SGR à laquelle participaient des représentants de l'État-major, du SGR, de la Sécurité nucléaire et de l'Institut géographique national (IGN); son but était d'examiner l'opportunité d'une modification des règles au sujet des autorisations de prise et de publication des photos aériennes.

Tous les participants à cette réunion ont été d'accord pour reconnaître le bien-fondé des remarques formulées par l'IGN selon lesquelles la commercialisation actuelle de photos satellitaires à haute résolution, aussi valables que les photos aériennes classiques, ne permettait plus d'exercer un quelconque contrôle sur leur prise ou leur diffusion.

Dès lors, on a estimé que les mesures restrictives encore en application quant à la publication des photos aériennes d'objectifs militaires étaient devenues quelque peu obsolètes.

Cependant, le SGR a aussi estimé qu'une suppression totale de toute législation en la matière serait un handicap en cas de situation de crise; elle priverait la Défense nationale de moyens suffisants de poursuite à l'encontre de personnes malveillantes, que ce soit en matière d'espionnage proprement dit ou de recherches de renseignements par des organisations subversives ou terroristes.

Le SGR a constaté également qu'une photo aérienne pouvait s'obtenir dans des délais beaucoup plus courts qu'une image satellitaire.

Il fut donc décidé de maintenir en vigueur la législation actuelle, tout en assouplissant son application,

het bijzonder met betrekking tot de toelatingen tot publicatie.

Een eerste aanpassing van deze bepaling bestond erin een veiligheidsofficier te benoemen binnen elke grote onderneming die luchtfoto's gebruikt; de betrokkene moest houder zijn van een veiligheidsmachtiging. Ook de onderneming zelf moest houder zijn van een veiligheidsmachtiging.

De veiligheidsofficier werd behoorlijk gebrieft door de ADIV en ontving de vertrouwelijke lijst van te beschermen onderwerpen; hij was aldus gemachtigd om een beslissing te nemen in naam van de ADIV. Vandaag zijn er nog twee Belgische ondernemingen die veiligheidsofficieren hebben.

Als tweede aanpassing werden alle onderwerpen op de vertrouwelijke lijst tegen luchtfoto's te beschermen onderwerpen geschrapt. De lijst is momenteel blanco en bestaat bijgevolg louter pro forma, maar het blijft mogelijk er onderwerpen op te plaatsen indien dat absoluut noodzakelijk zou zijn.

Ondernemingen die luchtfoto's van het Belgisch grondgebied willen maken en publiceren moeten dus niet langer houder zijn van een veiligheidsmachtiging, zolang de lijst van te beschermen onderwerpen blanco blijft.

Voorts, aangezien militaire luchtfoto's vandaag niet meer geclassificeerd zijn, kan hun publicatie automatisch worden toegelaten, tenzij ze aanvullende inlichtingen of aantekeningen bevatten die deze foto's gevoelig maken.

Met betrekking tot luchtfoto's die door burgers worden gemaakt, past het bestuur der Luchtvaart nog steeds het principe toe volgens hetwelk alle luchtfoto's onderworpen zijn aan een voorafgaande toelating die door dit bestuur wordt uitgereikt.

Deze toelating wordt uitsluitend uitgereikt aan natuurlijke personen (fotografen) en is niet overdraagbaar. De toelating is geldig voor een periode van twee jaar.

In principe is het voorafgaand akkoord van de minister van Landsverdediging dus niet langer vereist, ongeacht de nationaliteit van de fotograaf. Het uitreiken van de toelating door het bestuur der Luchtvaart heeft automatisch tot gevolg dat ook de toelating tot publiceren wordt verleend.

De toelatingen die dit bestuur uitreikt, worden nadien ter kennisgeving verzonden aan het ministerie van Landsverdediging. De ADIV blijft dus op de hoogte van de toelatingen die worden verleend, zodat deze dienst toezicht kan blijven uitoefenen.

Het geheel van de hierboven beschreven maatregelen is van toepassing sinds 1 januari 1999.

Wanneer het bestuur der Luchtvaart echter een toelating uitreikt tot het maken van luchtfoto's boven

en particulier dans le domaine de l'autorisation de publication.

Un premier aménagement de cette disposition fut de faire désigner un officier de sécurité, titulaire d'une habilitation de sécurité, dans chaque grande firme utilisatrice de photos aériennes qui, elle-même devait être en possession d'une habilitation de sécurité.

L'officier de sécurité était mis en possession de la liste confidentielle des objectifs à préserver après avoir été dûment «briefé» par le SGR; il était alors habilité pour statuer au nom du SGR. Il existe encore actuellement deux de ces firmes belges qui disposent d'officiers de sécurité.

Une deuxième mesure fut de supprimer de la liste confidentielle des objectifs à protéger contre les prises de vues aériennes tous les objectifs qui s'y trouvaient mentionnés. Cette liste actuellement vierge existe donc encore pro forma et la possibilité d'y faire à nouveau figurer des objectifs à protéger en cas d'absolue nécessité demeure.

Les firmes qui souhaitent prendre et publier des photos aériennes du territoire belge ne doivent donc plus être titulaires d'habilitations de sécurité aussi longtemps que la liste des objectifs à protéger restera vierge.

D'autre part, les photos aériennes militaires n'étant plus à présent classifiées, leur publication peut être autorisée automatiquement à moins que n'y figurent des renseignements complémentaires ou des annotations les rendent sensibles.

Pour les photos aériennes prises par des civils, l'administration de l'Aéronautique applique toujours le principe selon lequel toutes les prises de vues aériennes sont soumises à une autorisation préalable délivrée par ce service.

Cette autorisation est délivrée exclusivement à une personne physique (le photographe) et n'est pas cessible. Elle est valable pour une période de deux ans.

En principe, l'accord préalable du ministre de la Défense nationale n'est donc plus requis, quelle que soit la nationalité du photographe. La délivrance de l'autorisation par l'administration de l'Aéronautique implique automatiquement la délivrance de l'autorisation de publication.

Les autorisations délivrées par cette administration sont transmises a posteriori pour information au ministère de la Défense nationale. Le SGR reste donc informé des autorisations accordées de manière à lui permettre d'exercer un contrôle.

L'ensemble des dispositions précitées est d'application depuis le 1er janvier 1999.

Néanmoins, lorsqu'elle délivre une autorisation d'effectuer des prises de vues aériennes au-dessus du

het Belgisch grondgebied, geeft dit bestuur kennis van haar beslissing met behulp van een voorgedrukt formulier waarop staat dat de fotograaf moet vermijden foto's te maken van militaire installaties en die foto's te publiceren.

Dit is het gevolg van een aanbeveling in die zin die de ADIV in 1999 nog aan dit bestuur heeft gericht, in weerwil van de nieuwe bepalingen.

Bovendien vermeldt het bestuur der Luchtvaart dat het voorafgaand akkoord van het parket vereist kan zijn voor luchtfoto's van gebeurtenissen met actualiteitswaarde, zoals een brand of een ernstig ongeluk, en dat dit akkoord steeds via de Militaire Veiligheidsdienst moet worden aangevraagd.

Dit is het gevolg van een procedure die de gerechtelijke overheden in het verleden volgden, vóór de inwerkingtreding van de nieuwe bepalingen, maar die sindsdien niet meer wordt toegepast.

6.3. De toepassing van het verdrag inzake het open luchtruim

De ADIV verklaart dat hij geen enkele bevoegdheid geniet met betrekking tot de toepassing van het verdrag inzake het open luchtruim, aangezien de foto's die in het kader van dit verdrag worden gemaakt niet voor publicatie zijn bestemd.

6.4. Aantal behandelde aanvragen

In 1997 heeft de ADIV 1 097 aanvragen behandeld, 1 950 in 1998 en 245 in 1999, waaronder een veertigtal van niet EU-ingezetenen. Geen enkele aanvraag voor een toelating tot het maken of publiceren van foto's werd geweigerd.

7. Besluiten

Alle partijen zijn het erover eens dat de bepalingen van het koninklijk besluit van 21 februari 1939 «tot het reglementeren van luchtfoto-opnamen boven het nationaal grondgebied en het vervoeren van fototoestellen aan boord van luchtvaartuigen» achterhaald zijn, niet alleen door de ontwikkeling van de technologie van observatiesatellieten, maar ook als gevolg van de ondertekening door België van het verdrag van Helsinki van 24 maart 1992 inzake het open luchtruim.

Niettemin is de ADIV van mening dat het volledig intrekken van alle wetgeving ter zake een handicap zou betekenen in geval van een crisis, en Landsverdediging zou beroven van gepaste middelen om kwaadwillige personen te vervolgen, ongeacht of het gaat om echte spionage of om het zoeken naar inlichtingen door subversieve of terroristische organisaties.

territoire belge, l'administration de l'Aéronautique notifie cette décision au moyen d'un formulaire préimprimé qui mentionne que le photographe doit éviter des prises de vues d'installations militaires et leur publication.

Ceci résulte d'une recommandation en ce sens que le SGR a encore adressée en 1999 à cette administration, nonobstant les nouvelles dispositions.

En outre, l'administration de l'Aéronautique mentionne également que l'accord préalable du parquet peut être nécessaire pour des photographies aériennes d'événements d'actualité comme des incendies ou des accidents graves et que cet accord est toujours demandé par la voie du Service de sécurité militaire.

Ceci résulte d 'une procédure que les autorités judiciaires appliquaient autrefois avant la mise en vigueur des nouvelles dispositions mais qui n'est plus appliquée depuis lors.

6.3. L'application du traité «ciel ouvert»

Le SGR déclare n'avoir reçu aucune compétence dans l'application du traité «ciel ouvert» étant donné que les prises de vues réalisées dans le cadre de ce traité ne sont pas destinées à être publiées.

6.4. Nombre de demandes traitées

Le nombre de demandes traitées par le SGR était de 1 097 en 1997, 1 950 en 1998, 245 en 1999 dont une quarantaine en provenance de ressortissants hors UE. Aucune demande de prise de vues, ni de publication n'a été refusée.

7. Conclusions

Tout le monde s'accorde à reconnaître que les dispositions de l'arrêté royal du 21 février 1939 «réglementant la prise de vues aériennes au-dessus du territoire national et le transport d'appareils photographiques à bord d'aéronefs» sont devenues obsolètes, tant par l'apparition de la technologie des satellites d'observation, que par l'adhésion de la Belgique au Traité d'Helsinki du 24 mars 1992 sur le régime «ciel ouvert».

Cependant le SGR estime qu'une suppression totale de toute législation en la matière serait un handicap en cas de situation de crise; elle priverait la Défense nationale de moyens suffisants de poursuite à l'encontre de personnes malveillantes, que ce soit en matière d'espionnage proprement dit ou de recherche de renseignements par des organisations subversives ou terroristes.

De ADIV meent dus dat een middel van controle *a posteriori* op luchtfoto's moet worden bewaard. Uiteindelijk werd beslist het koninklijk besluit van 1939 niet op te heffen, maar de procedure voor het toekennen van de toelatingen in aanzienlijke mate te verlichten, waardoor het tegelijk mogelijk blijft een strikte toepassing opnieuw in te voeren.

Toch vraagt het Vast Comité I zich af of artikel 120*ter* van het Strafwetboek en het koninklijk besluit van 21 februari 1939 niet moeten worden herzien en aangepast, rekening houdend met de nieuwe internationale juridische context, enerzijds, en de technologische ontwikkeling inzake ruimte- en luchtobservatie, anderzijds.

Het Vast Comité I denkt dat de bescherming van militaire onderwerpen tegen het maken van luchtfoto's met vijandige bedoelingen of met bedoelingen van spionage kan worden gegarandeerd in een juridisch kader gelijkaardig aan dat van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen.

Le SGR estime donc devoir conserver un moyen de contrôle *a posteriori* sur les prises de vues aériennes. La solution retenue a été de ne pas abroger l'arrêté royal du 1939 tout en allégeant fortement la procédure pour l'octroi des autorisations, et en se réservant ainsi la possibilité d'en rétablir une stricte application.

Le Comité R se demande néanmoins si l'article 120*ter* du Code pénal et l'arrêté royal du 21 février 1939 ne devraient pas être revus et adaptés compte tenu du nouvel environnement juridique international, d'une part, de l'évolution technologique en matière d'observation spatiale et aérienne, d'autre part.

Le Comité R pense que la protection des objectifs militaires à l'égard de prises de vues à des fins hostiles ou d'espionnage pourrait être assurée dans un cadre juridique similaire à la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

HOOFDSTUK 6

VERSLAG VAN HET ONDERZOEK NAAR « HET EVENTUELE TOEZICHT DOOR DE ADIV OP EEN SYNDICALE BETOGING VAN MILITAIREN »

1. Inleiding

Op woensdag 19 juli 2000 betoogden militairen voor het kabinet van de minister van Landsverdediging. Deze betoging werd georganiseerd door de CCOD (Christelijke Centrale der openbare diensten) en had tot doel bepaalde looneisen kracht bij te zetten.

Het Comité I vernam dat leden van de ADIV op de plaats van de betoging aanwezig zouden zijn geweest en pogingen zouden hebben ondernomen om de identiteit van de deelnemers vast te stellen door ze op discrete wijze te ondervragen. Ze waren echter niet onopgemerkt gebleven.

Het Comité I wilde deze informatie nagaan en te weten komen of de ADIV de gewoonte heeft rechtstreeks of onrechtstreeks toezicht te houden op syndicale betogingen van militairen.

Indien dit inderdaad het geval zou zijn, hoe kan men een dergelijk toezicht dan rechtvaardigen in het kader van de wettelijke opdrachten van de ADIV? Zou een dergelijk toezicht niet indruisen tegen de rechten van vrije meningsuiting en van vereniging die militairen genieten, net als de andere burgers?

CHAPITRE 6

RAPPORT DE L'ENQUÊTE SUR « LA SURVEILLANCE ÉVENTUELLE D'UNE MANIFESTATION SYNDICALE DE MILITAIRES PAR LE SGR »

1. Introduction

Le mercredi 19 juillet 2000 eut lieu une manifestation de militaires devant le cabinet du ministre de la Défense nationale organisée par la CCSP (Centrale chrétienne des services publics) à l'appui de revendications salariales.

Une information est parvenue au Comité R selon laquelle des membres du SGR auraient été présents sur les lieux de cette manifestation et auraient cherché à relever l'identité des participants en les interrogeant discrètement, sans toutefois réussir à passer inaperçus.

Le Comité R a voulu vérifier cette information et savoir s'il était coutumier pour le SGR de surveiller, directement ou indirectement, des manifestations syndicales de militaires.

Dans l'affirmative, comment une telle surveillance peut-elle se justifier par rapport aux missions légales du SGR? Ne serait-elle pas contraire aux droits de libre expression et l'association dont jouissent les militaires à l'instar des autres citoyens?

2. Procedure

Op zijn vergadering van woensdag 23 augustus 2000 besliste het Comité I een onderzoek te openen naar «het eventuele toezicht door de ADIV op een syndicale betoging van militairen».

Met een kantschrift van 28 augustus 2000 gaf de voorzitter van het Comité I aan de Dienst enquêtes de opdracht bij de ADIV de nodige controles te verrichten.

Overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, werd de voorzitter van de Senaat in kennis gesteld van de opening van dit onderzoek met een schrijven van 31 augustus 2000.

De minister van Landsverdediging werd op diezelfde datum, krachtens artikel 43-1º van dezelfde wet, op de hoogte gebracht van de opening van het onderzoek.

Op 18 oktober 2000 is de Dienst enquêtes van het Comité I overgegaan tot het verhoor van het Hoofd van de Dienst militaire veiligheid van de ADIV.

Op 20 oktober 2000 diende de Dienst enquêtes zijn verslag in bij het Comité I.

Het Comité I heeft dit verslag op 14 november 2000 onderzocht. Vervolgens werd op 17 november 2000 een aanvullend kantschrift verstuurd naar de Dienst enquêtes.

Op 19 februari 2001 heeft de Dienst enquêtes zijn aanvullend verslag bezorgd aan het Comité I.

Het Comité I gaf op 22 februari 2001 zijn goedkeuring aan dit verslag.

Op 25 april 2001 heeft de minister van Landsverdediging aan het Comité I schriftelijk laten weten dat hij geen opmerkingen wenste te formuleren wat betreft de publicatie van dit verslag.

3. Vaststellingen

Zoals dit het geval is bij elke betoging op de openbare weg, heeft de rijkswacht, met het oog op het handhaven van de orde, toezicht gehouden op de syndicale bijeenkomst van militairen die op 19 juli 2000 door de CCOD (Christelijke Centrale der openbare diensten) werd georganiseerd voor het kabinet van de minister van Landsverdediging, met als doel bepaalde looneisen kracht bij te zetten.

Onder de betogers liep het gerucht dat de ADIV aanwezig was. Het Comité I heeft echter vastgesteld dat de ADIV niet de opdracht had gekregen toezicht te houden op deze syndicale actie. Het onderzoek heeft geen enkel element aan het licht gebracht waaruit men kan opmaken dat er in werkelijkheid wel toezicht is gehouden. Geen enkel lid van de ADIV was

2. Procedure

Réuni le mercredi 23 août 2000, le Comité R a décidé d'ouvrir une enquête sur la surveillance éventuelle d'une manifestation syndicale de militaires par le SGR.

Par apostille du 28 août 2000, le président du Comité R a chargé le Service d'enquêtes de procéder à des vérifications auprès du SGR.

Le président du Sénat, a été averti de l'ouverture de cette enquête par lettre du 31 août 2000, conformément à l'article 32 de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements.

Le ministre de la Défense nationale, a été averti de l'ouverture de cette enquête par lettre du 31 août 2000, conformément à l'article 43-1º de la même loi.

Le Service d'enquêtes du Comité R a procédé à l'audition du chef du Service de la sécurité militaire du SGR en date du 18 octobre 2000.

Le Service d'enquêtes a déposé son rapport au Comité R le 20 octobre 2000.

Ce rapport a été examiné par le Comité R le 14 novembre 2000, à la suite de quoi une apostille complémentaire a été adressée au Service d'enquêtes le 17 novembre 2000.

Le rapport complémentaire du Service d'enquêtes a été remis au Comité R le 19 février 2001.

Le présent rapport a été approuvé par le Comité R le 22 février 2001.

Par courrier du 25 avril 2001, le ministre de la Défense nationale a fait part au Comité R qu'il n'avait aucune remarque à formuler quant à la publication du présent rapport.

3. Constatations

Comme dans chaque cas de manifestation organisée sur la voie publique, le rassemblement syndical de militaires organisé le 19 juillet 2000 devant le cabinet du ministre de la Défense nationale par la CCSP (centrale chrétienne des services publics) à l'appui de revendications salariales a fait l'objet d'une surveillance de la part de la gendarmerie en vue du maintien de l'ordre.

Une rumeur a couru parmi les manifestants selon laquelle le SGR aurait été présent parmi eux. Cependant, le Comité R a constaté qu'aucun ordre n'avait été donné au SGR en vue de surveiller cette activité syndicale. Aucun élément de l'enquête ne permet de conclure qu'il en aurait été autrement dans la réalité. Aucun membre du SGR n'a été présent sur les lieux de

aanwezig op de plaats van de betoging, en de Rijkswacht en de ADIV hebben over deze betoging geen informatie uitgewisseld.

De ADIV volgt een gedragslijn waarbij deze dienst geen toezicht houdt op de syndicale activiteiten van de militairen, zolang er geen activiteiten worden gevoerd die een bedreiging vormen voor het land of voor de veiligheid van de strijdkrachten.

HOOFDSTUK 7

VERSLAG VAN HET ONDERZOEK NAAR DE MANIER WAAROP DE VEILIGHEID VAN DE STAAT HAAR NIEUWE OPDRACHT INZAKE DE BESCHERMING VAN HET WETENSCHAPPELIJK OF ECONOMISCH POTENTIEEL VAN HET LAND VERVULT

1. Inleiding

« Vandaag zijn conflicten niet langer systematisch open of bekendgemaakt. Vooral daden van economische agressie verlopen veel meer in het geniep en kunnen onze moderne samenlevingen ernstig uit evenwicht brengen. De 21e eeuw, die ongetwijfeld de eeuw van de complexiteit wordt, vereist nu reeds dat we een allesomvattende strategie bedenken en in de praktijk brengen waarmee we de uitdaging kunnen aangaan. De samenhang en de doeltreffendheid van die strategie zullen pas gegarandeerd zijn indien de burgermaatschappij en de Staat voortdurend en in beide richtingen met elkaar blijven communiceren » (1).

Marc Ladreit de Lacharrière, voorzitter van het *Institut d'études et de recherches pour la sécurité des entreprises* (Parijs)

1.1. Voorwerp van het onderzoek

In 1998, terwijl in het Parlement werd gedebatteerd over het ontwerp van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten, voerde het Comité I een onderzoek met de bedoeling de politieke overheden het belang te doen inzien van deze nieuwe opdracht inzake de bescherming van het wetenschappelijk of economisch potentieel van het land (2).

In zijn aanbevelingen die uit dit onderzoek voortvloeiden, had het Comité I gepleit voor de oprichting van een overlegorgaan tussen enerzijds de ministers bevoegd voor deze materie en anderzijds de ondernemingen die een voor België essentieel wetenschappelijk of economisch potentieel bezitten.

(1) Vrije vertaling.

(2) Comité I, jaarverslag 1998, blz. 76.

cette manifestation. Il n'y a eu aucun échange d'informations entre la gendarmerie et le SGR à son sujet.

Le SGR a pour ligne de conduite de ne pas surveiller les activités syndicales des militaires aussi longtemps qu'aucune activité menaçante pour le pays ou pour la sécurité des forces armées ne s'y développe.

CHAPITRE 7

RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LA SÛRETÉ DE L'ÉTAT S'ACQUITTE DE SA NOUVELLE MISSION DE PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE

1. Introduction

« Aujourd'hui, les conflits ne sont plus systématiquement ouverts ni déclarés. Les agressions économiques notamment sont plus sournoises, elles peuvent déstabiliser gravement nos sociétés modernes. Le XXI^{e} siècle, qui sera celui de la complexité, nécessite dès aujourd'hui la conception et la mise en oeuvre d'une stratégie globale répondant au défi. La cohérence et l'efficacité de cette démarche ne seront garanties que si la société civile et l'État maintiennent des échanges permanents et translatéraux » (1).

Marc Ladreit de Lacharrière président de l'Institut d'études et de recherches pour la sécurité des entreprises (Paris)

1.1. Objet de l'enquête

Au cours de l'année 1998, alors que le Parlement débattait du projet de loi organique des services de renseignement et de sécurité, le Comité R a mené une enquête en vue de sensibiliser les autorités politiques sur l'importance de cette nouvelle mission de protection du potentiel scientifique et économique (2).

Dans les recommandations résultant de son enquête, le Comité R avait préconisé la création d'un organe de concertation entre les ministres concernés par cette matière et les entreprises détentrices d'un potentiel scientifique et économique vital pour la Belgique.

(2) Comité R, rapport d'activités 1998, p. 70 (fr.).

Het Comité I had er ook op gewezen dat men niet mocht nalaten aan de Veiligheid van de Staat de middelen toe te kennen die deze dienst vroeg; zoniet bestond het gevaar dat de nieuwe wet dode letter zou blijven.

Sindsdien is de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten in werking getreden. Artikel 7 van deze wet belast de veiligheid van de Staat met een aantal opdrachten, waaronder «het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die (...) het wetenschappelijk of economisch potentieel, zoals gedefinieerd door het Ministerieel Comité (van Inlichtingen en Veiligheid) bedreigt of zou kunnen bedreigen.»

Twee jaar na de inwerkingtreding van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, onderzocht het Comité I hoe de Veiligheid van de Staat zich van deze nieuwe opdracht heeft gekweten.

Daartoe heeft het Comité I om te beginnen een rijke documentatie afkomstig uit open bronnen (persartikels, boeken, gespecialiseerde tijdschriften, websites enz.) verzameld en geraadpleegd, teneinde een algemeen beeld te krijgen van de problematiek inzake de bescherming van het wetenschappelijk en economisch potentieel. Op basis van zijn eigen opzoekingen heeft het Comité vervolgens een algemeen rapport opgesteld dat het voorwerp is van de inleiding van dit verslag.

1.2. Procedure

Het Comité I heeft beslist dit onderzoek te openen op 14 februari 2000.

Het Comité I heeft de documenten en interne nota's van de Veiligheid van de Staat bestudeerd, waarover het beschikte krachtens artikel 33 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten: het heeft daarin gezocht naar alle beschikbare informatie en naar eender welke richtlijnen gegeven in het kader van de uitvoering van haar nieuwe opdracht.

Op 2 maart 2000 hebben de leden van het Comité I de administrateur-generaal, *ad interim* van de Veiligheid van de Staat, verhoord in het kader van het aanvullend onderzoek dat de Senaat had gevraagd met betrekking tot het interceptiesysteem «Echelon».

Tijdens dit verhoor werden ook vragen gesteld betreffende de uitvoering van de nieuwe opdracht inzake de bescherming van het wetenschappelijk en economisch potentieel.

Teneinde beter vertrouwd te raken met de praktijken op het gebied van economische inlichtingen, heeft een lid van het Comité I op 16 en 17 mei 2000 in Parijs

Le Comité R avait également indiqué qu'il ne faudrait pas négliger de fournir à la Sûreté de l'État les moyens qu'elle réclamait, au risque de voir la future disposition législative rester lettre morte.

Depuis lors, est entrée en vigueur la loi du 30 novembre 1998 organique des services de renseignement et de sécurité dont l'article 7 donne à la Sûreté de l'État entre autres missions, celle «de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer (...) le potentiel scientifique et économique défini par le Comité ministériel (du Renseignement)».

Deux années après la mise en vigueur de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, le Comité R a examiné de quelle manière la Sûreté de l'État avait pris en charge sa nouvelle mission.

Pour ce faire, le Comité R a d'abord réuni et consulté une abondante documentation issue de sources ouvertes (articles de presse, livres, revues spécialisées, websites, etc.) afin de se forger une idée générale sur la problématique de la protection du potentiel scientifique et économique. À partir de sa propre recherche, le Comité R a élaboré un rapport d'ordre général repris en introduction du présent rapport d'enquête.

1.2. Procédure

Le Comité R a décidé d'ouvrir cette enquête le 14 février 2000.

Le Comité R a examiné les documents et notes internes de la Sûreté de l'État dont il était en possession en vertu de l'article 33 de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements: il y a recherché toutes les informations disponibles et toutes les instructions données à propos de l'exécution de la nouvelle mission.

Le 2 mars 2000, les membres du Comité R ont entendu Mme G. Timmermans, administrateur général *ad interim* de la Sûreté de l'État, dans le cadre de l'enquête complémentaire demandée par le Sénat sur le système d'interception «Echelon».

À cette occasion, des questions ont aussi été posées sur l'exécution de la nouvelle mission de protection du potentiel scientifique et économique.

Pour se familiariser avec les pratiques du renseignement (ou intelligence) économique, le Comité R a envoyé un de ses membres à Paris les 16 et 17 mai 2000

een seminarie bijgewoond met als thema «Maîtriser les outils de la veille et de l'intelligence économique».

Met een kantschrift van 7 juni 2000 heeft de voorzitter van het Comité I aan de Dienst Enquêtes de opdracht gegeven bepaalde controles te verrichten.

Overeenkomstig artikel 43-1º van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten heeft het hoofd van de Dienst Enquêtes de minister van Justitie per brief van 7 juni 2000 kennis gegeven van de opening en het voorwerp van het onderzoek.

Op dinsdag 4 juli 2000 organiseerde het Comité I een informatievergadering met twee vertegenwoordigers van het Verbond van Belgische Ondernemingen, namelijk de heren Marc Verschaeve, administratief directeur, en Yvan De Mesmaeker (ir.), veiligheidsadviseur.

Op 23 november 2000 heeft de Dienst Enquêtes zijn rapport bezorgd aan het Comité I.

Er werd over deze materie gecorrespondeerd met de Veiligheid van de Staat.

Dit verslag werd door het Comité I goedgekeurd op 23 januari 2001.

De minister van Justitie heeft op 13 maart 2001 een aantal opmerkingen geformuleerd waarmee het Comité I heeft rekening gehouden. Hij is van mening dat het opportuun zou zijn, mits akkoord van het Comité I, dat dit rapport overgemaakt wordt aan de werkgroep op het kabinet van de eerste minister die belast is met het voorbereiden van de richtlijnen van het Ministerieel Comité voor inlichting.

1.3. Belangstelling van het Parlement

1.3.1. Het Belgisch Parlement

Samen met de amendementen ingediend bij de bespreking van het ontwerp van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten, heeft het Comité I de volgende parlementaire vragen en interpellaties teruggevonden met betrekking tot de materie die het voorwerp is van dit rapport:

— Vragen nr. 870/1 en nr. 870/2 d.d. 16 februari 1998 van senator Boutmans (Agalev) aan de ministers van Economische Zaken en van Landsverdediging. Voor zover het Comité I weet, zijn deze vragen nog onbeantwoord op de datum van goedkeuring van dit rapport(1). Deze vragen hadden betrekking op de toepassing van de wet d.d. 10 januari 1955 betreffende de bekendmaking en de toepassing der uitvindingen

(1) 22 januari 2001.

pour assister à un séminaire intitulé «Maîtriser les outils de la veille et de l'intelligence économique».

Par apostille du 7 juin 2000, le Président du Comité R a chargé le Service d'enquêtes de procéder à certaines vérifications.

Par courrier du 7 juin 2000, conformément à l'article 43-1º de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le ministre de la Justice a été averti de l'ouverture et de l'objet de l'enquête par les soins du Chef du Service d'enquêtes.

Le mardi 4 juillet 2000, le Comité R a tenu une réunion d'information avec deux représentants de la Fédération des entreprises de Belgique, MM. Marc Verschaeve, directeur administratif, et Yvan De Mesmaeker (ir.), conseiller en sécurité.

Le Service d'enquêtes a transmis son rapport au Comité R le 23 novembre 2000.

Des courriers ont été échangés avec la Sûreté de l'État sur le sujet.

Le présent rapport a été approuvé le 23 janvier 2001.

Le ministre de la Justice a formulé des remarques dont le Comité R a tenu compte dans le présent rapport. Dans son courrier du 13 mars 2001, le ministre de la Justice estimait opportun avec l'accord du Comité R de transmettre ce rapport au groupe de travail relevant du Cabinet de M. le premier ministre chargé de préparer les directives du Comité ministériel de renseignement.

1.3. L'intérêt parlementaire

1.3.1. Le Parlement belge

Outre les amendements déposés à l'occasion de la discussion du projet de loi organique des services de renseignement et de sécurité, le Comité R a relevé les questions et interpellations parlementaires suivantes sur le sujet:

— Questions nº 870/1 et 870/2 du 16 février 1998 posée par le sénateur Boutmans (Agalev) aux ministres des Affaires économiques et de la Défense nationale. À la connaissance du Comité R, aucune réponse n'a encore été donnée à cette question à la date d'approbation du présent rapport(1). La question portait sur l'application de la loi du 10 janvier 1955 concernant la mise en œuvre des inventions et des

(1) 22 janvier 2001.

en fabrieksgeheimen welke de verdediging van het grondgebied of de Veiligheid van de Staat aangaan (1).

— Interpellatie nr. 84 van de heer Bourgeois, volksvertegenwoordiger (VU-ID), op 20 oktober 1999 aan de minister van Justitie over « de economische oorlog en de rol van de Veiligheid van de Staat en het parket » (2).

Naast deze vragen en interpellaties, heeft het Belgisch Parlement recentelijk gedebatteerd over de hele problematiek van het interceptienetwerk Echelon.

In het STOA-rapport dat aan het Europees Parlement is overgelegd, worden enkele gevallen beschreven waarin Europese bedrijven belangrijke overheidsopdrachten zouden zijn misgelopen tengevolge van de interceptie van hun communicatie tijdens internationale handelstransacties (*Panavia European Fighter Aircraft Consortium, Thomson CSF, Airbus Industrie*).

1.3.2. Het Europees Parlement

Op de vergadering van woensdag 5 juli 2000 in Straatsburg heeft het Europees Parlement zich uitgesproken over de oprichting van een tijdelijke onderzoekscommissie betreffende het telecommunicatie-interceptiesysteem Echelon.

Tijdens de voorafgaande discussies in de commissie Vrijheden en Rechten van de burgers, Justitie en Binnenlandse Zaken verklaarde de Duitse gedeputeerde Martin Schulz (PSE) op 5 april 2000 dat niet alleen de Verenigde Staten en het Verenigd Koninkrijk, maar ook andere landen zoals Frankrijk, Nederland en... België activiteiten van economische spionage beoefenden (3).

2. Poging tot een algemene beschrijving van de problematiek

Om de opdracht inzake bescherming van het wetenschappelijk en economisch potentieel, toevertrouwd aan de Veiligheid van de Staat, te beschrijven, moet men eerst en vooral de volgende vier fundamentele vragen stellen :

1. Wat is het wetenschappelijk of economisch potentieel van een land en, in het bijzonder, dat van België ?

(1) Senaat, Bulletin van *Vragen en Antwoorden* - nr. 1-69.

(2) Kamer, 2e zitting van de 50e legislatuur (HA 50 COM 025).

(3) *Cf.* www.europarl.eu.int/, verklaring ook te vinden op : homeusers.brutele.be/cdc/euro.htm.

secrets de fabrique intéressant la défense du territoire ou la Sûreté de l'État (1).

— Interpellation nº 84 de M. le député Bourgeois (VU-ID), le 20 octobre 1999, au ministre de la Justice sur « la guerre économique et le rôle de la Sûreté de l'État et du Parquet » (2).

À ces questions et interpellations, on peut aussi également joindre les récents débats au Parlement belge concernant la problématique du réseau d'interception « Echelon ».

Le rapport STOA présenté au Parlement européen cite en effet quelques cas dans lesquels des firmes européennes auraient été évincées de marchés importants par suite de l'interception de leurs communications au cours de transactions commerciales internationales (*Panavia European Fighter Aircraft consortium, Thomson CSF, Airbus industrie*).

1.3.2. Le Parlement européen

Réuni le mercredi 5 juillet 2000 à Strasbourg, le Parlement européen s'est prononcé sur la constitution d'une commission temporaire d'enquête sur le système d'interception des télécommunications « Echelon ».

Au cours des discussions préalables qui se sont tenues au sein de la commission des Libertés et des droits des citoyens, de la Justice et des Affaires intérieures, le député allemand Martin Schulz (PSE) a déclaré le 5 avril 2000 que l'espionnage économique n'était pas seulement pratiqué par les États-Unis et le Royaume Uni, mais aussi par d'autres pays comme la France, les Pays-Bas et ... la Belgique (3).

2. Essai de description générale de la problématique

Décrire la mission de protection du potentiel scientifique et économique confiée à la Sûreté de l'État nécessite que soient posées les quatre questions fondamentales suivantes :

1. Qu'est-ce que le potentiel scientifique et économique d'un pays et, singulièrement, celui de la Belgique ?

(1) Sénat, *Questions et Réponses* - bulletin nº 1-69.

(2) Chambre, 2e session de la 50e législature (HA 50 COM 025).

(3) *Cf.* www.europarl.eu.int/, déclaration aussi disponible sur : homeusers.brutele.be/cdc/euro.htm.

2. Wie zijn de actoren betrokken bij de ontwikkeling van het wetenschappelijk en economisch potentieel van een land?

3. Aan welke bedreigingen is het wetenschappelijk en economisch potentieel van een land blootgesteld?

4. Welke acties en middelen kan een inlichtingendienst ontwikkelen om het wetenschappelijk en economisch potentieel van een land te beschermen?

2.1. Wat is het wetenschappelijk of economisch potentieel van een land?

Al in het eerste verslag dat het Comité I aan deze materie heeft gewijd, wees het erop dat het moeilijk is een precieze definitie te geven van het begrip «wetenschappelijk of economisch potentieel».

Volgens de artikelen 7, 1º, en 8, 4º, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, wordt met «wetenschappelijk of economisch potentieel» bedoeld: «de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel».

Het is de taak van het Ministerieel Comité Inlichtingen en Veiligheid dit begrip nauwkeuriger te beschrijven.

In juli 2000 kreeg de ministerraad kennis van een beleidsnota van de minister van Economie en Wetenschappelijk Onderzoek betreffende de evolutie van het federaal wetenschapsbeleid.

Het Comité I is in dit document op zoek gegaan naar een aantal elementen die konden toelaten het begrip «wetenschappelijk of economisch potentieel» preciezer te beschrijven.

In de nota staat dat de economie voortaan steunt op de kennis; de auteur benadrukt dat ongeveer 50 % van de economische groei verband houdt met de nieuwe technologieën en de nieuwe producten.

Bijgevolg is het wetenschappelijk onderzoek heel belangrijk geworden, op Europees en nationaal niveau. In België valt het wetenschapsbeleid onder de bevoegdheid van de Federale Diensten voor Wetenschappelijke, Technische en Culturele Aangelegenheden (afgekort DWTC).

Deze beleidsnota bevat nauwelijks enige informatie over geavanceerd wetenschappelijk onderzoek in België, maar legt wel de nadruk op de kwaliteit van het onderzoek, de technologieën en de toepassingen met betrekking tot de ruimtevaart in België.

De minister van Economie en Wetenschappelijk Onderzoek kondigt slechts aan dat hij de bedoeling heeft het wetenschappelijk potentieel te laten evalueren dat aanwezig is binnen de «technologische groeipolen» (TGP) en de «interuniversitaire groeipolen» (IGP) in België.

2. Qui sont les acteurs concernés par le développement du potentiel scientifique et économique d'un pays?

3. À quelles menaces est exposé le potentiel scientifique et économique d'un pays?

4. Quelles actions et quels moyens un service de renseignement peut-il mettre en œuvre pour protéger le potentiel scientifique et économique d'un pays?

2.1. Qu'est-ce que le potentiel scientifique et économique d'un pays?

Le premier rapport que le Comité R a consacré à cette matière faisait déjà apparaître la difficulté de cerner la notion de potentiel scientifique et économique.

Au sens des articles 7, 1º, et 8, 4º, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, on entend par «potentiel scientifique et économique», «la sauvegarde des éléments essentiels du potentiel scientifique et économique».

Il appartient au Comité ministériel du Renseignement et de la sécurité de définir plus avant cette notion.

En juillet 2000, le Conseil des ministres a pris connaissance d'une note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale.

Le Comité R a cherché dans ce document quelques éléments susceptibles de préciser davantage la notion de potentiel scientifique et économique.

Cette note indique que l'économie est désormais fondée sur la connaissance; elle souligne qu'environ 50 % de la croissance économique est liée aux nouvelles technologies et aux nouveaux produits.

La recherche scientifique est donc devenue une préoccupation majeure tant au niveau européen que national. En Belgique, la politique scientifique ressort des Services fédéraux des Affaires scientifiques, techniques et culturelles (SSTC en abrégé).

La note d'orientation ne donne guère d'indications sur les recherches scientifiques de pointe effectuées en Belgique; elle souligne cependant la qualité des recherches, des technologies et des applications spatiales en Belgique.

Le ministre de l'Économie et de la Recherche scientifique annonce seulement son intention de procéder à une évaluation du potentiel scientifique présent dans les «pôles d'attractions technologiques» (PAT) et «pôles d'attractions interuniversitaires» (PAI) en Belgique.

Voorts verklaart hij dat hij zich voorneemt «ambtenaren belast met de prospectie in de geavanceerde sectoren ter beschikking te stellen van de federale onderzoekscentra en van de platformen universiteiten-ondernemingen aan de Belgische universiteiten, teneinde onze capaciteit inzake technologische transfers te versterken».

Il annonce aussi son intention «de mettre à la disposition des centres de recherches fédéraux et des Interfaces universités-entreprises des universités belges, des agents chargés de la prospection dans les secteurs de pointe afin de renforcer notre capacité de transferts technologiques».

Het begrip economische veiligheid, dat een logisch uitvloeisel is van het vorige begrip, is een algemene doelstelling die in principe door eender welke regering moet worden nagestreefd. Dit begrip werd als volgt gedefinieerd door de Canadese inlichtingendienst voor de veiligheid:

La notion corollaire de sécurité économique, objectif général auquel doivent en principe tendre tous les gouvernements, a été définie comme suit par le Service canadien du renseignement de sécurité:

«De tijd waarin de wereldveiligheid voorrang kreeg op economische bekommernissen en regionale conflicten in de internationale betrekkingen is voorgoed voorbij. De steeds grotere economische interdependentie en internationale concurrentie zijn belangrijke oorzaken van spanningen en conflicten tussen de wereldmachten geworden.

In dit klimaat van onzekerheid worden de geïndustrialiseerde landen enerzijds, die hun levensstandaard absoluut willen behouden, en de ontwikkelingslanden anderzijds, die al even vastberaden zijn hun levensstandaard te verbeteren, ertoe aangezet alle middelen waarover ze beschikken te gebruiken om hun productiviteit te verhogen en hun economische veiligheid te verzekeren. Economische spionage is een van die middelen (...)» (2).

«L'époque où la question de la sécurité mondiale primait sur les préoccupations d'ordre économique et les conflits régionaux dans les relations internationales est révolue. L'interdépendance économique et la concurrence internationale croissantes sont devenues des sources importantes de tensions et de conflits entre les puissances mondiales.

Dans ce climat d'incertitude, les pays industrialisés qui désirent vivement maintenir leur niveau de vie et les pays en développement qui sont tout aussi déterminés à améliorer le leur sont poussés à utiliser tous les moyens à leur disposition pour améliorer leur productivité et assurer leur sécurité économique. L'un de ces moyens est l'espionnage économique (...)» (1).

In Frankrijk betekent economische veiligheid dat men erop toeziet dat de middelen, de kennis of de informatie die toelaten de fundamentele belangen van de natie te beschermen, worden bewaard onder Frans toezicht en dat ze voortdurend worden ontwikkeld en aangepast in functie van de evolutie van de context en van de mondiale geostrategische risico's (3).

En France, la sécurité économique consiste à veiller à ce que les moyens, connaissances ou informations permettant de préserver les intérêts essentiels de la nation, soient conservés sous le contrôle français et qu'ils soient développés et adaptés en permanence à l'évolution du contexte et des risques géo-stratégiques mondiaux (2).

In Canada verstaat men onder «economische veiligheid» het feit de passende voorwaarden in stand te houden met het oog op het bevorderen van een aanhoudende relatieve toename, op lange termijn, van de productiviteit van arbeid en kapitaal. Dit garandeert voor de bevolking een hoge en steeds toenemende levensstandaard, en behoudt men een rechtvaardige,

Au Canada, on entend par sécurité économique le fait de maintenir des conditions propres à favoriser une augmentation relative soutenue et à long terme de la productivité du travail et du capital, ce qui assure à la population un niveau de vie élevé et en progression constante, et garantit un environnement économique équitable, sûr et dynamique, propice aux innova-

---

(1) *Cf.* www.europarl.eu.int/, verklaring ook te vinden op: homeusers.brutele.be/cdc/euro.htm.

(2) Vrije vertaling — «La sécurité économique», rapport van de Canadese inlichtingendienst voor de veiligheid, verschenen in *Série d'aperçus*, nr. 6, mei 1998 — www.csis-scrs.gc.ca.

(3) «De la défense économique à la sécurité de l'économie», Jean-Louis Levet — rapport van het Franse «Commissariatgénéral du Plan» — 1997.

(1) *Cf.* www.europarl.eu.int/, déclaration aussi disponible sur: homeusers.brutele.be/cdc/euro.htm.

(2) «La sécurité économique», rapport du Service canadien du renseignement de sécurité paru dans *Série d'aperçus* nº 6, mai 1998 — www.csis-scrs.gc.ca.

(3) «De la défense économique à la sécurité de l'économie», Jean-Louis Levet — rapport du Commissariat général du Plan, 1997.

veilige en dynamische economische omgeving waar vernieuwingen en binnen- en buitenlandse investeringen gedijen en waar er sprake is van constante groei (2).

2.2. Wie zijn de drijvende krachten achter het wetenschappelijk en economisch potentieel van een land ?

In verband hiermee wordt de situatie gekenmerkt door de diversificatie en de toenemende heterogeniteit van de drijvende krachten achter het wetenschappelijk en economisch potentieel van een land.

Naast de Staat zelf, zijn infrastructuren (materieel of virtueel), zijn diensten en zijn autonome overheidsbedrijven (bijvoorbeeld NMBS, Belgacom enz.), zijn er ook de gefedereerde entiteiten (gemeenschappen en gewesten), de universiteiten, hogescholen en andere organen van openbaar belang, vernieuwende private bedrijven met een hoge toegevoegde waarde, onderzoekslaboratoria, alsook hun werknemers die, elk met hun eigen logica — van openbare dienstverlening of winstoogmerk — een belangrijke plaats innemen, niet alleen op het vlak van de handelseconomie, maar ook in het wetenschappelijk en technologisch onderzoek, collectieve diensten, de cultuursector en de internationale betrekkingen.

Dit veronderstelt dat een lijst wordt opgemaakt van essentiële activiteiten die binnen deze verschillende sectoren moeten worden beschermd, en dat ze tevens volgens hun belang worden gerangschikt. Men moet echter beseffen dat de industriële herstructureringen en de globalisering van procédés in de hele wereld het bijzonder moeilijk maken de nationaliteit van een onderneming vast te stellen.

Politieke verantwoordelijken, directeuren, ambtenaren, kaderleden, onderzoekers en andere personeelsleden die bijdragen tot de ontwikkeling van het wetenschappelijk of economisch potentieel, moeten zich bewust zijn van de activiteiten die een bedreiging kunnen vormen voor hun sector, alsook van hetgeen ze kunnen doen om hun sector te beschermen.

2.3. Aan welke bedreigingen is het wetenschappelijk en economisch potentieel van een land blootgesteld ?

Bedreigingen die ontspruiten aan de menselijke boosaardigheid zijn van uiteenlopende aard, zoals :

— terrorisme, sabotage gericht op de materiële vernietiging van infrastructuren;

(1) « De la défense économique à la sécurité de l'économie », Jean-Louis Levet — rapport van het Franse « Commissariatgénéral du Plan » — 1997.

(2) *Série d'aperçus*, nr. 6 — mei 1998 — publicatie van de Canadese inlichtingendienst voor de veiligheid.

tions, aux investissements intérieurs et étrangers, ainsi qu'une croissance soutenue (1).

2.2. Qui sont les moteurs du potentiel scientifique et économique d'un pays ?

À cet égard, la situation se caractérise par la diversification et l'hétérogénéité croissante des moteurs du potentiel scientifique et économique d'un pays.

À côté de l'État lui-même, de ses infrastructures (physiques ou virtuelles), de ses services, entreprises publiques autonomes (SNCB, Belgacom, etc.), on trouve les entités fédérées (communautés et régions), les universités, hautes écoles et autres organismes d'intérêt public, les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires de recherches, ainsi que leurs personnels qui, chacun avec une logique propre, les uns de service public, les autres de profit, occupent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

Ceci implique qu'une liste de secteurs d'activités vitales à protéger dans ces différents secteurs soit établie en définissant un ordre de priorité. Il faut toutefois être conscient que les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises.

Les responsables politiques, dirigeants, fonctionnaires, cadres, chercheurs et autres membres du personnel participant au développement du potentiel scientifique et économique, doivent être conscients des activités qui peuvent menacer leur secteur et du rôle qu'ils peuvent jouer pour le protéger.

2.3. À quelles menaces est exposé le potentiel scientifique et économique d'un pays ?

Les menaces issues d'une volonté humaine malveillante sont de plusieurs natures parmi lesquelles :

— le terrorisme, le sabotage visant la destruction physique d'infrastructures;

(1) « De la défense économique à la sécurité de l'économie », Jean-Louis Levet — rapport du Commissariat général du Plan, 1997.

(2) *Série d'aperçus* nº 6 — mai 1998, publication du Service canadien de renseignement de sécurité.

— het destabiliseren van de economie door corruptie, het binnenbrengen en witwassen van kapitalen afkomstig van criminele activiteiten (1), desinformatie, enz.

— het roven van informatie, spionage.

In dit rapport besteden we vooral aandacht aan deze laatste soort bedreiging, namelijk spionage. We proberen een onderscheid te maken tussen spionage en economische inlichtingenactiviteiten.

3. Spionage — Economische inlichtingen — Economische «Intelligence» — Algemene definities

In het onderhavige rapport worden de begrippen «economische inlichtingen», «economische «intelligence» en «economische of bedrijfsspionage» herhaaldelijk gebruikt. Deze begrippen zijn het voorwerp van talrijke, min of meer gelijkluidende definities, naargelang de opsteller. De Canadese inlichtingendienst voor de veiligheid heeft ze als volgt gedefinieerd.

Economische spionage is het feit waarbij een overheid gebruik maakt van, of het gebruik bevordert, van illegale, clandestiene, dwingende of bedrieglijke middelen om zonder toelating toegang te krijgen tot economische of technologische inlichtingen in exclusieve eigendom, teneinde er economische voordelen uit te halen (2).

Bedrijfsspionage is het feit waarbij een privaat orgaan of zijn vertegenwoordigers gebruik maakt van, of het gebruik bevordert, van illegale, clandestiene, dwingende of bedrieglijke middelen om zonder toelating toegang te krijgen tot economische of technologische inlichtingen in exclusieve eigendom, teneinde er economische voordelen uit te halen (3).

In een intern document, waarin de Veiligheid van de Staat voorstellen ter goedkeuring voorlegde aan het Ministerieel Comité inlichtingen en veiligheid, schreef deze dienst:

«Bezit de opdrachtgever van de spion de Belgische nationaliteit, dan gaat het om bedrijfsspionage en daarvoor is de Veiligheid van de Staat niet bevoegd. Is de opdrachtgever daarentegen afkomstig uit het buitenland, dan is er sprake van economische spionage, en de bestrijding daarvan sluit perfect aan bij de opdrachten van de Veiligheid van de Staat».

(1) In verband hiermee verwijzen we naar de jaarverslagen van de Cel voor financiële gegevensverwerking.

(2) «*Série d'aperçus*», nr. 6 — mei 1998, publicatie van de Canadese inlichtingendienst voor de veiligheid.

(3) Idem.

— la déstabilisation de l'économie par la corruption, l'introduction et le blanchiment de capitaux provenant d'activités criminelles (1), la désinformation, etc.

— la prédation de l'information ou l'espionnage.

Le présent rapport visera plus particulièrement cette dernière forme de menace qu'est l'espionnage. Il tentera de distinguer cette activité du renseignement ou de l'intelligence économique.

3. L'espionnage—Lerenseignementéconomique—L'intelligence économique — Définitions générales

Le présent rapport aura plusieurs fois recours aux notions de «renseignement économique«, «intelligence économique», «espionnage économique et industriel». Ces concepts font l'objet de nombreuses définitions plus ou moins semblables selon les écoles. Le Service canadien du renseignement de sécurité retient les définitions suivantes.

L'espionnage économique est le fait pour un gouvernement d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques (2).

L'espionnage industriel est le fait, pour un organisme du secteur privé ou ses représentants, d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques (3).

Dans un document interne soumettant des propositions à l'approbation du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'État écrit:

«Si le mandant de l'espion est de nationalité belge, il s'agit d'espionnage industriel et ce domaine n'est pas du ressort de la Sûreté de l'État. Si par contre, le mandant est originaire d'un pays étranger, il s'agit d'espionnage économique et la lutte contre cette activité s'inscrit parfaitement dans le cadre des missions de la Sûreté de l'État.»

(1) Voir à ce sujet ce qu'en disent les rapports annuels d'activités de la Cellule de traitement des informations financières.

(2) «*Série d'aperçus*», nº 6 — mai 1998, publication du Service canadien de renseignement de sécurité.

(3) Idem.

Volgens deze dienst zou de nationaliteit van de opdrachtgever van de spion dus bepalen of er sprake is van economische spionage dan wel van bedrijfsspionage.

Het Comité I heeft de administrateur-generaal van de Veiligheid van de Staat hierover ondervraagd, omdat het Comité I nogal wat voorbehoud maakt bij deze zienswijze.

Immers, als gevolg van de industriële herstructureringen en de globalisering van de procédés in de hele wereld is het vrij moeilijk de nationaliteit van een onderneming te bepalen.

Economische inlichtingen en economische «intelligence» zijn twee begrippen die elkaar aanvullen, maar toch duidelijk verschillen:

Met economische inlichtingen wordt bedoeld: alle economische inlichtingen van politieke of commerciële aard, met inbegrip van technologische, financiële en commerciële gegevens in exclusieve eigendom, alsook overheidsinformatie, die rechtstreeks of onrechtstreeks kunnen bijdragen tot de stijging van de productiviteit of tot de verbetering van de concurrentiepositie van de vreemde mogendheden die deze informatie verwerven (1).

Economische «intelligence» (intelligence économique) (2) kan op diverse manieren worden gedefinieerd.

In Frankrijk gaat het gewoonlijk om het geheel van gecoördineerde acties inzake het onderzoek, de verwerking en de verspreiding, met het oog op de exploitatie ervan, van de informatie nuttig voor de economische actoren (3).

Stevan Dedijer, de eerste geleerde die het begrip «economische intelligence» in de jaren zeventig aan de Universiteit van Lund (Zweden) heeft geformaliseerd, is van mening dat de rol van economische «intelligence» erin moet bestaan een voedingsbodem te zijn voor de «intuïtie van de beslissingnemers».

Sommigen echter aarzelen niet om «economische intelligence» voor te stellen als een doeltreffend gebruik van de informatie via activiteiten van lobbying en beïnvloeding, en zelfs van corruptie.

Een Frans onderzoeksteam, verbonden aan het «Centre des hautes études de l'armement (CHEAR)»,

(1) *«Série d'aperçus»*, nr. 6 — mei 1998, publicatie van de Canadese inlichtingendienst voor de veiligheid.

(2) Franstaligen geven vaak de voorkeur aan dit anglicisme boven de Franse term «renseignement économique» (economische inlichtingen), omdat ze vinden dat het beter uitdrukking geeft aan de rijkdom van deze activiteit en aan de omvang van de kennis en de cultuur die ermee gepaard gaan.

(3) Rapport van het 10e Franse plan (februari 1994), *«Intelligence économique et stratégique des entreprises»* (het rapport wordt vaak het «rapport-Martre» genoemd).

Pour ce service, ce serait donc la nationalité du mandant de l'espion qui ferait la différence entre espionnage économique et espionnage industriel.

Le Comité R a interrogé l'administrateur général de la Sûreté de l'État sur ce point de vue à l'égard duquel il émet de nettes réserves.

En effet, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises.

Le renseignement économique et l'intelligence économique sont deux notions complémentaires mais cependant distinctes.

On entend par renseignement économique toutes les informations économiques à caractère politique ou commercial, y compris les données technologiques, financières, commerciales en propriété exclusive, ainsi que les informations gouvernementales, qui sont susceptibles de contribuer directement ou indirectement à l'accroissement de la productivité ou à l'amélioration de la position concurrentielle des puissances étrangères qui en font l'acquisition (1).

L'intelligence économique (2) peut être définie de plusieurs manières.

En France, on la considère généralement comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques (3).

Stevan Dedijer, premier universitaire à avoir formalisé l'intelligence économique dans les années 70 à l'université de Lund (Suède), estime pour sa part qu'elle doit avoir pour rôle de nourrir les «intuitions des décideurs».

Mais certains n'hésitent pas à présenter l'intelligence économique comme une utilisation efficace de l'information à travers des activités de lobbying et d'influence, voir même de corruption.

Une équipe française de recherche associée au Centre des hautes études de l'armement (CHEAr)

(1) «*Série d'aperçus*» nº 6 — mai 1998, publication du Service canadien de renseignement de sécurité.

(2) Cet anglicisme est souvent préféré par les francophones au terme français «renseignement économique», car il leur paraît mieux refléter la richesse de cette activité et l'étendue des connaissances et de la culture qu'il met en œuvre.

(3) Rapport du Xe plan français (février 1994) «*Intelligence économique et stratégique des entreprises*» (souvent désigné sous l'appellation «rapport Martre»).

is de mening toegedaan dat, «aangezien concurrentie niet met oorlog kan worden gelijkgesteld, de activiteit inzake economische inlichtingen geen vorm van inlichtingenactiviteit is zoals de andere. Immers, men maakt daarbij vooral gebruik van open methodes en de vele actoren bevinden zich zowel in de openbare als in de private sector. Veeleer dan een niet passende vorm van economische spionage is de werkelijke inzet het creëren van een economisch informatienetwerk, teneinde de verspreiding van de informatie binnen de nationale economie te bevorderen, alsook bepaalde culturele zwakheden zoals het achterhouden van informatie te overstijgen» (1).

Sommige auteurs zijn de mening toegedaan dat economische informatie, naargelang deze activiteit wordt beoefend door ondernemingen of door Staten, niet steeds aan dezelfde logica beantwoordt.

Ze stellen het volgende schema voor (2):

Economische «Intelligence»	Van de ondernemingen	van de Staten
einddoel	het ontwikkelen van de onderneming,	economische macht,
doelwit	de producten,	de wereldmarkt,
zoekt in de eerste plaats naar	informatie gericht op de beroepen,	informatie gericht op de netwerken,
praktijk	lobbying,	beïnvloeding,
zoekt de informatie	op de particuliere informatiemarkt,	in het inlichtingenproces,
bezorgt de informatie	aan de algemeen directeur, de raad van bestuur,	aan de overheid bevoegd inzake economie,
is doordrongen	van de bedrijfscultuur,	van de inlichtingencultuur.

In werkelijkheid gaan met de praktijk van economische «intelligence» door de ondernemingen enerzijds, en door de staten anderzijds, wellicht heel wat minder clichés gepaard dan deze auteurs wel zouden willen.

Het Comité I van zijn kant stelt vast dat de doelstellingen van economische «intelligence», zoals deze activiteit wordt beoefend door de ondernemingen, niet altijd samenvallen met het instandhouden van de economische macht van een Staat.

(1) Vrije vertaling — *«Le renseignement économique: enquête sur un faux débat»* — Nicole Chaix, Philippe Dubost, Arnaud Voisin in *«Les cahiers de la sécurité intérieure»*, nr. 30, 1997 — IHESI.

(2) Naar *«une approche française de l'intelligence économique»* — Christian Harbulot — 1995.

estime que «parce que la concurrence ne s'assimile pas à la guerre, le renseignement économique n'est pas une forme de renseignement comme les autres. En effet, il utilise essentiellement des méthodes ouvertes et ses multiples acteurs sont autant publics que privés. Plus qu'un espionnage économique inadapté, le véritable enjeu est de créer un réseau d'intelligence économique, favorisant la diffusion de l'information au sein de l'économie nationale et dépassant certains travers culturels tels que la rétention d'informations» (1).

Certains auteurs estiment que l'intelligence économique, selon qu'elle est pratiquée par les entreprises ou les États, n'obéit pas toujours à la même logique dans les deux cas.

Et ceux-ci de développer le tableau suivant (2):

L'intelligence économique	des entreprises	des États
a pour objectif final	le développement de l'entreprise,	la puissance économique,
cible	les produits,	le marché mondial,
recherche d'abord	l'information centrée sur les métiers,	l'information centrée sur les réseaux,
pratique	le lobbying,	l'influence,
recherche l'information	dans le marché privé de l'information,	dans le processus de renseignement,
transmet l'information	au PDG, au conseil d'administration,	à l'autorité politique responsable de l'économie
est imprégnée	de la culture d'en treprise,	de la culture du renseignement.

Dans la réalité, la pratique de l'intelligence économique par les entreprises et celle des États ne sont probablement pas aussi clichées que le voudraient ces auteurs.

Le Comité R retiendra pour sa part que les objectifs de l'intelligence économique pratiquée par les entreprises ne coïncident pas toujours avec la préservation de la puissance économique de la nation.

(1) «*Le renseignement économique: enquête sur un faux débat*» — Nicole Chaix, Philippe Dubost, Arnaud Voisin dans «*Les cahiers de la sécurité intérieure*», nº 30, 1997 — IHESI

(2) D'après «*une approche française de l'intelligence économique*» — Christian Harbulot — 1995.

4. De moeilijke bescherming van de economische, wetenschappelijke en technologische geheimen van een landin een maatschappij gekenmerkt door internationale openheid, informatie en technologische vooruitgang

We moeten de bescherming van de wetenschappelijke en economische geheimen situeren in de context van de globalisering, de informatiemaatschappij en de technologische vooruitgang.

4.1. De openheid van het wetenschappelijk beleid van de Europese Unie en de federale regering

Reeds in het eerste rapport dat het Comité I aan deze materie heeft gewijd, wees het erop hoe moeilijk het is universiteiten en onderzoekscentra bewust te maken van de noodzaak hun activiteiten te beschermen: «Universiteiten en onderzoekscentra zijn steeds een bevoorrecht doelwit voor informatiewinning geweest. De geest van openheid en het chronisch gebrek aan wantrouwen die onderzoekers aan de dag leggen tegenover hun buitenlandse collega's en homologen, hebben altijd al dergelijke openbare onderzoekscentra tot een gemakkelijk doelwit gemaakt voor agenten van inlichtingendiensten »(1).

Op de top van de staatshoofden en regeringsleiders van de Europese Unie, in mei 2000 te Lissabon, heeft men zich tot strategisch doel gesteld de meest concurrerende en de meest dynamische kenniseconomie ter wereld uit te bouwen.

Met het oog daarop heeft de Europese Unie, op korte en op middellange termijn, voorzien in het vaststellen van Europese indicatoren inzake onderzoek en ontwikkeling, het creëren van een groot Europees hogesnelheidsnet voor elektronische communicatie, het invoeren van een communautair octrooi en het opheffen van elk obstakel voor de mobiliteit van de vorsers.

Contacten tussen onderzoekers, hun onderlinge samenwerking en hun mobiliteit worden beschouwd als noodzakelijke voorwaarden voor de totstandbrenging van een Europees onderzoeksplatform.

Om dit platform aantrekkelijk te maken voor onderzoekers uit de hele wereld, neemt men zich voor de uitbreiding van de «technologische groeipolen» (TGP(2)) en de «interuniversitaire groeipolen» (IGP(3)) aan te moedigen, alsook een programma van beurzen voor wetenschappers uit derde landen te creëren.

(1) Comité I, jaarverslag 1998, blz. 79 en volgende.

(2) Federale onderzoekscentra gewijd aan de traditionele of nieuwe bedrijfssectoren, om er de innovatie aan te moedigen.

(3) Federale programma's voor de financiering van universitair onderzoek.

4. La difficile protection des secrets économiques, scientifiques et technologiques nationaux dans une société d'ouverture internationale, d'information et de progrès technologiques

Il convient de situer la protection des secrets scientifiques et économiques dans le contexte de la mondialisation, de la société de l'information et des progrès technologiques.

4.1. L'ouverture de la politique scientifique de l'Union européenne et du gouvernement fédéral.

Le premier rapport que le Comité R a consacré à cette matière faisait déjà apparaître la difficulté de sensibiliser les universités et les centres de recherche à la protection de leurs travaux d'autre part: «Les universités et les centres scientifiques ont toujours été une cible privilégiée en matière de renseignement. L'esprit d'ouverture et le manque chronique de méfiance des chercheurs vis-à-vis de leurs collègues et homologues étrangers ont de tout temps fait de ces centres publics de recherche une cible facile pour les agents des services de renseignement» (1).

Le sommet des chefs d'États et de gouvernements de l'Union européenne qui s'est déroulé à Lisbonne en mai 2000 s'est fixé comme objectif stratégique de développer l'économie de la connaissance la plus compétitive et la plus dynamique du monde.

À cet égard, l'Union européenne a notamment prévu, à court et à moyen termes, la mise sur pied d'indicateurs européens pour la recherche et le développement, la création d'un grand réseau européen à haute vitesse pour les communications électroniques, la mise sur pied d'un brevet communautaire et la levée de toute entrave à la mobilité des chercheurs.

La mise en contact des chercheurs, leur collaboration mutuelle et leur mobilité sont considérées comme des conditions essentielles à la création d'un espace européen de recherche.

Pour le rendre attrayant aux chercheurs du monde entier, il est prévu d'encourager l'extension des «Pôles d'attractions technologiques» (PAT(2)), des «Pôles d'attractions inter universitaires» (PAI(3)), de même que de créer un système de bourses pour les scientifiques des pays tiers.

(1) Comité R, rapport d'activités 1998, pp. 70 et suivantes.

(2) Centres de recherches fédéraux dédiés aux secteurs industriels classiques ou nouveaux pour y stimuler l'innovation.

(3) Programmes fédéraux de financement de recherches universitaires.

Met het oog op het verwezenlijken van deze doelstelling, waartoe elke lidstaat zich heeft verbonden, is er een Europees convergentieplan nodig, alsook een coördinatie van de wetenschappelijke materies in ons land. « Immers, alleen een totale samenhang van de onderzoeksinspanningen vormt een garantie voor het vereiste massa-effect dat Europa zal toelaten een geloofwaardige plaats te blijven innemen in de confrontatie met de Verenigde Staten en Japan » (1).

Tot slot wijzen we er nog op dat de Europese akkoorden tot oprichting van samenwerkingsverbanden tussen de Europese Gemeenschappen, hun lidstaten en sommige landen van het vroegere Oostblok stuk voor stuk een luik omvatten betreffende de samenwerking op het gebied van wetenschap en technologie.

Deze akkoorden voorzien in het bijzonder in het uitwisselen van informatie, het organiseren van gezamenlijke wetenschappelijke bijeenkomsten, het uitwerken van gezamenlijke onderzoeks- en ontwikkelingsprogramma's ter bevordering van de wetenschappelijke vooruitgang en de overdracht van technologieën en knowhow.

De minister van Economie en van het Wetenschappelijk Onderzoek heeft zich voorgenomen het wetenschappelijk potentieel in de « technologische groeipolen » (TGP) en de « inter-universitaire groeipolen » (IGP) in België te laten evalueren. In de nieuwe fase van de IGP's wil hij de verplichting laten opnemen deel te nemen aan onderzoeksteams in het noorden en het zuiden van het land, maar ook op Europees en zelfs op een ruimer internationaal niveau's.

In dit kader heeft België er het grootste belang bij, net als alle landen die op dit vlak al grote vorderingen hebben geboekt, meer buitenlandse onderzoekers naar ons land te halen teneinde het eigen potentieel te versterken.

De minister wil dan ook bepaalde fiscale maatregelen voorstellen ten gunste van buitenlandse onderzoekers die in het kader van hun postdoctorale opleiding naar België komen.

In deze context van globalisering en wetenschappelijke openheid bestaat de moeilijkheid erin de te beschermen geheimen duidelijk af te bakenen, teneinde het voortbestaan van het wetenschappelijk of economisch potentieel van het land te verzekeren, overeenkomstig de wet houdende regeling van de inlichtingen- en veiligheidsdiensten.

(1) Beleidsnota van de minister van Economie en van het Wetenschappelijk Onderzoek betreffende de evolutie van het federaal wetenschappelijk beleid.

La rencontre de cet objectif, auquel chaque État membre a souscrit, nécessite un plan de convergence européen ainsi qu'une coordination des matières scientifiques dans notre pays. « Seule, en effet, une cohérence globale des efforts de recherche assurera l'indispensable effet de masse permettant à l'Europe de garder une place crédible dans la confrontation qui l'associe aux États-Unis et au Japon » (1).

Notons enfin que les accords européens établissant des associations entre les Communautés européennes, leurs États membres et certains États de l'ancien bloc de l'Est comportent tous un volet relatif à la coopération dans les domaines de la science et de la technologie.

Ces accords prévoient notamment des échanges d'informations, l'organisation de réunions scientifiques communes, des programmes communs de recherches et développement qui visent à favoriser le progrès scientifique et le transfert de technologies et de savoir-faire.

Le ministre de l'Économie et de la Recherche scientifique compte procéder à une évaluation du potentiel scientifique présent dans les « pôles d'attraction technologiques » (PAT) et « Pôles d'attractions inter universitaires » (PAI) en Belgique. Il veut également faire inscrire dans la nouvelle phase des « PAI » l'obligation de participer à des équipes de recherche du nord et du sud du pays, mais aussi européennes, voire plus largement internationales.

À cet égard, la Belgique a, comme tous les pays avancés en la matière, grand intérêt à renforcer l'accueil de chercheurs étrangers afin d'accroître son propre potentiel.

Le ministre souhaite donc proposer des mesures fiscales en faveur des chercheurs étrangers engagés en Belgique dans un post-doctorat.

Dans un tel contexte de mondialisation et d'ouverture d'esprit scientifique, la difficulté apparaît clairement de cibler les secrets à protéger pour assurer la pérennité du potentiel scientifique et économique du pays ainsi que le veut la loi organique des services de renseignement et de sécurité.

(1) Note d'orientation du ministre de l'Économie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale.

4.2. De bescherming van de technologische en economische geheimen van een maatschappij in beweging

Voor de analyse in dit deel van ons verslag hebben we ons geïnspireerd op het werk van de eminente Franse jurist Bertrand Warusfel, Lector aan de faculteit Rechten van Parijs V, en auteur van een thesis over de bescherming van het geheim (1).

Volgens Bertrand Warusfel is de ingrijpende gedaanteverwisseling die onze samenleving momenteel ondergaat — en die in hoofdzaak het gevolg is van de technische vooruitgang — «de oorzaak van een grondige wijziging van de waarde van de voornaamste parameters in de vergelijking van het geheim».

Drie kenmerken beschrijven deze moderniteit:

— de diversificatie van de machtsactoren: naast de traditionele factoren van de politieke, diplomatieke en militaire macht, zijn we getuige van een verschuiving van de machtsinzet en de strategische strijd naar de economie, de technologie en de cultuur. Dit heeft tot gevolg dat rekening moet worden gehouden met economische, wetenschappelijke en technologische geheimen in de wettelijke mechanismen van bescherming van het geheim;

— de diversificatie van de machtsfactoren: benevens de Staten spelen ook economische actoren, ongeacht of ze nationaal of supranationaal zijn, een steeds belangrijker strategische rol;

— de wijziging van de plaatsen en de dragers van de macht: de nieuwe situatie stelt de spreiding van de macht en de immaterialiteit van de middelen van de informatie tegenover de oude orde, die was gebaseerd op territorialiteit, de materialiteit van de macht en de fysieke toe-eigening van de middelen.

Vandaag zijn de middelen en dragers van het geheim vooral elektronische informatiesystemen die kwetsbaar zijn voor manipulatie en voor technieken waarmee communicatie wordt geïntercepteerd (2).

Het Comité I is van mening dat ook de globalisering van de economie een nieuw kenmerk van onze samenleving is. Immers, de industriële herstructureringen en de globalisering van de procédés in de hele wereld hebben tot gevolg dat het moeilijk wordt de nationaliteit van een onderneming te gaan bepalen. Hoe kan men onder deze voorwaarden uitmaken wat

(1) Bertrand Warusfel: *Contre-espionnage et protection du secret — Histoire, droit et organisation de la sécurité nationale en France*, juni 2000 — uitgeverij Lavauzelle.

(2) In verband hiermee *«Development of surveillance technology and risk of abuse of economic information», door Duncan Campbell — working document for the Scientific and Technological Options Assessment (STOA) panel — European Parliament* — http://www.gn.apc.org/duncan/stoa.htm.

4.2. La protection des secrets technologiques et économiques dans une société en mutation

L'analyse contenue dans la présente section s'inspire des travaux de l'éminent juriste français Bertrand Warusfel, maître de conférences à la faculté de droit de Paris V, auteur d'une thèse sur la protection du secret (1).

Selon Bertrand Warusfel, la transformation profonde — due pour l'essentiel aux progrès techniques — que connaît notre société «modifie fondamentalement la valeur des principaux paramètres de l'équation du secret».

Trois caractéristiques décrivent cette modernité:

— la diversification des facteurs de puissance: à côté des facteurs traditionnels de la puissance politique, diplomatique et militaire, les enjeux de puissance et les luttes stratégiques se déplacent vers l'économie, la technologie et la culture, ce qui conduit à la prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret;

— la diversification des acteurs de la puissance: à côté des États, les acteurs économiques, qu'ils soient nationaux ou supranationaux, jouent un rôle stratégique de plus en plus important;

— la transformation des lieux et des supports de la puissance: la nouvelle donne oppose la délocalisation de la puissance et l'immatérialité des ressources de l'information à l'ancien ordre basé sur la territorialité, la matérialité du pouvoir et l'appropriation physique des ressources.

Les moyens et supports du secret sont aujourd'hui essentiellement des systèmes électroniques d'informations vulnérables aux manipulations et aux techniques d'interceptions des communications (2).

Le Comité R considère par ailleurs que la mondialisation de l'économie constitue aussi une caractéristique nouvelle de notre société. En effet, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent plus difficile l'attribution d'une nationalité aux entreprises. Comment déterminer dans ces conditions ce qui constitue le caractère

(1) Bertrand Warusfel: *Contre-espionnage et protection du secret — Histoire, droit et organisation de la sécurité nationale en France*, juin 2000 — éditions Lavauzelle.

(2) Lire à ce sujet *«Development of surveillance technology and risk of abuse of economic information», by Duncan Campbell - working document for the Scientific and Technological Options Assesment (STOA) panel — European Parliament* — http://www.gn.apc.org/duncan/stoa.htm.

aan het te beschermen economisch of wetenschappelijk potentieel een nationale identiteit verleent?

Vertegenwoordigers van het Belgisch Verbond van Ondernemingen (VBO) hebben aan het Comité I verklaard dat zij elke onderneming die op het nationaal grondgebied is gevestigd en daar een toegevoegde waarde produceert als een Belgische onderneming beschouwen, ongeacht de nationaliteit van de aandeelhouders of de bedrijfsleiders.

4.3. Rekening houden met economische, wetenschappelijke en technologische geheimen in de wettelijke mechanismen tot bescherming van het geheim

Tot voor kort werden deze geheimen slechts op marginale wijze beschermd. In België behoren ze niet tot de geheimen die betrekking hebben op de verdediging van het grondgebied of de veiligheid van de Staat, waarvan de bescherming wordt georganiseerd door een aantal bepalingen in hoofdstuk II van titel I van boek II van het Strafwetboek (getiteld «misdaden en wanbedrijven tegen de externe veiligheid van de Staat»), alsook door bepaalde bijzondere wetten.

Overeenkomstig de bepalingen van de wet van 10 januari 1955 «betreffende de bekendmaking en de toepassing der uitvindingen en fabrieksgeheimen welke de verdediging van het grondgebied of de veiligheid van de Staat aangaan» echter wordt de bekendmaking, opzettelijk of door nalatigheid, van deze uitvindingen en fabrieksgeheimen bestraft met strafsancties.

Men moet echter bewijzen dat de dader van de bekendmaking er niet onwetend van kon zijn dat deze bekendmaking strijdig was met de belangen van de verdediging van het grondgebied of de veiligheid van de Staat.

In verband hiermee kunnen de minister tot wiens bevoegdheid de nijverheidseigendom behoort (de minister van Economische Zaken) en de minister van Landsverdediging gezamenlijk verklaren dat de bekendmaking van een uitvinding of een fabrieksgeheim in strijd is met de belangen van de verdediging van het grondgebied of de veiligheid van de Staat, en dat ze verboden is gedurende een door hen te bepalen termijn.

De twee voornoemde ministers, die gezamenlijk handelen, kunnen ook tijdelijk controleren en bepalen onder welke voorwaarden uitvindingen geëxploiteerd en bepaalde octrooien toegepast kunnen worden, waarvan ze menen dat ze hen geheim moeten houden; ze kunnen de exploitatie van uitvindingen of het toepassen van fabrieksgeheimen zelfs tijdelijk verbieden, ofwel het recht om ze volledig of gedeeltelijk te exploiteren tijdelijk exclusief voor de Staat voorbehouden.

national du potentiel économique et scientifique à protéger?

Des représentants de la Fédération des entreprises de Belgique (FEB) ont fait part au Comité R qu'ils considéraient comme belge toute entreprise implantée sur le territoire national et qui y crée une valeur ajoutée, quelle que soit la nationalité de ses actionnaires ou de ses dirigeants.

4.3. La prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret

Jusqu'il y a peu en effet, ces secrets n'étaient protégés que de manière périphérique. En Belgique, ils ne figurent pas parmi les secrets qui intéressent la défense du territoire ou la sûreté de l'État et dont la protection est organisée par un certain nombre de dispositions figurant au chapitre II du titre I^{er} du livre II du Code pénal (intitulé «crimes et délits contre la sûreté extérieure de l'État») et par des lois particulières.

Cependant, aux termes de la loi du 10 janvier 1955 relative à la divulgation et à la mise en œuvre des inventions et des secrets de fabrique intéressant la défense du territoire ou la sûreté de l'État, la divulgation volontaire ou par négligence de ces inventions et secrets de fabrique est passible de sanctions pénales.

Il faut cependant prouver que l'auteur de la divulgation ne pouvait ignorer qu'elle était contraire aux intérêts de la défense du territoire ou de la sûreté de l'État.

À cet égard, le ministre qui a la propriété industrielle dans ses attributions (le ministre des Affaires économiques) et le ministre de la Défense nationale peuvent déclarer conjointement que la divulgation d'une invention ou d'un secret de fabrique est contraire aux intérêts de la défense du territoire ou de la sûreté de l'État et qu'elle est interdite pendant la période qu'ils déterminent.

Les deux ministres précités, agissant conjointement, peuvent également déterminer et contrôler temporairement les conditions d'exploitation, d'invention et de mise en œuvre de certains brevets qu'ils estiment devoir maintenir secrets; ils peuvent même en interdire temporairement leur exploitation ou leur mise en œuvre, ou bien encore réserver à l'État, et à lui seul, le droit de les exploiter en tout ou en partie.

Deze maatregelen kunnen te allen tijde volledig of gedeeltelijk worden opgeheven door de ministers van wie ze uitgaan. De houder van het recht dat aan verbod of beperking onderworpen is, kan deze opheffing aanvragen. Inbreuken op deze maatregelen worden bestraft met strafsancties.

De wet van 1955 stelt een procedure vast volgens dewelke de minister van Economische Zaken een octrooiaanvraag overlegt aan de minister van Landsverdediging, met het oog op het in werking laten treden van de hierboven beschreven maatregelen.

Deze wet bepaalt ook dat «wanneer een vreemde Staat, in het belang zijner verdediging, de bekendmaking van een uitvinding waarvoor octrooi wordt aangevraagd, verbiedt, zal de minister tot wiens bevoegdheid de nijverheidseigendom behoort, op verzoek van de Staat of van de aanvrager die het bewijs van het verbod levert, er zich van onthouden de uitvinding aan het publiek bekend te maken en afschriften van de beschrijving ervan af te geven, zulks voor de duur van het verbod.»

Een dergelijk verzoek kan echter alleen in aanmerking worden genomen indien er een verdrag bestaat tussen België en de vreemde staat die het verbod heeft uitgevaardigd.

De parlementaire vraag nr. 870 betreffende de toepassing van deze wet uit 1955, die op 16 februari 1998 door senator Eddy Boutmans (Agalev) werd gesteld, was nog steeds niet beantwoord op de datum waarop het onderhavige rapport werd goedgekeurd (1).

Tot de goedkeuring van de wet van 11 december 1998 «betreffende de classificatie en de veiligheidsmachtigingen» was de wet van 1955 de enige in het Belgisch recht die aan een politieke overheid de verantwoordelijkheid toekende om te verordenen dat bepaalde economische informatie geheim kon zijn.

Tussen 1949 en 1994 heeft België deelgenomen aan het overleg in het kader van het COCOM (COordinating COMmittee) van de westerse landen die zich op initiatief van de Verenigde Staten hadden verenigd om een embargo na te leven op de uitvoer van een aantal producten en technologieën van militaire, nucleaire en, vooral, burgerlijke aard voor tweeërlei gebruik (civiel en militair) naar de USSR, China en andere communistische landen.

In verband hiermee heeft België gedurende ongeveer veertig jaar een door het COCOM opgestelde gemeenschappelijke lijst gepubliceerd en bijgehouden van producten en technologieën die aan controle onderworpen waren, in de vorm van een «bericht aan de

(1) Senaat — *Bulletin van Vragen en Antwoorden*, 24 maart 1998 (nr. 1-69) vraag nr. 870/1.

Ces mesures peuvent être levées à tout moment, partiellement ou totalement, par décision des ministres dont elles émanent. Le titulaire du droit sujet à interdiction ou limitation peut solliciter cette mainlevée. Des sanctions pénales sont aussi prévues pour les infractions à ces mesures.

La loi de 1955 fixe une procédure par laquelle le ministre des Affaires économiques soumet une demande de brevet au ministre de la Défense nationale en vue de la mise en œuvre des mesures précitées.

Cette loi prévoit encore que lorsque, dans «l'intérêt de sa défense, un État étranger interdit la divulgation d'une invention, objet d'une demande de brevet, le ministre ayant la propriété industrielle dans ses attributions s'abstiendra, sur requête de cet État ou du déposant qui établira la preuve de l'interdiction, de la communiquer au public et de délivrer des copies de sa description, aussi longtemps que durera cette interdiction».

Une telle requête ne peut toutefois être prise en considération que s'il existe une convention entre la Belgique et l'État étranger auteur de l'interdiction.

La question parlementaire n° 870 relative à l'application de cette loi de 1955 posée le 16 février 1998 par le sénateur Eddy Boutmans (Agalev) est restée sans réponse à la date d'approbation du présent rapport (1).

Jusqu'au vote de la loi du 11 décembre 1998 «relative à la classification et aux habilitations de sécurité», la loi de 1955 était la seule en droit belge qui attribuait à une autorité politique la responsabilité de décréter le secret d'informations à caractère économique.

Entre 1949 et 1994, la Belgique a participé à la concertation COCOM (Coordinating Committee) des pays occidentaux regroupés à l'initiative des États-Unis en vue d'exercer un embargo sur les exportations d'une série de produits et de technologies militaires, nucléaires mais aussi, et surtout, civiles à double usage (civil et militaire) à destination de l'URSS, de la Chine et des autres pays communistes.

À ce titre, la Belgique a publié et tenu à jour pendant environ quarante ans une liste commune établie par le COCOM de produits et technologies soumis à contrôle, sous la forme d'un «avis aux importateurs et exportateurs relatif aux produits et

(1) Sénat — *Bulletin des Questions et Réponses*, 24 mars 1998 (n° 1-69), question n° 870/1.

invoerders en uitvoerders met betrekking tot producten en technologieën waarvan de eindbestemming aan controle onderhevig is».

België neemt ook deel aan diverse internationale initiatieven die tot doel hebben de proliferatie van bepaalde massavernietigingstechnologieën en -wapens te beperken. Het geheel van deze producten en technologieën onder toezicht is samengebracht op één controlelijst van producten en technologieën voor tweeërlei gebruik, opgesteld door de lidstaten van de Europese Unie (1).

Deze Europese reglementering staat borg voor een geharmoniseerd toezicht op de uitvoer naar landen buiten de Europese Gemeenschap, waarbij het vrij verkeer van bijna alle producten en technologieën voor tweeërlei gebruik binnen de Unie mogelijk blijft.

Benevens deze Europese verordening is er ook het Akkoord van Wassenaar van 19 december 1995, dat in werking is getreden in juli 1996. Het werd ondertekend door drieëndertig Staten, waaronder de lidstaten van het voormalige COCOM en sommige andere geïndustrialiseerde landen of ex-leden van het Oostblok, zoals Rusland, Hongarije, Polen, Slovakije en de Tsjechische Republiek.

Elk van deze landen heeft zich ertoe verbonden de uitvoer te verbieden van burgerlijke goederen of technologieën voor tweeërlei gebruik, zoals oorlogsmaterieel, naar landen «waarvan het onverantwoord gedrag een bedreiging vormt voor de internationale vrede en veiligheid» (rogue states).

We wijzen er echter op dat de bescherming van het wetenschappelijk of economisch potentieel op zich niet het voornaamste doel is van deze internationale verdragen. Ze zijn veeleer gesloten met het oog op het behoud van de wereldstabiliteit en de non-proliferatie van massavernietigingswapens, niet van alleen maar de nationale veiligheid. Dat verklaart waarom sommige producten die op deze lijsten voorkomen niet de minste hoogtechnologische waarde bezitten.

De bescherming van de economische belangen wordt voorzien in de wet van 11 april 1994 betreffende de openbaarheid van bestuur. De artikelen 4 en 5 van deze wet creëren en organiseren het recht van particulieren kennis te nemen van een bestuurlijk document of van een document van persoonlijke aard van een federale bestuurlijke overheid, het ter plaatse te raadplegen, uitleg daarover te krijgen en er een afschrift van te ontvangen.

Het verzoek tot inzage moet echter worden afgewezen wanneer het belang van de openbaarheid niet opweegt tegen de bescherming van bepaalde collectieve belangen, waaronder «een federaal economisch

(1) EEG-verordening nr. 3381/94 van de Raad van 19 december 1994 tot instelling van een communautaire regeling voor controle op de uitvoer van goederen voor tweeërlei gebruik.

technologies soumis au contrôle de la destination finale».

Par ailleurs, la Belgique participe à différentes initiatives internationales destinées à limiter la prolifération de certaines technologies et armes de destruction massive. L'ensemble de ces produits et technologies contrôlés est regroupé au sein d'une liste unique de contrôle des produits et technologies à double usage mise au point par les États membres de l'Union européenne (1).

Cette réglementation européenne assure un contrôle harmonisé sur les exportations extracommunautaires tout en permettant la libre circulation au sein de l'Union de la quasi-totalité des produits et technologies à double usage.

À cette réglementation européenne, il faut ajouter l'Arrangement de Wassenaar du 19 décembre 1995, entré en vigueur en juillet 1996, qui regroupe trente-trois États, parmi lesquels les pays de l'ancien COCOM et certains autres pays industrialisés ou anciens membres du bloc de l'Est, comme la Russie, la Hongrie, la Pologne, la Slovaquie et la République tchèque.

Chacun de ces pays s'est engagé à ne pas autoriser l'exportation de biens ou technologies civiles à double usage ainsi que des matériels de guerre vers des pays dont «le comportement irresponsable menace la paix et la sécurité internationale» (rogue states).

Il faut cependant souligner que le premier but de ces conventions internationales n'est pas la protection du potentiel scientifique et économique en soi. Elles ont été conçues plus en vue du maintien de la stabilité mondiale et de la non prolifération des armes de destruction massive que de la simple sécurité nationale. C'est la raison pour laquelle certains produits figurant sur ces listes n'ont aucune valeur de haute technologie.

La protection des intérêts économiques est prise en compte dans la loi du 11 avril 1994 relative à la publicité de l'administration. Les articles 4 et 5 de cette loi instituent et organisent le droit des particuliers de prendre connaissance d'un document administratif ou d'un document à caractère personnel d'une autorité administrative fédérale, de le consulter sur place, d'obtenir des explications à son sujet et d'en recevoir une copie.

La demande de consultation doit cependant être rejetée lorsque l'intérêt de la publicité ne l'emporte pas sur la protection de certains intérêts collectifs parmi lesquels figurent «un intérêt économique ou

(1) Règlement CE nº 3381/94 du Conseil, du 19 décembre 1994 instituant un régime communautaire de contrôle des exportations de biens à double usage.

of financieel belang, de munt, het openbaar krediet», alsook «het uit de aard van de zaak vertrouwelijke karakter van de ondernemings- en fabricagegegevens die aan de overheid zijn meegedeeld».

Tot slot kunnen geheimen die het wetenschappelijk en economisch belang van het land aanbelangen voortaan het voorwerp zijn van een classificatie overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen.

De houder van een veiligheidsmachtiging die geclassificeerde documenten, informatie of materieel in de uitoefening van zijn functie op een niet-geëigende wijze aanwendt of laat aanwenden, wordt gestraft met strafsancties. Deze inbreuk wordt bestraft, ongeacht of ze opzettelijk of door ernstige nalatigheid is begaan(1).

4.4. De bescherming van het geheim bij bedrijven en onderzoekscentra heeft het verschijnen van nieuwe actoren tot gevolg

Niet alleen de inhoud van het geheim evolueert, maar ook de producenten ervan, zijn bezitters, zijn beschermers en ... zijn «belagers».

Terwijl het klassieke beschermingsstelsel aanvankelijk werd bedacht in functie van een militair geheim of een geheim geproduceerd door de overheid, door deze laatste beheerd en op gerichte wijze toevertrouwd aan externe personen «die er kennis van moesten hebben» om zelf deel te nemen aan de actie van deze overheid, zorgt de nieuwe economische en strategische realiteit voor een ware omwenteling van de context.

Die context wordt voortaan gekenmerkt door de diversificatie en de steeds grotere heterogeniteit van de actoren, waaronder vernieuwende bedrijven met een sterke toegevoegde waarde, laboratoria, alsmede hun personeelsleden die, met hun eigen logica van winstbejag, vandaag een belangrijke plaats bekleden, niet alleen in de handelseconomie, maar ook in het wetenschappelijk en technologisch onderzoek, de collectieve diensten, de culturele sector en de internationale betrekkingen.

Met deze nieuwe situatie wordt ten dele rekening gehouden in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen. De bevoegde overheid kan immers bepalen dat rechts- of natuurlijke personen een veiligheidsmachtiging moeten bezitten met het oog op het aangaan of uitvoeren van bepaalde overeenkomsten of overheidsopdrachten met betrekking tot Landsverdediging, kernenergie en veiligheid (artikel 12, lid 1).

(1) Artikel 11 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen.

financier fédéral, la monnaie, le crédit public» ainsi que «le caractère par nature confidentiel des informations d'entreprises ou de fabrication communiquées à l'autorité».

Enfin, les secrets intéressant le potentiel scientifique et économique du pays peuvent désormais faire l'objet d'une classification au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le titulaire d'une habilitation de sécurité qui, dans l'exercice de ses fonctions, utilise ou laisse utiliser «de manière inappropriée» des documents, informations ou matériels classifiés est passible de sanctions pénales. Cette infraction est sanctionnée qu'elle ait été commise de manière délibérée, ou par négligence grave(1).

4.4. La protection du secret au sein des entreprises et des centres de recherches a pour conséquence une mutation des acteurs du secret

Si donc le contenu du secret évolue, il en va de même aussi bien pour ses producteurs, que pour ses détenteurs, ses protecteurs et ... ses «prédateurs».

Alors que le système classique de protection a d'abord été conçu en fonction d'un secret militaire ou d'un secret produit par l'autorité publique, géré par elle et ponctuellement confié à des personnes extérieures «qui ont besoin d'en connaître» pour participer eux-mêmes à l'action de cette autorité, la nouvelle réalité économique et stratégique bouleverse le contexte.

Celui-ci se caractérise par la diversification et l'hétérogénéité croissante des acteurs, parmi lesquels les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires, ainsi que leurs personnels qui, avec une logique autonome de profit, occupent à présent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

Cette nouvelle situation a été partiellement prise en compte par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité puisque l'autorité compétente peut imposer la possession d'une habilitation de sécurité à des personnes morales ou physiques pour la passation et l'exécution de certains contrats ou marchés publics en rapport avec la Défense nationale, l'énergie nucléaire et la sécurité (article 12, alinéa 1er).

(1) Article 11 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Lid 2 van hetzelfde artikel bepaalt:

«In de door de Koning bepaalde gevallen is deze wet eveneens van toepassing op de veiligheidsmachtigingen die worden gevraagd door rechtspersonen of natuurlijke personen die een veiligheidsmachtiging willen verkrijgen om in het buitenland toegang te krijgen tot geclassificeerde informatie, documenten of gegevens, materieel, materialen of stoffen, tot lokalen, gebouwen of terreinen, waartoe alleen de houder van een veiligheidsmachtiging toegang krijgt.»

Daartoe moeten ondernemingen die houder zijn van een veiligheidsmachtiging een personeelslid, dat eveneens houder is van een veiligheidsmachtiging, benoemen tot de functie van «veiligheidsofficier». De betrokkene moet dan toezien op het naleven van de veiligheidsvoorschriften binnen de onderneming.

4.5. De moeilijkheid om zich een idee te vormen over de omvang van het fenomeen van economische spionage

Vaak aarzelen de verantwoordelijken van bedrijven die het slachtoffer zijn van economische spionage om voor dergelijke feiten klacht neer te leggen. Ze zijn beducht voor de negatieve publiciteit die dit zou kunnen meebrengen voor hun onderneming en voor het mogelijk verlies aan vertrouwen bij hun klanten, leveranciers, aandeelhouders enz.

In een enquête die het National Counterintelligence Center in 1995 in de Verenigde Staten uitvoerde, verklaarde 42% van de ondervraagde bedrijfsleiders dat ze nooit feiten van spionage aan de overheid hadden gemeld, ook al wisten ze dat ze daarvan het slachtoffer waren. Bovendien, ook al erkennen de verantwoordelijken van grote industriële groepen dat ze te maken hebben met economische spionage, valt het hen moeilijk te achterhalen op welke manier informatie over hen wordt verkregen. In het bijzonder kunnen ze moeilijk bewijzen dat ze contracten zijn misgelopen tengevolge van het afluisteren of intercepteren van hun communicatie.

Volgens advocaat Fernand de Visscher, specialist in het recht inzake nijverheidseigendom, vindt men in de Belgische rechtspraak weinig gevallen van bedrijfs- of commerciële spionage, aangezien het bijzonder moeilijk blijkt dergelijke inbreuken te bewijzen (1).

4.6. De Amerikaanse benadering van economische en commerciële geheimen

Het Amerikaanse Congres houdt zich intens bezig met economische spionage en de middelen om zich ertegen te beschermen. In 1996 keurde het Congres de

(1) *La Libre Belgique*, van 16 januari 2001, blz. 15: «Que les espions lèvent le doigt ...».

L'alinéa 2 du même article dispose:

«Dans les cas déterminés par le Roi, la présente loi s'applique également aux habilitations de sécurité demandées par des personnes morales ou physiques qui souhaitent obtenir une habilitation de sécurité en vue d'accéder à l'étranger à des informations, documents ou données, à des matériels, matériaux ou matières classifiées, à des locaux, des bâtiments ou des sites, dont l'accès est réservé au titulaire d'une habilitation de sécurité».

À cet effet, les entreprises titulaires d'une habilitation de sécurité doivent désigner un membre de leur personnel, lui même titulaire d'une habilitation de sécurité, pour remplir la fonction d'«officier de sécurité». Cette fonction consiste à veiller à l'observation des règles de sécurité dans l'entreprise.

4.5. La difficulté de connaître l'ampleur du phénomène de l'espionnage économique

Les responsables d'entreprises victimes d'actes d'espionnage économique hésitent souvent à porter plainte pour de tels faits. Ils craignent en effet la publicité négative qu'une telle affaire pourrait entraîner pour leurs firmes ainsi que la perte de confiance des clients, des fournisseurs, des actionnaires, etc ...

Dans une enquête effectuée aux États-Unis en 1995 par le National Counterintelligence Center, 42% des dirigeants d'entreprises interrogés ont déclaré qu'ils n'avaient jamais signalé de faits d'espionnage aux autorités alors même qu'ils se savaient victimes de tels actes. En outre, même si les responsables de grands groupes industriels reconnaissent qu'ils sont concernés par l'espionnage économique, il ne leur est pas facile de savoir de quelle manière des informations ont été obtenues à leur sujet. Il leur est particulièrement impossible d'affirmer que des marchés ont été perdus en raison d'écoutes et d'interception de leurs communications.

Selon l'avocat Fernand de Visscher, spécialiste du droit de la propriété industrielle, on trouve peu de cas d'espionnage industriel ou commercial dans la jurisprudence belge, la preuve de telles infractions étant difficile à apporter (1).

4.6. L'approcheaméricainedessecretséconomiques et commerciaux.

L'espionnage économique et la manière de s'en prémunir sont des matières qui préoccupent le Congrès américain de manière intense. En 1996, celui-

(1) *La Libre Belgique*, du 16 janvier 2001, p. 15: « Que les espions lèvent le doigt ... ».

Economic Espionage Act (EEA) goed. Deze wet streeft ernaar de ongepaste toe-eigening van trade secrets (handelsgeheimen) te bestraffen, ongeacht of de daders inlichtingendiensten, buitenlandse regeringen of nationale concurrenten zijn.

In de Verenigde Staten verschilt de manier waarop men trade secrets beschermt grondig van de wijze waarop de geheimen inzake nationale veiligheid worden beschermd.

Deze laatste worden beschermd met behulp van een streng classificatiestelsel dat het bezit zelf van geclassificeerde informatie door een persoon zonder machtiging daartoe bestraft, ongeacht de manier waarop de betrokkene in het bezit is geraakt van die informatie.

Het bijzondere aan de *Economic Espionage Act* bestaat erin dat deze wet niet de eigenlijke kennisneming van een commercieel geheim ten laste legt; alleen de deloyale, bedrieglijke of oneerlijke wijze die wordt aangewend om kennis te nemen (of daartoe een poging te ondernemen) van een dergelijk geheim kan worden ten laste gelegd.

Om bepaalde informatie als geheim te kunnen beschouwen, mag ze niet behoren tot het publiek domein, moet ze voor de bezitter ervan de bron zijn van economische waarde, en moet de bezitter redelijke maatregelen hebben getroffen om de informatie geheim te houden.

Dit belet niet dat iemand een poging kan ondernemen om het geheim van een concurrent te doorgronden of te begrijpen, op voorwaarde dat de aangewende middelen eerlijk zijn (bij voorbeeld : het analyseren van open bronnen). Dit stelsel van bescherming van handelsgeheimen berust dus op het verantwoordelijk maken van de economische actoren zelf (1).

5. Enkele manieren om economische, wetenschappelijke of industriële inlichtingen te verzamelen

Informatie van economische, wetenschappelijke, technologische of industriële aard wordt vandaag intens opgespoord en zelfs gestolen. In de literatuur over economische inlichtingen of over de inlichtingendiensten vinden we diverse manieren waarop dit soort informatie wordt verkregen, van de meest traditionele tot de meest gesofisticeerde.

De meeste van de beschreven methodes bestaan in het systematisch zoeken naar open bronnen, al komen sommige in de buurt van de echte spionage. De meest klassieke en brutale methodes zijn het stelen van documenten, het doorzoeken van vuilnisbakken,

(1) *«OSINT — An American legal and practical perspective»* by Richard Horowitz, Attorney at Law, EUFIS — Brussels, 19 October 2000.

ci a adopté l'*Economic Espionage Act (EEA)* qui tend à réprimer l'appropriation indue des trade secrets (les secrets commerciaux) aussi bien par des services de renseignement ou gouvernements étrangers que par des concurrents nationaux.

Aux États-Unis, la manière de protéger les trade secrets diffère fondamentalement de la manière de protéger les secrets de la sécurité nationale.

Ces derniers sont protégés par un rigoureux système de classification qui incrimine la possession même d'une information classifiée par une personne non habilitée, et ce, quelle que soit la manière dont elle a été acquise.

La particularité de l'*Economic Espionage Act* est de ne pas incriminer la prise de connaissance d'un secret commercial en soi; c'est seulement la manière déloyale, trompeuse ou malhonnête utilisée pour prendre connaissance (ou tenter de prendre connaissance) d'un tel secret qui peut l'être.

Pour qu'une information soit considérée comme telle, elle ne doit pas être répandue dans le domaine public, elle doit être la source d'une valeur économique pour son détenteur et celui-ci doit avoir pris des mesures raisonnables pour la garder secrète.

Ceci n'empêche donc personne de tenter de percer ou de comprendre le secret d'un concurrent pourvu que les moyens employés soient honnêtes (par exemple : par l'analyse de sources ouvertes). Ce système de protection des secrets commerciaux repose donc sur la responsabilisation des acteurs économiques eux-mêmes (1).

5. Quelques manières de collecter le renseignement économique, scientifique ou industriel

L'information d'ordre économique, scientifique, technologique ou industrielle est devenue objet de recherche et même de prédation. La littérature relative à l'intelligence économique ou aux services de renseignement livre de nombreuses manières de recueillir ce type d'information, des plus classiques aux plus sophistiquées.

La plupart des méthodes décrites consistent dans une recherche systématique des sources ouvertes, mais certaines s'apparentent néanmoins à de l'espionnage pur et simple. Les méthodes les plus classiques et brutales sont le vols de documents, la fouille

(1) *«OSINT — An American legal and practical perspective»* by Richard Horowitz, Attorney at Law, EUFIS — Brussels, 19 October 2000.

het beïnvloeden van personen, corruptie, chantage, bedreigingen enz. Nog andere manipulatietechnieken worden aangewend, om nog te zwijgen van de nieuwe technologieën. We geven hierna een kort overzicht:

5.1. Observeren van wetenschappers op reis in het buitenland

In een rapport dat het *General Accounting Office (GAO)* op 25 juni 2000 indiende bij het Amerikaanse Congres, werden 75 recente pogingen tot spionage in het buitenland geteld, gericht tegen Amerikaanse kerngeleerden.

Dit rapport, gebaseerd op het verslag van honderden reizen van wetenschappers in de hele wereld, beschrijft gevallen waarin wetenschappers werden afgeluisterd in hotels, waarin hun persoonlijke spullen werden doorzocht of waarbij hun diensten van prostituees werden aangeboden.

Het GAO beveelt aan dat de reizen van bepaalde wetenschappers naar het buitenland voorafgaandelijk zouden worden goedgekeurd door de contraspionagediensten.

5.2. Universitaire vorsers op stage in het buitenland

Ook universitaire laboratoria kunnen het doelwit zijn van inlichtingendiensten. De techniek bestaat erin beursstudenten of vorsers op stage uit te zenden, met de opdracht belangrijke wetenschappelijke informatie te verzamelen.

Bij zijn terugkeer wordt de student of de onderzoeker in zijn thuisland grondig «gedébrieft» inzake de technische en wetenschappelijke kennis die hij in het buitenland heeft opgedaan.

De academische wereld staat gewoonlijk vrij open voor de verspreiding van kennis en internationale samenwerking. Onderzoekers hebben het dan ook niet moeilijk om informatie in te winnen, soms moeten ze er niet eens naar vragen.

Daarom moeten inlichtingendiensten waakzaam zijn voor de aanwezigheid van buitenlandse stagiairs in laboratoria waar geavanceerd onderzoek plaatsvindt.

5.3. Participeren in een vennootschap

Sommige ondernemingen die zich actief bezighouden met technologische bewaking beschikken over investeringsfondsen waarmee ze participeren in hoogtechnologische bedrijven.

Een «neutrale» persoon, die handelt voor rekening van een onderneming (of een Staat) die in de schaduw

des poubelles, la subornation de personnes, la corruption, le chantage, les menaces, etc. Des techniques de manipulation peuvent également être mises en oeuvre, sans parler des technologies nouvelles. En voici quelques aperçus:

5.1. La surveillance des scientifiques en voyage à l'étranger

Un rapport présenté le 25 juin 2000 par le *General accounting Office (GAO)* au Congrès des États-Unis a recensé 75 tentatives récentes d'espionnage à l'étranger sur des savants nucléaires américains.

Ce rapport, basé sur le compte-rendu de centaines de voyages effectués par des scientifiques de par le monde expose des cas de mises sous écoute dans des hôtels, de fouilles d'effets personnels, ou bien encore d'offres de services de prostituées.

Le GAO recommande que les voyages de certains scientifiques à l'étranger soient soumis à l'autorisation préalable des services de contre-espionnage.

5.2. Les chercheurs universitaires en stage à l'étranger

Les laboratoires universitaires peuvent aussi être la cible de services de renseignement. La technique consiste à y envoyer des étudiants boursiers ou des chercheurs stagiaires pour y recueillir des informations importantes d'ordre scientifique.

Le séjour terminé, l'étudiant-chercheur rentre dans son pays d'origine où il sera soigneusement «débriefé» de ses connaissances techniques et scientifiques fraîchement acquises.

Le monde académique se montre en général assez ouvert à la diffusion du savoir et à la coopération internationale, d'où la facilité pour n'importe quel chercheur de recueillir des informations sans même les avoir demandées.

C'est la raison pour laquelle les services de sécurité devraient être attentifs à la présence de stagiaires étrangers dans des laboratoires de recherches de pointe.

5.3. La prise de participation dans une société

Certaines entreprises engagées dans la veille technologique disposent de fonds d'investissement afin de prendre des participations dans des sociétés de haute technologie.

Une personne «neutre», agissant pour le compte d'une compagnie (ou d'un État) qui désire rester dans

wenst te blijven, neemt via « façade-bedrijven » en tussenpersonen een participatie in de beoogde vennootschap, bijvoorbeeld wanneer deze laatste leverancier is in een geavanceerde sector.

Zo krijgt men toegang tot technologische informatie, eventueel tot geclassificeerd materieel, of kan men materieel verkopen dat het voorwerp is van een embargo.

5.4. Verduisteren van octrooien

Een octrooi verleent aan de uitvinder het monopolie inzake de exploitatie van een procédé of een uitvinding, maar vormt zeker geen waarborg voor de vertrouwelijkheid.

Wel integendeel, de documentatie in de octrooien is een open bron die heel wat inlichtingen bevat. Dat is ook de reden waarom bepaalde bedrijven aarzelen om octrooien in te dienen voor sommige van hun uitvindingen die ze geheim willen houden.

5.5. Valse aanbestedingen

Met behulp van een aanbesteding laat een staat weten dat hij een exploitatielicentie of een sleutelklare fabriek wenst te verwerven. Onmiddellijk nadat ze daarvan kennis hebben genomen, sturen grote bedrijven hun handelsingenieurs ter plaatse.

Wanneer de onderhandelingen aanslepen, verstrekken de bedrijven die de opdracht in de wacht willen slepen steeds meer informatie zonder daar veel erg in te hebben. Op die manier leveren ze de inlichtingen die het betrokken land hoopte te verkrijgen.

Ook een private onderneming kan op deze manier te werk gaan, door zich via een onderzoeksbureau aan te bieden als een potentiële klant.

5.6. Valse rekruteringsadvertenties

Ook rekruteringsbureaus kunnen dienen om economische inlichtingen te verzamelen. De werkwijze bestaat erin een aantrekkelijke advertentie te publiceren die de aandacht kan trekken van kaderleden of onderzoekers van een onderneming die het doelwit vormt.

Al wie op zoek is naar een hoger loon, betere onderzoeksvoorwaarden en diverse voordelen (bedrijfswoning en -wagen, diverse vergoedingen, enz.) sturen hun CV op.

De betrokkenen worden vervolgens uitgenodigd voor een interview tijdens hetwelk ze langdurig worden ondervraagd over hun kwalificaties en over hun vroegere en huidige werkzaamheden.

l'ombre, procède grâce à des sociétés-écrans et des relais à la prise de participation dans la société cible, par exemple lorsque celle-ci est fournisseur dans un secteur de pointe.

Cela permet d'avoir accès à des informations d'ordre technologique, éventuellement à du matériel classifié ou de vendre du matériel soumis à embargo.

5.4. Le détournement de brevets d'invention

Le brevet entraîne le monopole d'exploitation d'un procédé ou d'une invention au profit de son inventeur mais il ne garantit aucunement sa confidentialité.

Bien au contraire, la documentation contenue dans les brevets constitue une source ouverte extrêmement riche de renseignements. C'est d'ailleurs la raison pour laquelle certaines entreprises hésitent à déposer des brevets pour certaines de leurs inventions dont elles désirent garder le secret.

5.5. Les faux appels d'offres

Un État fait savoir par des appels d'offres qu'il désire se rendre acquéreur d'une licence d'exploitation ou d'une usine livrée clé sur porte. Aussitôt sollicitées, les grandes sociétés réagissent en dépêchant sur place leurs ingénieurs commerciaux.

Les tractations traînant en longueur, les sociétés en lice fournissent de plus en plus d'informations sur leur offre sans y voir malice, espérant obtenir le marché. Elles livrent ainsi des renseignements qu'attendait le pays demandeur.

Une firme privée peut aussi agir de la sorte en se présentant, via un cabinet d'investigation, comme client potentiel.

5.6. Les fausses annonces de recrutement

Les cabinets de recrutement peuvent aussi servir à la collecte de renseignements d'ordre économique. La méthode consiste à publier une annonce alléchante capable de retenir l'attention de cadres ou de chercheurs d'une entreprise cible.

Les personnes intéressées par une meilleure proposition salariale, des conditions de recherche améliorées et divers avantages (appartement et voiture de fonction, indemnités diverses, etc.) expédient leur CV.

Celles-ci sont convoquées pour un entretien au cours duquel elles sont longuement interrogées sur leur qualification, leurs travaux antérieurs et actuels.

Wanneer ze de functie heel graag willen, zullen ze geneigd zijn zich te doen gelden door vertrouwelijke informatie te onthullen waarvoor de concurrerende onderneming of de staat die achter het rekruteringsbureau schuilgaat zeker belangstelling zal hebben.

5.7. Netwerken van informanten van de bedrijven

Sommige bedrijven richten echte netwerken van gespecialiseerde correspondenten op, die de opdracht krijgen om te observeren en inlichtingen op informele, niet-gestructureerde wijze te verzamelen. Om hun informatie aan de analisten te bezorgen, gebruiken ze standaardformulieren.

Deze personen zijn «reizigers» van het bedrijf of vertegenwoordigers, die dankzij hun bevoorrechte relatie met de leveranciers, de onderaannemers en de klanten nieuwe informatie kunnen verkrijgen over de behoeften, de projecten, de evoluties van de concurrenten.

5.8. Bezoeken van tentoonstellingen, colloquia, congressen, beurzen en salons

Deze bijeenkomsten van experts vormen een belangrijke bron van informatie voor al wie op professionele wijze economische inlichtingen verzamelt ... en voor spionnen.

De handelingen van dergelijke bijeenkomsten worden systematisch bestudeerd. Interessante prospectussen worden verzameld, gescand en ingevoerd in databanken.

Monsters worden geanalyseerd, stukken worden gefotografeerd — met of zonder toelating —, specimens worden gekocht (of gestolen) en vervolgens ontleed. Debatten kunnen bijzonder interessante informatie opleveren, en hetzelfde geldt voor gesprekken in de wandelgangen of met een «drankje».

5.9. Intercepteren van communicatie (COMINT)(1)

Sinds september 1998 hebben de media aandacht voor het bestaan van een globaal netwerk voor het intercepteren van communicatie, dat de naam Echelon kreeg en is opgericht door de Verenigde Staten en

(1) Het concept «Comint» *(communication intelligence)* wordt gedefinieerd als het verzamelen van inlichtingen door het bewaken van telecommunicatie en het intercepteren van hun inhoud.

(2) Het zou gaan om een geheime alliantie die in 1947 werd opgericht met het oog op de organisatie van de samenwerking inzake inlichtingen tussen de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland.

Désireuses d'obtenir le poste, elles sont susceptibles de chercher à se faire valoir en livrant des informations confidentielles qui ne manqueront pas d'intéresser la société concurrente ou l'État caché derrière le bureau de recrutement.

5.7. Les réseaux d'informateurs des entreprises

Certaines entreprises mettent sur pied de véritables réseaux de correspondants spécialisés chargés d'observer et de recueillir des renseignements de nature informelle, non structurée. Ils utilisent, pour transmettre leurs informations aux analystes, des formulaires standardisés aussi appelés «capteurs d'informations».

Ce sont soit des «voyageurs» de l'entreprise, soit des représentants, qui par leurs contacts privilégiés avec les fournisseurs, les sous-traitants, les clients, peuvent obtenir de l'information fraîche sur les besoins, les projets, les évolutions des concurrents.

5.8. La fréquentation des expositions, des colloques, congrès, foires et salons

Ces rassemblements d'experts constituent une source considérable d'information pour les professionnels de l'intelligence économique, ... et pour les espions.

Les comptes rendus en sont systématiquement étudiés. Les prospectus intéressants sont récoltés pour être passés au scanner et introduits dans des banques de données.

Des échantillons sont analysés, des pièces sont photographiées — parfois clandestinement —, des spécimens sont acquis (ou dérobés) pour être décortiqués. Les questions débattues en séances contiennent des informations très intéressantes, les conversations de couloirs, autour d'un «drink», également.

5.9. L'interception des communications (COMINT)(1)

L'existence d'un réseau global d'interception des communications baptisé «Echelon» mis en place par les États-Unis et par les autres États membres de l'alliance UKUSA(2) a été médiatisée dès septembre

(1) Le concept Comint *(communication intelligence)* est défini comme étant la collecte de renseignements effectuée par la surveillance des télécommunications et l'interception de leur contenu.

(2) Il s'agirait d'une entente secrète de 1947 organisant la coopération entre les États-Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande en matière de renseignements.

de andere lidstaten van UKUSA(1). Deze media-aandacht is het gevolg van een reeks rapporten bestemd voor het Europees Parlement(2).

Volgens het vierde rapport, *«Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control) — part 4/4»*, zou dit netwerk, dat aanvankelijk op het Oostblok was gericht, lang vóór de ineenstorting van de communistische regimes van zijn oorspronkelijk militair doel zijn afgewend.

Hoofdstuk 5, getiteld *Comint and economic intelligence*, bevat enkele interessante passages waarin we onder meer lezen: *«Comint involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunication became available.*

Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. (...) Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint.»

De wetgeving van de UKUSA-lidstaten laat de inlichtingendiensten en sommige ministeries in deze landen inderdaad toe het opsporen van economische of commerciële inlichtingen te organiseren en dergelijke inlichtingen te verzamelen door gebruik te maken van Comint.

Zo laat de Amerikaanse *Economic Espionage Act* uit 1996 het FBI en andere federale instanties toe communicatie te intercepteren in het kader van economische contraspionage. Het STOA-rapport verwijst echter naar bepaalde gevallen (zonder weliswaar bewijzen daarvan te leveren) waarin Europese bedrijven belangrijke opdrachten zouden zijn misgelopen na de interceptie van hun communicatie tijdens internationale handelstransacties (Panavia European Fighter Aircraft Consortium, Thomson CSF, Airbus Industrie).

5.10. Nieuwe communicatietechnologieën

Vandaag zijn de moderne technieken van elektronische communicatie het doelwit van spionage: de illegale reproductie van computerbestanden, het cyberterrorisme enz. zijn middelen die kunnen worden aangewend om de infrastructuren van een Staat of een onderneming te saboteren.

(1) Het zou gaan om een geheime alliantie die in 1947 werd opgericht met het oog op de organisatie van de samenwerking inzake inlichtingen tussen de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland.

(2) Comité I, jaarverslag 1999, titel II A. Hoofdstuk 3.

1998 par une série de rapports destinés au Parlement européen(2).

Selon le quatrième rapport *«Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control) — part 4/4»*, ce système orienté à l'origine vers le bloc de l'est, aurait été détourné de sa finalité militaire initiale bien avant l'effondrement des régimes communistes.

Le chapitre 5 intitulé Comint and economic intelligence contient quelques passages intéressants qui indiquent notamment: *«Comint involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunication became available.*

Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. (...) Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint.»

La législation des pays membres de l'alliance UKUSA autorise en effet leurs agences de renseignement ainsi que certains ministères à programmer la recherche de renseignements d'ordre économique ou commercial et à en recevoir par le recours au Comint.

Ainsi, la loi américaine *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique. Mais le rapport STOA cite plutôt des cas (sans en apporter la preuve, il est vrai) dans lesquels des firmes européennes auraient été évincées de marchés importants par suite de l'interception de leurs communications au cours de transactions commerciales internationales (Panavia European Fighter Aircraft consortium, Thomson CSF, Airbus industrie).

5.10. Les nouvelles technologies de la communication

L'espionnage s'attaque à présent aux techniques modernes de communications électroniques. Le piratage des fichiers informatiques, le cyberterrorisme, etc. sont des techniques susceptibles d'être utilisées en vue de saboter les infrastructures d'un État ou d'une entreprise.

(1) Il s'agirait d'une entente secrète de 1947 organisant la coopération entre les États-Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande en matière de renseignements.

(2) Comité R, rapport d'activités 1999, titre II A. Chapitre 3.

Informaticaspecialisten doorzoeken voortdurend de websites van concurrerende bedrijven om de netwerken illegaal te kraken en op bedrieglijke wijze de hand te leggen op waardevolle informatie. Voorts kan men ook een kopie maken van de harde schijf van een draagbare computer.

6. De rol van de inlichtingendiensten op economisch gebied (in het buitenland)

6.1. Algemeen

Welke acties kan een inlichtingendienst ondernemen en welke middelen kan hij aanwenden om het wetenschappelijk en economisch potentieel van een land te beschermen?

België is niet het enige land dat zijn inlichtingendiensten heeft belast met de opdracht zijn wetenschappelijk of economisch potentieel te beschermen. Men kan deze opdracht op defensieve en op offensieve wijze invullen.

Gedurende de lange jaren die de Koude Oorlog heeft geduurd, gingen de inlichtingendiensten vooral op zoek naar macro-economische *intelligence* om inzicht te krijgen in de grote tendensen van de wereldeconomie en te kunnen anticiperen op haar ontwikkeling.

In de hele wereld wijdden inlichtingendiensten een belangrijk deel van hun activiteiten aan de werking van de economische systemen in de communistische landen. Uit de literatuur over de operaties van deze diensten in die tijd blijkt echter dat ze de economische toestand in die landen niet correct hebben ingeschat.

Zo zouden ze het BBP van de USSR, haar productiecapaciteiten en haar financiële situatie schromelijk hebben overschat, en bijgevolg konden ze de uiteindelijke val van het communisme vanaf 1989 niet voorzien.

De aard van de economische toekomstleer oogt vandaag heel anders. Het inzetten van de officiële inlichtingendiensten om s' lands economische activiteiten te bevorderen is vandaag werkelijkheid geworden. Landen zoals Japan en de Verenigde Staten richten hun inspanningen op sterke groeimarkten en -regio's. Sommige Europese landen, zoals Duitsland en Frankrijk, volgen hun voorbeeld op de voet.

Er zijn diverse strategische redenen om economische inlichtingen te gaan verzamelen: de evolutie van de prijs van sommige voedingsmiddelen voorzien, op voorhand het standpunt van sommige landen bij commerciële onderhandelingen te weten komen, toezicht houden op de wapenhandel, op gevoelige technologieën, de politieke en economische stabiliteit van een land beoordelen, enz.

Des spécialistes de l'informatique fouillent en permanence des sites web d'entreprises concurrentes afin de forcer illégalement les réseaux et de saisir de façon frauduleuse toute une série de données précieuses. Il est également possible de récupérer un ordinateur portable et d'en tirer une copie du disque dur.

6. Le rôle des services de renseignement en matière économique (à l'étranger)

6.1. Généralités

Quelles actions et quels moyens un service de renseignement peut-il mettre en oeuvre pour protéger le potentiel scientifique et économique d'un pays?

D'autres pays que la Belgique ont confié à leurs services de renseignement la mission de protéger leur potentiel scientifique et économique. Cette mission peut se concevoir de manière défensive et de manière offensive.

Durant les longues années de la guerre froide, la préoccupation des services de renseignement était la recherche d'information macro-économique pour comprendre les grandes tendances de l'économie mondiale et anticiper ses évolutions.

Les services de renseignement du monde entier ont déployé une part considérable de leurs activités à se poser des questions sur le fonctionnement des systèmes économiques dans les pays communistes. À lire la littérature consacrée à l'action de ces services à cette époque, ceux-ci n'auraient pourtant pas été en mesure d'apprécier correctement la situation économique de ces pays.

Par exemple, le PIB de l'URSS, ses capacités de production et sa situation financière auraient été largement surévaluée, d'où l'incapacité de prévoir l'effondrement final du système communiste à partir de 1989.

Aujourd'hui, la nature de la prospective économique a changé. L'utilisation des services officiels de renseignement pour promouvoir les activités économiques de la nation est devenu une réalité. Des pays comme le Japon et les États-Unis concentrent leurs efforts sur des marchés et des zones à fort potentiel de croissance. Certains pays européens comme l'Allemagne et la France leur emboîtent le pas dans cette direction.

Le renseignement économique peut être recherché pour de multiples raisons d'ordre stratégique telles que, prévoir l'évolution des prix de certaines denrées, connaître à l'avance la position de certains pays dans des négociations commerciales, surveiller le commerce des armes, les technologies sensibles, évaluer la stabilité politique et économique d'un pays, etc.

6.2. Japan

In Japan is de economie prioriteit nummer één. Vanaf het midden van de 19de eeuw kent dit land aan de verwerking van de technologische en industriële informatie een plaats van nationaal belang toe, door die informatie te beschouwen als een rijkdom die collectief moet worden geëxploiteerd. Bijgevolg staat de Japanse staat volledig ten dienste van zijn bedrijven en van de economische prioriteiten, in die mate dat zijn inspanningen nergens ter wereld worden geëvenaard.

Sommige auteurs ramen het budget dat Japan aan het zoeken naar informatie besteedt op 480 miljard frank (1), dat geld is in hoofdzaak afkomstig van de privé-sector.

Het ministerie van Handel en Industrie *(MITI — Ministry of International Trade and Industry)* beschikt over een organisatie die gespecialiseerd is in het inwinnen van economische en commerciële inlichtingen. Het gaat om *JETRO (Japanese External Trade Organisation)*, een instantie met tientallen kantoren in het buitenland die zich in hoofdzaak bezighouden met het zoeken naar informatie en, een stapje verder, met het verzamelen van inlichtingen.

Het Agentschap voor wetenschappen en techniek (STA), belast met het wetenschappelijk onderzoek onder toezicht van de eerste minister, kent talrijke beurzen toe om Japanse studenten de kans te bieden hun studies in het buitenland voort te zetten. Dit agentschap heeft onder meer een Centrum voor wetenschappelijke en technologische inlichtingen (JICST). Ook Japanse commerciële bedrijven, die wereldwijd ongeveer 60 000 personen tewerkstellen, vormen een zeer geschikt kader voor het bijeenbrengen van informatie, via een oneindig aantal contacten in de landen waar deze bedrijven zijn gevestigd.

Heel veel bedrijven beschikken bovendien over een eigen, bijzonder uitgewerkt systeem om informatie te verzamelen.

Deze strategie inzake wetenschappelijke en technologische inlichtingen wordt op het hoogste niveau gecoördineerd met de inlichtingendienst van de eerste minister, die Naichô wordt genoemd. De Japanse staat en de bedrijfswereld werken dus perfect met elkaar samen.

6.3. De Verenigde Staten

Sinds 1977 is een departement van het NSA *(National Security Agency)* belast met de opdracht aan het ministerie van Handel *(Department of*

(1) *DST, police secrète* — Roger Faligot en Pascal Krop — Flammarion.

6.2. Le Japon

Au Japon, l'économie a pris rang de priorité absolue. C'est dès le milieu du XIX^{e} siècle que ce pays a accordé au traitement de l'information technologique et industrielle une importance nationale, en la considérant comme une ressource à exploiter de manière collective. L'État nippon se consacre donc tout entier au service de ses entreprises et des priorités économiques, au point d'y consentir des efforts sans commune mesure avec ce qui se passe ailleurs dans le monde.

Certains ouvrages évaluent à 480 milliards de francs belges le budget de la recherche d'informations au Japon (1) essentiellement financé par le secteur privé.

C'est ainsi que le ministère du Commerce et de l'Industrie *(MITI — Ministry of International Trade and Industry)* dispose d'une organisation spécialisée dans le renseignement économique et commercial, le *JETRO (Japanese External Trade Organisation),* qui entretient plusieurs dizaines de bureaux à l'étranger, pour l'essentiel voués à la recherche de l'information et, au-delà, du renseignement.

L'Agence des sciences et des techniques (STA), chargée de la recherche scientifique sous la tutelle du premier ministre, octroie de nombreuses bourses pour permettre à des étudiants japonais de poursuivre leurs études à l'étranger. Cette agence dispose d'un Centre de renseignement scientifique et technologique (le JICST). Les compagnies commerciales japonaises, qui emploient près de 60 000 personnes dans le monde, offrent également un cadre parfait pour le recueil d'informations, par le biais d'une infinité de contacts dans les pays où elles sont implantées.

De très nombreuses entreprises disposent de leur propre système de collecte, extrêmement élaboré.

Cette stratégie de renseignement scientifique et technologique est coordonnée au plus haut niveau avec le service de renseignement du premier ministre, le Naichô. L'État japonais et les entreprises fonctionnent donc en parfaite symbiose.

6.3. Les États-Unis

Il existe depuis 1977 un département de la NSA *(National Security Agency)* qui a pour mission de fournir des données au *Departement of Commerce*

(1) *DST, police secrète* — Roger Faligot et Pascal Krop — Flammarion.

Commerce) informatie te bezorgen die kan worden aangewend bij het ondersteunen van economische en commerciële belangen.

De benadering van de Amerikanen is een stuk minder centraliserend en veel liberaler dan die van Japan. Een van de huidige doelstellingen van het algemeen beleid in de Verenigde Staten bestaat erin overal ter wereld de Amerikaanse economische belangen, van overheidsinstanties en van de privé-sector, te verdedigen en te steunen. Dit gebeurt binnen het kader van een samenleving die is gebaseerd op de open toegang tot alle markten, de vrijheid van ondernemen, globalisering en deregularisatie.

In de Verenigde Staten is er lange tijd een heftig debat gevoerd tussen, enerzijds, de aanhangers van de stelling volgens dewelke de inlichtingendiensten hun middelen ten dienste moesten stellen van de ondernemingen en, anderzijds, de verdedigers van een liberaler standpunt dat voorschreef dat staatszaken niet mochten worden vermengd met de belangen van de privé-sector.

In het eerste geval ligt de grootste moeilijkheid in de manier waarop de inlichtingendiensten en de bedrijven moeten samenwerken om te voorkomen dat bepaalde industriëlen worden bevoordeeld ten nadele van anderen en te verzekeren dat de normale gang van de markteconomie niet wordt verstoord.

Het debat hierover heeft een centrale plaats ingenomen in de discussie over de rol van de geheime diensten sinds het einde van de Koude Oorlog.

In april 1992 lichtte Robert Gates, directeur van de CIA, in een verklaring voor het Huis van Afgevaardigden zijn verzet toe tegen de praktijk van economische of bedrijfsspionage (1).

Daarmee week hij af van de zienswijze van een van zijn voorgangers, admiraal Stanfield Turner, die de CIA had geleid van maart 1977 tot januari 1981 en betreurde dat zijn dienst ter zake steeds blijk had gegeven van terughoudendheid:

«Ik heb aanzienlijke inspanningen geleverd om de Amerikaanse bedrijfswereld vooruit te helpen; maar de professionelen van de CIA zeiden me dat deze dossiers geen uitstaans hadden met de nationale veiligheid» (2).

Na zijn verkiezing tot president van de Verenigde Staten beschouwde Bill Clinton het consolideren van de regio's waar de Amerikanen traditioneel commerciële invloed uitoefenen, alsook het veroveren van nieuwe markten, als een van de prioriteiten van zijn

(1) *Washington Post*, 14 maart 1993, geciteerd door Jean Guisnel in *Guerre dans le Cyberespace*, 1995.

(2) *Time Magazine*, 28 mei 1990, geciteerd door Jean Guisnel in *Guerre dans le Cyberespace*, 1995.

susceptibles d'être utilisées en vue de soutenir des intérêts économiques et commerciaux.

L'approche américaine est beaucoup moins centralisatrice et beaucoup plus libérale que celle du Japon. Un des objectifs actuels de la politique générale des États-Unis est de défendre et de promouvoir leurs intérêts économiques, publics et privés, partout dans le monde, dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Le débat est longtemps demeuré vif aux États-Unis entre les tenants de la thèse voulant que les services de renseignement mettent leur moyen au service des entreprises, et ceux qui optent pour une position plus conforme avec les principes libéraux exigeant que les affaires de l'État ne soient pas confondues avec celles du secteur privé.

Dans la première hypothèse, le principal problème réside dans la manière dont les services et les entreprises doivent coopérer afin de ne pas favoriser certains industriels aux dépens d'autres, et de ne pas fausser le jeu normal de l'économie de marché.

Le débat sur cette question est devenu un thème central de discussion sur le rôle des services secrets dès la fin de la guerre froide.

En avril 1992, le directeur de la CIA Robert Gates, s'exprimant devant la Chambre des représentants, affirmait clairement son opposition à la pratique de l'espionnage économique et industriel (1).

Cette attitude n'était cependant pas celle d'un de ses prédécesseurs, l'amiral Stanfield Turner, en poste de mars 1977 à janvier 1981 qui regrettait l'attitude timide de son service en cette matière:

«J'ai fait de gros efforts pour aider le monde américain des affaires; mais les professionnels de la CIA m'ont dit qu'il ne s'agissait pas là de dossiers intéressant la sécurité nationale» (2).

Parvenu à la présidence des États-Unis, Bill Clinton a considéré la consolidation des zones d'influence commerciales américaines traditionnelles, de même que la conquête de nouveaux marchés, comme l'une des priorités de son mandat en matière de politique

(1) *Washington Post*, 14 mars 1993, cité par Jean Guisnel *Guerre dans le cyberespace*, 1995.

(2) *Time Magazine*, 28 mai 1990, cité par Jean Guisnel *Guerre dans le Cyberespace*, 1995.

mandaat op het vlak van buitenlands beleid. In 1993 bood hij de ondersteuning van de Amerikaanse inlichtingengemeenschap aan privé-ondernemingen aan via de oprichting van de *National Economic Council*, parallel met de *National Security Council*.

In de Verenigde Staten worden economische inlichtingen dus beschouwd als een wezenlijk onderdeel van de nationale veiligheid, en staan ze op hetzelfde niveau als diplomatieke, militaire en technologische inlichtingen.

In 1994 verklaarde James Woolsey, directeur van de CIA: «Wij spioneren niet voor privé-ondernemingen. Indien we echter vaststellen dat vreemdelingen zich schuldig maken aan corruptie, brengen we het Witte Huis, het ministerie van Buitenlandse Zaken en het ministerie van Handel op de hoogte, die vervolgens proberen de situatie recht te trekken, en vaak slagen ze daar ook in».

Op 14 juli 1995 heeft Bill Clinton de CIA hartelijk gelukgewenst, nadat deze dienst gevallen van corruptie had ontdekt die ertoe zouden hebben geleid dat Amerikaanse ondernemingen contracten ter waarde van miljarden dollar misliepen. «Uw werk heeft bijgedragen tot de welvaart van Amerika», verklaarde hij.

In 1997 gaf een voormalig adjunct-directeur van de CIA, John Gannon, die voorzitter was geworden van de *National Intelligence Council*, uitleg bij de opdrachten inzake economische inlichtingen, die van tweeërlei orde waren:

— op strategisch vlak gaat het erom te waarschuwen in verband met internationale economische tendensen die invloed kunnen hebben op de Amerikaanse belangen; meer specifiek betekent dit dat men moet anticiperen op economische crisissen, op de bedreigingen van het energieaanbod in de wereld, dat men de economische prestaties van sommige landen moet evalueren, en moet toezien op de economische impact van internationale sancties;

— op tactisch vlak komt het erop aan informatie over en een analyse van belangrijke economische factoren te bezorgen aan de Amerikaanse beleidsvormers, ter ondersteuning van hun dagelijkse besluitvormingsprocessen en van hun interactie met hun confraters in het buitenland. Het gaat er met name om «zich ervan te vergewissen dat alle landen dezelfde economische spelregels naleven».

De CIA-verantwoordelijken zijn dus van mening dat ze niet rechtstreeks moeten tussenkomen voor rekening van Amerikaanse bedrijven tegen buitenlandse ondernemingen, maar dat ze de clandestiene economische spionage moeten beperken tot domeinen zoals commerciële onderhandelingen, het beschermen van nationale bedrijven tegen de penetratie door geheim- agenten uit het buitenland en het aan

étrangère. En 1993, il a offert l'appui de la communauté américaine du renseignement aux compagnies privées en créant le *National Economic Council* parallèlement au *National Security Concil*.

Aux États-Unis, le renseignement économique est donc considéré comme une composante essentielle de la sécurité nationale, bénéficiant d'une priorité équivalente à celle du renseignement diplomatique, militaire et technologique.

En 1994, le directeur de la CIA, James Woolsey déclarait: «Nous n'espionnons pas au profit de firmes privées. Mais nous portons les cas de corruption pratiquée par des étrangers à la connaissance de la Maison Blanche, du Département d'État et du ministère du Commerce, qui ensuite tentent de redresser la barre, souvent avec succès.».

Le 14 juillet 1995, Bill Clinton a félicité chaudement la CIA d'avoir su découvrir des cas de corruption qui auraient permis de soustraire des milliards de dollars de contrats à des entreprises américaines. «Votre travail a contribué à la prospérité américaine» a-t-il déclaré.

En 1997, un ancien directeur adjoint de la CIA, John Gannon, devenu président du *National Intelligence Concil* a expliqué que les missions de renseignement économique sont de deux ordres:

— au plan stratégique, il s'agit d'alerter sur les tendances économiques internationales qui peuvent avoir un impact sur les intérêts américains; plus spécifiquement cela signifie anticiper les crises économiques, les menaces sur l'offre énergétique mondiale, évaluer les performances économiques de certains États, surveiller l'impact économique des sanctions internationales;

— au niveau tactique, il s'agit de fournir une information et une analyse sur les enjeux économiques importants aux responsables américains, en appui à leurs processus quotidiens de décision et à leurs interactions avec leurs homologues étrangers. Il convient notamment de «s'assurer que tous les pays jouent avec les mêmes règles du jeu économique».

Les officiels de la CIA pensent donc qu'ils ne doivent pas mener directement des actions contre des firmes étrangères pour le compte d'entreprises américaines, mais qu'ils doivent contenir l'espionnage économique clandestin à des domaines tels que les négociations commerciales, la protection des firmes nationales contre la pénétration par des agents secrets étrangers et la mise à jour de corruption rendant diffi-

het licht brengen van gevallen van corruptie die de concurrentie in ontwikkelingslanden bemoeilijken (2).

In zijn boek *Guerre dans le Cyberespace*, gepubliceerd in 1995, beschrijft Jean Guisnel nochtans een paar gevallen waarin de interventie van de Amerikaanse inlichtingendiensten er wellicht toe heeft bijgedragen dat Amerikaanse bedrijven belangrijke internationale contracten in de wacht konden slepen. Daartoe behoren onder meer de gevallen die Duncan Campbell heeft beschreven in zijn rapport over het netwerk Echelon, dat hij in februari 2000 bij het Europees Parlement heeft ingediend (3).

De bespreking van dit rapport heeft overigens opnieuw aanleiding gegeven tot het rechtvaardigen van de praktijken inzake economische inlichtingen van de Amerikaanse inlichtingendiensten.

James Woolsey, niet langer directeur van de CIA, bevestigde dat zijn dienst inderdaad Europese bedrijven in het oog had gehouden die concurreerden met Amerikaanse ondernemingen binnen het kader van internationale transacties, omdat de Europeanen zich schuldig zouden hebben gemaakt aan corruptie om de beoogde opdrachten binnen te halen (1).

Alleen de buitenlandse regeringen die het voorwerp waren van deze manoeuvers zouden kennis hebben gekregen van het feit dat de Amerikanen de zaak niet licht opvatten.

Vervolgens gaf de heer Woolsey lucht aan zijn kritiek op het interventionisme van de Europese regeringen die, vaak op deloyale wijze, hun bedrijven steunen, ook al zijn ze duurder en minder performant dan hun Amerikaanse concurrenten: *It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith*, verweet hij de Europese regeringen.

Indien ze blijk zouden geven van de bereidheid hun staatsgeleide economieën te hervormen, teneinde ze doeltreffender te maken en meer ontvankelijk voor vernieuwing, dan zouden ze niet langer hun toevlucht moeten zoeken tot corruptie en zouden de Amerikanen het niet meer nodig vinden hen te bespioneren, besloot de heer Woolsey. Ook al gaf hij toe dat de CIA actief was op het gebied van economische inlichtingen, verklaarde hij ook dat 95 % van de ingewonnen informatie afkomstig was van open bronnen.

Hij herhaalde dat zijn dienst niet betrokken was bij activiteiten van economische spionage ten gunste van

(1) *The Wall Street Journal* d.d. 7 maart 2000.

(2) *Los Angeles Times*, 15 juli 1995, geciteerd door Jean Guisnel in *Guerre dans le Cyberespace*, 1995.

(3) De gevallen van ondernemingen als *Panavia European Fighter Aircraft Consortium*, *Thomson CSF* en *Airbus Industrie* worden genoemd in het STOA-rapport *Development of surveillance technology and risk of abuse of economic information — part 4/4*.

cile la compétition dans des nations en développement (1).

Le livre de Jean Guisnel *Guerre dans le Cyberespace*, paru en 1995, décrit pourtant quelques cas dans lesquels l'intervention des services de renseignement américains a sans doute permis à des firmes américaines de décrocher d'importants contrats internationaux. Parmi ceux-ci, on relève déjà les cas cités par Duncan Campbell dans son rapport présenté en février 2000 au Parlement européen sur le réseau « Echelon » (3).

La discussion de ce rapport a d'ailleurs donné lieu à une nouvelle justification de la pratique du renseignement économique de la part des services de renseignement américains.

En effet, James Woolsey, n'étant plus alors directeur de la CIA, a confirmé que son service avait bien surveillé des firmes européennes en compétition avec des firmes américaines au cours d'importantes transactions internationales et ce, parce que les européens auraient eu recours à la corruption pour obtenir les marchés convoités (1).

Seuls les gouvernements étrangers faisant l'objet de ces manoeuvres auraient été avertis que les américains ne le prenaient pas à la légère.

Et M. Woolsey de critiquer l'interventionnisme des gouvernements européens qui soutiennent, souvent de manière déloyale, leurs entreprises plus coûteuses et moins performantes que les entreprises américaines: *it is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith* lance-t-il à l'adresse des gouvernements européens.

Si ceux-ci voulaient bien réformer leurs économies étatiques, pour les conduire à plus d'efficacité et d'innovation, ils ne devraient plus avoir recours à la corruption et les américains n'auraient plus besoin de les espionner, conclut M. Woolsey. Mais s'il admet que la CIA pratique le renseignement économique, il affirme aussi que 95 % des informations collectées proviennent de sources ouvertes.

Il répète que son service n'est pas engagé dans des opérations d'espionnage économique au profit

(1) *Wall Street Journal*, 7 mars 2000.

(2) *Los Angeles Times*, 15 juillet 1995 cité par Jean Guisnel dans *Guerre dans le Cyberespace*, 1995.

(3) Les cas des firmes *Panavia European Fighter Aircraft Consortium*, *Thomson CSF* et *Airbus industrie* sont cités dans le rapport STOA *Development of surveillance technology and risk of abuse of economic information — part 4/4*».

Amerikaanse bedrijven of vennootschappen. Nochtans verschenen de voorbije jaren in de pers artikelen over Amerikaanse agenten (van wie sommigen het statuut van diplomaat hadden) die op beschuldiging van economische spionage door Europese landen waren uitgewezen.

Van zijn kant lijkt het *Federal Bureau of Investigation* (dit is de federale gerechtelijke politie) ter zake een louter defensieve rol te spelen. In 1998 verklaarde een verantwoordelijke inzake nationale veiligheid bij het FBI, tijdens een verhoor in het Congres, dat buitenlandse inlichtingendiensten een eersterangsrol vervulden op het vlak van bedrijfs- en economische spionage ten behoeve van hun eigen nationale bedrijven. Daarbij hadden ze vooral aandacht voor geavanceerde technologieën en octrooien, maar ook voor vertrouwelijke informatie betreffende contracten, aanbestedingen, handelsstrategieën, enz.

Op 13 september 2000, organiseerde het *International Economic Policy and Trade Subcommittee* van het Huis van Afgevaardigden opnieuw een reeks verhoren teneinde de ontwikkelingen op het vlak van economische spionage tegen Amerikaanse bedrijven te beoordelen.

Amerikaanse onderzoeks- en economische inlichtingenbureaus hebben overigens gepoogd de verliezen te ramen die de Amerikaanse economie heeft geleden tengevolge van economische spionage: de ramingen schommelen tussen 42 en 200 miljoen $ per jaar.

Het FBI houdt dus in het bijzonder buitenlandse communicatiebedrijven die zich in de Verenigde Staten willen vestigen nauwlettend in het oog. Het FBI vreest immers dat deze vreemde operatoren van hun controle op de Amerikaanse netwerken gebruik maken om bedrijven te gaan afluisteren voor rekening van de inlichtingendiensten van hun land.

Voorts houdt het FBI toezicht op de operaties waarbij buitenlandse groepen de controle verwerven over Amerikaanse ondernemingen; het doet dit binnen het kader van een federale wet krachtens dewelke de president van de Verenigde Staten bevoegd is om elke acquisitie te verbieden «die een weerslag kan hebben op de nationale veiligheid».

De *Economic Espionage Act* van 1996 laat het FBI en andere federale instanties toe communicatie te intercepteren binnen het kader van economische contraspionage.

6.4. Canada

De *Canadian Security Intelligence Service (CSIS)* heeft een structuur gecreëerd die gespecialiseerd is in raadgevingen inzake contraspionage ten behoeve van de bedrijfswereld.

In zijn jaarverslag van 1998 had het Comité I al gewezen op de problemen die de CSIS ondervond om

d'entreprises ou de sociétés américaines. Au cours de ces dernières années, la presse a cependant rapporté des cas d'agents américains (dont certains ayant le statut de diplomate) expulsés de pays européens sous l'accusation d'espionnage économique.

Le *Federal Bureau of Investigation* (c'est-à-dire la police judiciaire fédérale) semble quant à lui jouer un rôle purement défensif en la matière. En 1998, un responsable de la sécurité nationale au FBI a affirmé lors d'une audition au congrès que les services de renseignement étrangers jouaient un rôle de premier plan dans l'espionnage industriel et économique au profit de leurs propres entreprises nationales, visant particulièrement les technologies de pointe, les brevets, mais aussi des informations confidentielles sur des contrats, des appels d'offre, des stratégies commerciales, etc.

Le 13 septembre 2000, l'*International Economic Policy and Trade Subcommittee* de la Chambre des représentants a organisé une nouvelle série d'auditions afin d'évaluer les évolutions de l'espionnage économique contre les entreprises américaines.

Des cabinets d'investigation et d'intelligence économique américains ont d'ailleurs tenté d'estimer les pertes occasionnées à l'économie américaine par l'espionnage économique: les estimations oscillent entre 42 et 200 millions $ par an.

Le FBI surveille donc de manière particulièrement attentive les firmes de communication étrangères qui cherchent à s'implanter aux États-Unis. Le FBI redoute en effet que ces opérateurs étrangers ne profitent de leur contrôle sur des réseaux américains pour mettre sur écoute des entreprises pour le compte des services de renseignement de leurs pays.

De même, le FBI surveille les opérations de prise de contrôle d'entreprises américaines par des groupes étrangers dans le cadre d'une loi fédérale qui permet au président des États-Unis d'interdire toute acquisition «pouvant affecter la sécurité nationale».

Le *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique.

6.4. Le Canada

Le «Service Canadien du Renseignement de Sécurité» (SCRS) a créé une structure spécialisée dans le conseil de contre-espionnage au profit des entreprises.

Dans son rapport d'activités de 1998, le Comité R avait relevé la difficulté qu'éprouvait le SCRS à

zijn opdracht af te bakenen binnen een al te ruime definitie van het begrip «economische veiligheid». We vinden een preciezere beschrijving van deze opdracht inzake economische veiligheid in een periodieke publicatie van deze dienst, getiteld *Série d'aperçus* (nr. 6 van mei 1998).

Een van de voornaamste doelstellingen van de CSIS bestaat erin toe te zien op de activiteiten in Canada van bekende of vermoedelijke buitenlandse inlichtingenofficieren, alsook te beletten dat buitenlandse bezoekers, studenten of afgevaardigden, van wie men vermoedt dat ze actief zijn in het inlichtingenwezen, het Canadese grondgebied betreden.

De opdracht van de CSIS inzake economische spionage bestaat erin onderzoek te verrichten naar de clandestiene activiteiten van vreemde regeringen, aangezien ze nadelig kunnen zijn voor de economische en commerciële belangen van Canada.

Hij probeert de Canadese regering te waarschuwen wanneer de billijke spelregels van de concurrentie op de vrije markt opzettelijk worden omgebogen ten nadele van de Canadese bedrijfswereld.

De CSIS heeft geen belangstelling voor bedrijfsspionage, d.w.z. spionage beoefend door de ene privé-onderneming tegen de andere. Zijn dergelijke activiteiten van criminele aard, dan wordt een onderzoek gevoerd door de politiediensten.

De dienst maakt gewag van een geval waarin een buitenlandse regering ervan werd verdacht telefoongesprekken te hebben afgeluisterd tussen een Canadese zakenman op reis in het buitenland en de hoofdzetel van zijn onderneming in Canada.

De betrokken Canadezen hadden in detail gesproken over lopende onderhandelingen, i.h.b. over een precieze minimumofferte. De volgende dag diende een buitenlandse concurrent een tegenvoorstel in dat overeenstemde met die minimumofferte.

De CSIS preciseert verder dat economische spionage niet alleen wordt beoefend door regeringen die Canada traditioneel vijandig gezind zijn, maar dat er aanwijzingen bestaan dat ook zogenaamd bevriende landen zich daartoe lenen.

6.5. Frankrijk

De wet van 16 juli 1980 bestraft elke mededeling aan een vreemde overheid, «(die) van aard (is) schade toe te brengen aan de soevereiniteit, de veiligheid, de essentiële economische belangen van Frankrijk of aan de openbare orde, voor zover nodig nauwkeuriger beschreven door de administratieve overheid» (1).

De definitie van de «fundamentele belangen van de natie» in artikel 410 van het nieuwe Strafwetboek

(1) Vrije vertaling.

circonscrire sa mission dans le cadre d'une définition trop large de la notion de sécurité économique. Cette mission de sécurité économique se trouve décrite de manière plus précise dans une publication périodique éditée par ce service et intitulée *Série d'aperçus* (nº 6 de mai 1998).

Un des principaux objectifs du SCRS est de surveiller les activités menées au Canada par des officiers de renseignements étrangers, connus ou présumés, et d'empêcher des visiteurs, étudiants ou délégués étrangers soupçonnés d'activités de renseignement d'entrer au Canada.

Le mandat du SCRS en matière d'espionnage économique est d'enquêter sur les activités clandestines de gouvernements étrangers qui sont susceptibles de nuire aux intérêts économiques et commerciaux du Canada.

Le SCRS s'efforce de prévenir le gouvernement lorsque les règles du jeu équitables de la concurrence sur le marché libre sont délibérément infléchies contre le secteur industriel canadien.

Le SCRS ne s'intéresse pas à l'espionnage industriel, c'est-à-dire à l'espionnage exercé par une firme du secteur privé contre une autre. Lorsque ces activités sont de nature criminelle, ce sont les services d'application de la loi *law enforcement* qui enquêtent.

Le SCRS fait état d'un cas où un gouvernement étranger est soupçonné d'avoir intercepté des conversations téléphoniques entre un homme d'affaires canadien en voyage à l'étranger et le siège de son entreprise au Canada.

Les canadiens avaient discuté en détail de négociations en cours, notamment d'une offre minimale précise. Le lendemain, la société concurrente étrangère a fait une contre-proposition correspondant à cette offre minimale.

Le SCRS précise plus loin que l'espionnage économique n'est pas seulement le fait de gouvernements traditionnellement hostiles au Canada, mais qu'il existe des signes que certains pays considérés comme amis s'y livrent également.

6.5. La France

La loi du 16 juillet 1980 réprime notamment toute communication à une autorité publique étrangère, «de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin» (1).

La définition que l'article 410 du nouveau code pénal (1992) donne des «intérêts fondamentaux de la

(1) Traduction libre.

(1992) verwijst uitdrukkelijk naar «de essentiële belangen van haar wetenschappelijk en economisch potentieel».

De wet van 10 juli 1991 betreffende het geheim van de correspondentie via telecommunicatiemiddelen voorziet redenen ter rechtvaardiging van het administratief intercepteren van communicatie.

Daartoe behoren onder meer het terrorisme, de georganiseerde misdaad, de nationale veiligheid, maar ook de vrijwaring van het economisch en wetenschappelijk potentieel. In 1999 werden in Frankrijk 4 577 intercepties uit veiligheidsoverwegingen toegelaten, waarvan 186 met het oog op het beschermen van het economisch en wetenschappelijk potentieel (1), dit is 4%.

Frankrijk besliste al snel zijn inlichtingendiensten in te zetten in het kader van activiteiten van economische spionage en contraspionage. De doorgedreven nationalisering van de Franse economie na de Tweede Wereldoorlog was zeker niet vreemd aan die beslissing.

Op het einde van de jaren tachtig was de *Direction Générale de la Sécurité Extérieure* (DGSE) betrokken bij diverse zaken van economische spionage in de Verenigde Staten (2). De Angelsaksische landen zouden dan ook niet de enige zijn die satellieten gebruiken om telecommunicatie te intercepteren in het kader van economische inlichtingenactiviteiten.

In zijn boek «*Le renseignement français à l'aube du XX^e siècle*» (3) verwijst Jean-Jacques Cécile naar een geval waarbij de DGSE economische «intelligence» zou hebben onderschept. Deze informatie zou rechtstreeks ten goede zijn gekomen aan de Franse automobielindustrie, die op dat ogenblik in een concurrentiestrijd was verwikkeld met een Duitse firma voor het bouwen van een fabriek in Latijns-Amerika.

Admiraal Pierre Lacoste, directeur van de DGSE van 1982 tot 1985, was echter van mening dat zijn dienst niet het risico moest lopen betrokken te raken bij «agressieve» operaties tegen bedrijven uit bevriende staten (4).

Claude Silberzahn, directeur van de DGSE van 1989 tot 1993, meende dan weer dat deze dienst niet kon handelen in het voordeel van de bedrijfswereld: de DGSE moet de Staat dienen.

(1) *Commission nationale de contrôle des interceptions de sécurité* — 8e jaarverslag 1999.

(2) Lees in verband hiermee: Claude Silberzahn, «*Au cœur du secret*», blz. 172 en 173; Jean Guisnel, «*Guerre dans le Cyberespace*» 1995.

(3) Uitgeverij Lavauzelle, 1998 — hoofdstuk 9, blz. 189.

(4) Pierre Lacoste, «*Les entreprises doivent apprendre à se protéger*», Capital, februari 1995.

nation» couvre explicitement «les intérêts essentiels de son potentiel scientifique et économique».

La loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit des motifs qui justifient la conduite d'interceptions administratives de communications.

Parmi ces motifs, on trouve le terrorisme, la criminalité organisée, la sécurité nationale, mais aussi la sauvegarde du potentiel économique et scientifique. Au cours de l'année 1999, 4 577 interceptions de sécurité ont été autorisées en France dont 186 à des fins de sauvegarde du potentiel économique et scientifique (1), soit 4%.

La France a très tôt engagé ses services de renseignement dans des opérations d'espionnage et de contre-espionnage économique. Le fait que l'économie française se soit trouvée largement nationalisée après la Seconde Guerre mondiale a joué très largement en ce sens.

À la fin des années quatre-vingt, la direction générale de la Sécurité extérieure (DGSE) a été impliquée dans différentes affaires d'espionnage économique aux États-Unis (2). Les pays anglo-saxons ne seraient pas ainsi les seuls à intercepter les télécommunications par satellites à des fins de renseignement économique.

Le livre de Jean-Jacques Cécile intitulé *le renseignement français à l'aube du XXIème siècle* (3) mentionne le cas d'une information d'ordre économique interceptée par la DGSE et qui aurait directement profité à l'industrie automobile française alors en concurrence avec une firme allemande pour l'installation d'une usine en Amérique latine.

L'amiral Pierre Lacoste, directeur de la DGSE de 1982 à 1985, estimait pourtant que son service ne devait pas courir le risque d'être pris dans des opérations «agressives» contre des entreprises d'États amis (4).

Claude Silberzahn, directeur de la DGSE de 1989 à 1993, estime quant à lui que ce service ne peut agir au profit des entreprises: c'est l'État qu'il se doit de servir.

(1) Commission nationale de contrôle des interceptions de sécurité — 8e rapport d'activité 1999.

(2) Lire à ce sujet: Claude Silberzahn, *Au coeur du secret*, pp. 172 et 173; Jean Guisnel, *Guerre dans le cyberespace* 1995;

(3) Editions Lavauzelle, 1998 — chapitre 9, p. 189.

(4) Pierre Lacoste, *les entreprises doivent apprendre à se protéger*, Capital, février 1995.

Indien er echter één domein is waar de inlichtingendiensten hun rol ten dienste van het collectief ten volle moeten opnemen, is het wel dat van de ondergrondse en illegale economie, die soms in handen is van de maffia, en van het misdaadgeld(1). In 1991 creëerde de DGSE dan ook een dienst gespecialiseerd inzake het opsporen van onwettige geldstromen. Deze dienst werkt samen met Tracfin.

Krachtens een decreet van de President van de Republiek werd op 1 april 1995 een *Comité pour la compétitivité et la sécurité économique* (CCSE) opgericht, dat aanvankelijk onder het gezag stond van de Eerste minister en vervolgens onder het toezicht van de minister van Economie, Financiën en het Plan; het *Secrétariat général de la défense nationale* (SGDN) voert het secretariaat van het Comité. Het CCSE telt zeven leden en kreeg de opdracht de aanbevelingen van het rapport-Martre inzake economische intelligentie uit te werken. Het Comité is echter niet in zijn opdracht geslaagd en werd in juli 1998 ontbonden.

In een rapport uit 1997, met de titel «*De la défense économique à la sécurité de l'économie*», onderzocht het *Commissariat général du plan* welke «de offensieve hefbomen van de Staat (moesten zijn) op het vlak van economische veiligheid».

Het beveelt met name de versterking van de bevoegdheden van de regering aan, zodat zij zich kan verzetten tegen strategische overnames, het bepalen van strafsancties in geval van inbreuk op het bedrijfsgeheim, het uitwerken van een nationaal beleid inzake normen en octrooien, het creëren van een netwerk voor de bewaking van nieuwe technologieën en van de concurrenten met bijzondere aandacht voor strategische thema's, het ontwikkelen van offensieve beïnvloedingsstrategieën en, tot slot, het uitbreiden van de onderzoekscapaciteiten inzake economische criminaliteit van de gerechtelijke politie, van de dienst *Renseignements généraux*, van de DST en van de douane.

De *Direction de la sécurité du territoire* (DST) is bevoegd om op het Franse grondgebied activiteiten op te sporen en te voorkomen die worden geïnspireerd, gevoerd of ondersteund door vreemde mogendheden en die een bedreiging kunnen vormen voor 's lands veiligheid; meer in het algemeen is deze dienst bevoegd om dergelijke activiteiten te bestrijden.

Met het oog op het uitvoeren van haar opdrachten, en binnen het kader van de instructies van de regering, moet de DST in het bijzonder bijdragen tot de veiligheid van de gevoelige punten en de kernsectoren van de nationale activiteit, alsook tot de bescherming van defensiegeheimen.

(1) Claude Silberzahn, «*Au cœur du secret*», blz. 177.

Mais s'il est un domaine où les services de renseignement doivent pleinement jouer leur rôle au service de la collectivité, c'est celui de l'économie souterraine, illégale et parfois maffieuse, et de la finance criminelle(1). En 1991, la DGSE a donc créé un service spécialisé en matière de détection des flux financiers illicites. Ce service collabore avec Tracfin.

Un décret du Président de la République a créé le 1er avril 1995 un Comité pour la compétitivité et la sécurité économique (CCSE) d'abord placé sous l'autorité du premier ministre, puis sous celle du ministre de l'Économie, des Finances et du Plan et dont le secrétariat général de la Défense nationale (SGDN) assure le secrétariat. Composé de sept membres, le CCSE était chargé de mettre en œuvre les recommandations du rapport «Martre» en matière d'intelligence économique. Ce comité a cependant échoué dans sa mission et il a été mis fin à son existence en juillet 1998.

Un rapport de 1997 rédigé par le commissariat général du Plan et intitulé «de la défense économique à la sécurité de l'économie» examine quels devraient être «les leviers offensifs de l'État dans le domaine de la sécurité économique».

Il prône notamment le renforcement des pouvoirs du gouvernement afin qu'il puisse s'opposer à des acquisitions stratégiques, l'établissement de sanctions pénales en cas d'infraction au secret d'entreprise, la définition d'une politique nationale des normes et brevets, l'organisation d'un réseau de veille technologique et concurrentielle ciblé sur des thèmes stratégiques, le développement de stratégies d'influences offensives et enfin l'accroissement des capacités d'enquête de la police judiciaire, des renseignements généraux, de la DST et des douanes en matière de criminalité économique.

La Direction de la sécurité du territoire (DST) a compétence pour rechercher et prévenir, sur le territoire de la République française, les activités inspirées, engagées ou soutenues par des puissances étrangères et de nature à menacer la sécurité du pays et, plus généralement, pour lutter contre ces activités.

Pour l'exercice de ses missions, et dans le cadre des instructions du gouvernement, la DST est notamment chargée de participer à la sécurité des points sensibles et des secteurs clés de l'activité nationale, ainsi qu'à la protection des secrets de défense.

(1) Claude Silberzahn, *Au cœur du secret*, p. 177.

De DST heeft dus een onderdirectie voor de bescherming van het patrimonium, die belast is met economische dossiers en waarvan het personeel de voorbije jaren sterk is aangegroeid. Sinds het einde van de jaren tachtig heeft de DST de gewoonte aangenomen samen te komen met bedrijfsleiders om hen bewust te maken van de noodzaak hun computernetwerken te beschermen, hun buitenlandse stagiairs in het oog te houden en vooral studenten uit «bevriende» landen niet al te snel te vertrouwen.

De DST organiseert voor de kaderleden van bedrijven conferenties over de manieren waarop ze hun productiegeheimen, het resultaat van hun opzoekingen en hun klantenbestanden beter kunnen beschermen. De dienst voor de bescherming van het patrimonium van de DST biedt aan de bedrijven, samen met de DST zelf, een Minitel-verbinding aan die hen toelaat inlichtingen in te winnen over de laatste ontwikkelingen inzake de bedreigingen tegen het Franse economisch weefsel.

Algemeen kunnen we stellen dat de toegenomen agressiviteit van vreemde landen, zelfs van economische en politieke partners van Frankrijk zoals de Verenigde Staten, Japan of Duitsland, deze herpositionering van de DST rechtvaardigde, nog vóór de ineenstorting van de USSR.

De betrekkingen tussen de bedrijfswereld en de Franse inlichtingendiensten zijn vandaag zo nauw dat de grootste ondernemingen die in de gevoeligste sectoren actief zijn — vooral in de wapensector — regelmatig ambtenaren van contraspionagediensten rekruteren die bijgevolg hun contract met de Staat opzeggen. Ook de *Direction du renseignement militaire* (DRM) bouwt haar relaties met de Franse bedrijfswereld uit.

Diverse Franse universiteiten en hogescholen hebben beslist economische inlichtingen op te nemen in hun onderwijsprogramma's en opleidingen. Vaak krijgen ze daarbij de hulp, of gebeurt dit op initiatief, van gewezen militairen en verantwoordelijken inzake nationale veiligheid.

Zo organiseert het «*Institut des hautes études de défense nationale*» (IHEDN), dat afhangt van het ministerie van Landsverdediging, lescycli inzake economische inlichtingen; belangrijke figuren van de Franse inlichtingendiensten hebben er al exposés gegeven.

Dit instituut heeft zich tot doel gesteld een volledig overzicht te maken van de praktijken inzake economische inlichtingen in Frankrijk. Het gebruikt daarvoor een vragenlijst bestemd voor alle Franse ondernemingen die meer dan 200 personen te werk stellen (1).

(1) www.ihedn.fr.

La DST comporte donc une sous-direction de la protection du patrimoine en charge des dossiers économiques et dont les effectifs ont été considérablement étoffés ces dernières années. La DST a pris pour habitude, depuis la fin des années quatre-vingt, de rencontrer des industriels afin de les sensibiliser à la nécessité de protéger leurs réseaux d'ordinateurs, de surveiller leurs stagiaires étrangers, et de se méfier singulièrement des étudiants venant de pays «amis».

La DST organise des conférences destinées aux cadres d'entreprises sur la manière de mieux protéger leurs secrets de fabrication, le produit de leurs recherches et leurs fichiers «clients». Le service de protection du patrimoine de la DST offre aux entreprises en relation avec elle une liaison par minitel leur permettant de s'enquérir des dernières évolutions en matière de menaces contre le tissu économique français.

D'une manière générale, l'agressivité accrue de pays étrangers, même partenaires économiques et politiques de la France, comme les États-Unis, le Japon ou l'Allemagne, fut la justification de ce repositionnement de la DST avant même l'effondrement de l'URSS.

Les relations sont aujourd'hui si étroites entre le monde de l'entreprise et les services français de renseignement que les plus grandes firmes liées aux domaines les plus sensibles — surtout dans le secteur de l'armement — recrutent régulièrement des fonctionnaires du contre-espionnage qui quittent le service de l'État. La Direction du renseignement militaire (DRM) développe également des relations avec les industries françaises.

Plusieurs universités et hautes écoles françaises se sont attachées à intégrer l'intelligence économique dans leurs programmes de cours et de formation, souvent avec l'aide, ou même à l'initiative d'anciens militaires et de responsables de la sécurité nationale.

Ainsi, l'Institut des hautes études de défense nationale (IHEDN) dépendant du ministère de la Défense nationale organise des cycles de cours sur la question; de hauts responsables des services de renseignement français y ont pris la parole.

Cet institut a entrepris de dresser un panorama complet des pratiques d'intelligence économique en France au moyen d'un questionnaire destiné à toutes les entreprises françaises occupant plus de 200 personnes (1).

(1) www.ihedn.fr.

Het «*Institut d'études et de recherches pour la sécurité des entreprises*» (IERSE) in Parijs biedt aan hoge kaderleden een universitaire opleiding aan betreffende de veiligheid van installaties en inzake economische inlichtingen. Dit instituut is ontstaan als gevolg van een partnership tussen belangrijke overheids- en particuliere instellingen zoals de Universiteit van Parijs I, de nationale gendarmerie, de *Direction générale des douanes et droits indirects*, de club voor de economische bescherming van de onderneming en de vereniging van Franse bedrijven (1).

De «*École de guerre économique*» (sic), in 1997 opgericht door een op rust gesteld generaal, «biedt onderwijs aan inzake de offensieve en defensieve strategieën waarmee bedrijven te maken krijgen in de economische concurrentiestrijd op wereldvlak».

Het lesprogramma van deze school omvat onder meer cursussen over «de strategie voor het aanwenden van informatie», «een professionele benadering van open bronnen», «de informatieoorlog», «zich beschermen tegen desinformatie», de «inlichtingencyclus», enz. (2)

Tot slot verwijzen we nog naar de Universiteit Sophia Antipolis in Nice, de cursussen van admiraal met rust Lacoste (ex-chef van de DGSE) aan de Universiteit van Marne-la-Vallée, enz.

6.6. Duitsland

Volgens Henri Martre, rapporteur voor het Franse *Commissariat général du plan* (3) is het Duitse model het meest performante systeem inzake economische inlichtingen van heel Europa. Dit model steunt boven alles op een diepgeworteld collectief bewustzijn van «economisch patriottisme» en op een consensus over wat het begrip nationaal economisch belang precies inhoudt. Deze cultuur is een van de grote troeven van de Duitse concurrentiekracht.

De «Bundesnachrichtendienst» (BND), dit is de externe inlichtingendienst van de Bondsrepubliek Duitsland, zou het centrum zijn waar alle economische informatiestromen samenkomen (4).

Aangezien de Duitse regering van oordeel is dat Azië op strategisch vlak een regio is waar bedrijven hun krachten bij voorrang moeten ontplooien, niet alleen op economisch vlak maar ook op het vlak van de inlichtingen, is het geen toeval dat de BND kanto-

(1) www.ierse.org.

(2) www.ege.escala.fr.

(3) Rapport van Henri Martre: *Intelligence économique et stratégie des entreprises*, Franse documentatie.

(4) *DST, police secrète* — Roger Faligot, Pascal Krop — Flammarion.

L'Institut d'études et de recherches pour la sécurité des entreprises (IERSE) à Paris a pour vocation de fournir une formation universitaire en matière de sûreté des installations et d'intelligence économique à des cadres de haut niveau. Cet institut est le fruit d'un partenariat entre organismes publics et privés importants tels que l'Université de Paris I, la gendarmerie nationale, la direction générale des douanes et droits indirects, le club de défense économique de l'entreprise et l'union des entreprises de France (1).

L'École de guerre économique (sic) fondée en 1997, notamment par un général en retraite, «propose un enseignement sur les méthodes d'attaque et de défense auxquelles sont confrontées les entreprises dans la compétition économique mondiale».

Le programme d'enseignement de cette école comporte notamment des cours sur la «stratégie d'utilisation de l'information», «l'approche professionnelle des sources ouvertes», «la guerre de l'information», les «parades contre la désinformation», le «cycle du renseignement», etc. (2).

On peut également citer l'Université Sophia Antipolis à Nice, les cours de l'amiral en retraite Lacoste (ex chef de la DGSE) à l'Université de Marne-la-Vallée, etc.

6.6. L'Allemagne

Selon Henri Martre, rapporteur pour le commissariat général du Plan français (3), le système d'intelligence économique le plus performant en Europe est le modèle allemand. Celui-ci s'appuie avant tout sur un profond sentiment collectif de «patriotisme économique» et un consensus sur la notion d'intérêt économique national. Cette culture est un des atouts de la compétitivité allemande.

Le «Bundesnachrichtendienst» (BND), c'est-à-dire le service de renseignement extérieur de la RFA, serait le centre vers lequel converge l'ensemble des flux d'informations économiques (4).

Le gouvernement allemand considérant l'Asie comme une zone prioritaire en termes stratégiques pour le redéploiement des forces, tant sur le plan économique que sur celui du renseignement, ce n'est pas un hasard si le BND a ouvert des postes à New

(1) www.ierse.org.

(2) www.ege.escala.fr.

(3) Rapport de Henri Martre: Intelligence économique et stratégie des entreprises, la documentation française.

(4) DST, police secrète — Roger Faligot, Pascal Krop — Flamarion.

ren heeft geopend in New Delhi, Peking, Jakarta, Tokio, Manilla, Seoul en Taiwan. De BND heeft een gegevensbank gecreëerd voor bedrijven die zich in deze regio's willen vestigen(1).

De BND stelt ook rapporten op voor het federaal ministerie van Economie, waarin Duitse bedrijfsleiders ertoe worden aangespoord waakzaam te zijn in hun betrekkingen met bepaalde landen die hoogtechnologische systemen willen kopen.

Een ander federaal orgaan is belast met het coördineren van initiatieven op het gebied van economische inlichtingen: het gaat om het «Arbeitsgemeinschaft für die Sicherheit des Wirtschafts» (ASW). Dit orgaan staat in contact met de federale inlichtingendienst, het «Bundesamt für Verfassungsschutz» (dienst ter bescherming van de Grondwet of BfV). Uit een rapport van 1997 van het BfV blijkt dat 62% van de spionagezaken die in Duitsland aan het licht zijn gekomen, betrekking hebben op het wetenschappelijk en economisch potentieel van het land, 19% op politieke en administratieve zaken, 8% op militaire zaken en 11% op andere sectoren.

Er zou een duidelijke stijging waarneembaar zijn van spionageactiviteiten in opdracht van de Russische inlichtingendiensten tegen Duitse private ondernemingen. In zijn jaarverslag van 1999 bevestigt het BfV dat de activiteiten van de Russische externe inlichtingendienst (SVR), alsook van de inlichtingendiensten van de GOS-landen, in hoofdzaak zijn gericht op economische, wetenschappelijke en technische spionage.

In een interview met het Franse maandblad «*Le Monde du Renseignement*»(2) verklaarde Peter Frisch, hoofd van het BfV, dat het begrip «strategisch economisch erfgoed» een deel van de 2 218 agenten van het BfV ertoe heeft gebracht bepaalde ondernemingen uit te kiezen teneinde ermee te gaan samenwerken.

Vandaag zijn 1 600 ondernemingen een partnership aangegaan met het BfV op federaal niveau. Binnen elk van deze ondernemingen is een werknemer verantwoordelijk voor de economische veiligheid en is die persoon de gesprekspartner van de inlichtingendienst.

De betrokken ondernemingen behoren niet alleen tot de wapenindustrie, maar ook tot de automobielindustrie, de petrochemische nijverheid en tot geavanceerde technologische sectoren.

Daarnaast bestaat er ook een regionaal netwerk, met soortgelijke partnerships die worden beheerd door het «Landesamt für Verfassungsschutz», dit is de inlichtingendiensten van de deelstaten (länders).

(1) *Une approche française de l'intelligence économique* — Christian Harbulot — november 1995.

(2) *Le Monde du Renseignement*, nr. 375, 3 februari 2000.

Delhi, à Pékin, à Djakarta, à Tokyo, à Manille, à Séoul et à Taiwan. Le BND a mis en place une banque de donnée pour les entreprises qui s'implantent dans ces régions du monde(1).

Le BND rédige des rapports à l'intention du ministère fédéral de l'Économie, notamment pour inviter les industriels allemands à la vigilance dans leurs relations avec certains pays cherchant à acquérir des systèmes de haute technologie.

Il existe aussi un organisme fédéral chargé de coordonner les initiatives dans le domaine de l'intelligence économique: l'«Arbeitsgemeinschaft für die Sicherheit des Wirtschafts» (ASW). Cet organisme entretient des contacts avec le service fédéral de renseignement, le «Bundesampt für Verfassungsschutz» (l'office de protection de la Constitution ou BfV). Selon un rapport du BfV de 1997, 62% des affaires d'espionnage mises à jour en Allemagne concernent le potentiel scientifique et économique du pays, 19% concernent des affaires politiques et administratives, 8% se situent dans le domaine militaire et 11% dans d'autres secteurs.

Des activités d'espionnage commanditées par des services de renseignement russes à l'encontre d'entreprises privées allemandes seraient en nette augmentation. Le rapport annuel du BfV de 1999 confirme que les activités du service de renseignement extérieur russe, le SVR, ainsi que des pays de la CEI sont principalement orientées vers l'espionnage économique, scientifique et technique.

Dans un entretien accordé au mensuel français *Le Monde du Renseignement*(2), M. Peter Frisch, le chef du BfV déclare que la notion de «patrimoine économique stratégique» a conduit une partie des 2 218 agents du BfV à choisir certaines entreprises afin de développer des collaborations avec elles.

À ce jour, elles sont 1 600 à avoir établi des partenariats avec le BfV au niveau fédéral. Dans chacune d'elles, un salarié assure des fonctions de délégué à la sûreté économique et de correspondant pour le service de renseignement.

Les sociétés concernées appartiennent, non seulement à l'industrie de l'armement, mais aussi à la construction automobile, à la pétrochimie et aux secteurs des hautes technologies.

Ce dispositif est doublé par un réseau régional, avec de semblables partenariats gérés par les «Landesamt fûr Verfassungsschutz», c'est-à-dire les services de renseignement des länders.

(1) Une approche française de l'intelligence économique — Christian Harbulot — novembre 1995.

(2) *Le Monde du Renseignement* nº 375, 3 février 2000.

6.7. Groot-Brittannië

De Britse wetgeving kent zowel aan de *Security Service* (act van 1989) als aan de *Secret Intelligence Service* (act van 1994) een opdracht toe inzake de bescherming van het belang van het economisch welzijn van het Verenigd Koninkrijk (1).

Geen van beide wetten bevat een definitie van het begrip «economisch welzijn» (*economic well-being*). Krachtens de wet is het «Government Communications Head Quarter» (GCHQ) belast met het intercepteren van buitenlandse communicatie voor rekening van de regering, met name «*(...) in the interest of the economic well-being of the United Kingdom ... in relation to the actions or intentions of persons outside the British Islands*».

Economische en commerciële doelwitten kunnen worden aangewezen door het «Overseas Economic Intelligence Committee» van de regering, door de economische sectie van het «Joint Intelligence Committee» en zelfs door het ministerie van Financiën en de Bank van Engeland.

De bevoegde ministers moeten bepalen welke bedrijven een sleutelpositie bekleden in de Britse economie. Ze geven hun instructies via het «Joint Intelligence Committee» (JIC).

Zo kunnen ze de inlichtingendiensten de opdracht geven na te gaan hoe de olieprijzen zullen evolueren. Vervolgens kan de bevoegde minister zijn financieel beleid aanpassen.

De inlichtingendiensten werken dus voor de Staat, aan dewelke ze inlichtingen bezorgen, niet voor de bedrijven.

Na overleg met de ministers en de bedrijven geeft het JIC richtlijnen aan de inlichtingendiensten.

De bestaande relaties tussen de inlichtingendiensten en de ondernemingen zijn menselijke relaties, zonder enige structuur als ondersteuning.

6.8. Nederland

Tot voor kort bestond er in Nederland een externe inlichtingendienst, de Inlichtingendienst Buitenland (IDB), die in 1994 werd ontbonden.

Volgens Bob de Graaf en Cees Wiebes, auteurs van een boek met de titel «Villa Maarheeze» (2), had de IDB een economische sectie die belast was met de opdracht inlichtingen in te winnen voor het ministerie

(1) *Cf. Studie van de Britse wetgeving betreffende de inlichtingen- en veiligheidsdiensten*, jaarverslag van het Comité I 1998.

(2) Geschiedenis van de inlichtingendienst buitenland - Sdu Uitgeverij, Den Haag, 1999.

6.7. La Grande-Bretagne

La législation anglaise assigne une mission de protection de l'intérêt du bien-être économique du Royaume-Uni tant pour le «Security Service» (act 1989) que pour «The Secret Intelligence Service» (act 1994) (1).

Aucune des deux lois ne définit le concept de bien-être économique *(economic well being).* Le «Government Communications Head Quarter» (GCHQ) est spécialement chargé par la loi d'intercepter des communications étrangères pour le compte du gouvernement, notamment *«... in the interest of the economic well-being of the United Kingdom ... in relation to the actions or intentions of persons outside the British Islands».*

Des cibles économiques et commerciales peuvent être désignées par le «Overseas Economic Intelligence Committe» du gouvernement, par la section économique du «Joint Intelligence Committee» et même par le Trésor et la Banque d'Angleterre.

Les ministres concernés doivent désigner les entreprises clés pour l'économie britannique. Ils donnent des directives par le canal du «Joint Intelligence Committee» (JIC).

Ils demandent, par exemple, aux services de renseignement de s'informer sur la manière dont le prix du pétrole va varier de manière à permettre au ministre d'adapter sa politique financière.

Les services de renseignement travaillent donc pour l'État, à qui ils diffusent les informations, et non aux entreprises.

Le JIC donne des directives aux services de renseignement après discussion avec les ministres et consultation des entreprises.

Les relations qui existent entre les services de renseignement et les entreprises sont des relations humaines sans structure comme support.

6.8. Les Pays-Bas

Jusqu'il y a peu, les Pays-Bas ont disposé d'un service de renseignements extérieurs, de inlichtingendienst buitenland (IDB), dissout en 1994.

Selon Bob de Graaf et Cees Wiebes, auteurs d'un ouvrage intitulé «Villa Maarheeze» (2), l'IDB possédait une section économique chargée de collecter des renseignements en faveur du ministère des Affaires

(1) *Cf. «Étude de la législation du Royaume-Uni relative aux services de renseignement et de sécurité»*, rapport annuel d'activités du Comité R 1998.

(2) Geschiedenis van de inlichtingendienst buitenland - Sdu uitgeverij, Den Haag - 1999.

van Economische Zaken, Landbouw en Visserij. De inlichtingen werden in hoofdzaak ingewonnen via Nederlandse zakenlieden die in het buitenland op reis waren of er gedurende bepaalde tijd verbleven. De IDB onderhield ook contacten met de directie van grote Nederlandse ondernemingen en wisselde daarmee belangrijke economische «intelligence» uit.

Volgens de Graaf en Wiebes zou de IDB buitenlandse commerciële offertes, verzonden via telecommunicatie, hebben geïntercepteerd en vervolgens aan Nederlandse bedrijven hebben doorgespeeld.

Na de ontbinding van de IDB werden zijn taken overgenomen door de Binnenlandse Veiligheidsdienst (BVD, Nederlandse tegenhanger van de Veiligheid van de Staat). De wettelijke opdrachten van deze dienst werden als volgt vastgelegd:

— inlichtingen verzamelen over organisaties en personen waarvan men, gelet op hun doelstellingen of hun activiteiten, op ernstige wijze mag aannemen dat ze een gevaar vormen voor de democratie, de veiligheid of voor andere essentiële belangen van de Staat;

— veiligheidsonderzoeken uitvoeren;

— bevorderen van maatregelen tot bescherming van gegevens waarvan de vertrouwelijkheid noodzakelijk is in het belang van de Staat, de overheidssectoren en de bedrijfswereld, en die volgens de bevoegde ministers van wezenlijk belang zijn voor het behoud van het maatschappelijk leven.

De bescherming van de nationale economie is vervat in deze ruime definitie van de opdrachten. Binnen dit kader voert de BVD onderzoek naar de activiteiten van buitenlandse inlichtingendiensten die gericht zijn tegen de economische belangen van Nederland. Sinds zijn ontstaan is de BVD belast met een veiligheidsopdracht, i.h.b. ten overstaan van bedrijven die voor het leger werken, alsook van bedrijven die het slachtoffer kunnen zijn van sabotage. De Nederlandse wet op de inlichtingendiensten verleent aan de BVD de toelating om ondernemingen attent te maken op de te nemen beschermingsmaatregelen. Voorts mag deze dienst bepaalde vormen van onwettige concurrentie signaleren. In 1994 werd de opdracht van de BVD op economisch vlak opnieuw gedefinieerd (zie hierna) door een groep «Economische Veiligheidsbelangen», die het ministerie van Economische Zaken en vertegenwoordigers van de bedrijven samenbrengt:

1. De bedrijven beschikken over een brede waaier van informatie die het doelwit is van economische spionage.

2. Nederlandse bedrijven lopen bepaalde opdrachten mis, omdat hun buitenlandse concurrenten vrij oneerlijke methodes toepassen, zoals het afluisteren van communicatie of het gebruiken van informanten om die opdrachten binnen te halen.

économiques, de l'Agriculture et de la Pêche. Le recueil du renseignement s'effectuait principalement via des hommes d'affaires néerlandais voyageant ou séjournant à l'étranger. L'IDB entretenait aussi des contacts avec la direction des grandes entreprises hollandaises avec lesquelles il échangeait des informations d'ordre économique de première importance.

Selon de Graaf et Wiebes, l'IDB aurait intercepté des offres commerciales étrangères transmises par télécommunications pour les communiquer à des entreprises nationales.

Après la dissolution de l'IDB, ses opérations ont été transférées au *Binnenlandse Veiligheidsdienst* (BVD, homologue néerlandais de la Sûreté de l'État), dont les missions légales ont été définies comme suit:

— collecter des renseignements sur des organisations et personnes qui, par les buts qu'elles se fixent ou par leurs activités, permettent de supposer sérieusement qu'elles représentent un danger pour la démocratie, la sécurité ou pour d'autres intérêts vitaux de l'État;

— exécuter des enquêtes de sécurité;

— favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'État, des secteurs des pouvoirs publics et du monde économique et qui sont de l'avis des ministres compétents, d'un intérêt vital pour le maintien de la vie en société.

Cette définition large des missions inclut la protection de l'économie nationale. Dans ce cadre, le BVD enquête sur les activités des services de renseignement étrangers dirigées contre les intérêts économiques des Pays-bas. Dès sa création le BVD a rempli une mission de sécurité, particulièrement à l'égard des entreprises travaillant pour l'armée et de celles qui pourraient être victimes de sabotage. La loi hollandaise sur les services de renseignement autorise le BVD à attirer l'attention des entreprises sur les mesures de protection à prendre. Ce service peut également signaler certaines formes de concurrence illicite. En 1994, la mission du BVD relative au domaine économique a été redéfinie comme suit par un groupe «Economische Veiligheidsbelangen» (Intérêts de sécurité économique) associant le ministère des Affaires économiques et des représentants d'entreprises:

1. Les entreprises disposent d'un éventail important d'informations qui sont la proie de l'espionnage économique.

2. des marchés ne sont pas obtenus par les firmes néerlandaises car les concurrents étrangers de ces firmes utilisent des moyens peu avouables tels que des écoutes ou des informateurs pour gagner ces marchés.

3. Het is absoluut noodzakelijk onderzoeken te voeren naar de betrouwbaarheid van ondernemingen en beleggers die relaties onderhouden met de georganiseerde misdaad.

Bijgevolg werd beslist dat de BVD zijn activiteiten vooral op deze drie specifieke bedreigingen zou richten.

Voorts houdt de BVD zich ook bezig met de hierna beschreven bedreigingen:

— het inwinnen door buitenlandse inlichtingendiensten van essentiële economische gegevens betreffende Nederlandse bedrijven;

— het lanceren van lastercampagnes in de pers om Nederlandse bedrijven in diskrediet te brengen.

De minister van Binnenlandse Zaken heeft een vertrouwelijke lijst opgesteld van bedrijven die voor Nederland van wezenlijk belang zijn en die de BVD moet beschermen.

We kunnen dus besluiten dat Nederland een louter defensief beleid lijkt te voeren, waarbij de bedrijfswereld en de politieke wereld niettemin nauw samenwerken.

6.9. Rusland en de landen van het Gemenebest van Onafhankelijke Staten

In april 1994 hield Boris Jeltsin, president van de Russische Federatie, een toespraak tot de verantwoordelijken en de medewerkers van de externe inlichtingendiensten van zijn land (SVR en GRU). Het volgende uittreksel laat geen twijfel bestaan over de opdrachten van deze diensten:

«We verwachten dat de externe inlichtingendiensten informatie bezorgen die de Staat absoluut nodig heeft om belangrijke beslissingen te nemen inzake het buitenlands en binnenlands beleid van Rusland, het bepalen van onze koers op economisch gebied en op het gebied van wetenschappelijke en technische vooruitgang.»

In het jaarverslag 1999 van de Duitse inlichtingendienst «Bundesamt für Verfassungsschutz» (BfV) vinden we enige informatie over de activiteiten inzake economische en wetenschappelijke inlichtingen van de Russische, Oekraïense en Wit-Russische inlichtingendiensten.

Volgens dit verslag is het verzamelen van economische, wetenschappelijke en technische inlichtingen momenteel de grootste prioriteit van deze diensten.

De Russische externe inlichtingendienst (SVR) heeft ongeveer 15 000 personen in dienst. Volgens zijn woordvoerder is deze dienst belast met de opdracht in het buitenland gunstige voorwaarden te creëren voor

3. Il est indispensable de mener des enquêtes sur la fiabilité d'entreprises et d'investisseurs qui entretiennent des rapports avec le crime organisé.

Il a donc été décidé que les activités du BVD devaient porter sur ces trois menaces spécifiques.

Le BVD s'occupe aussi de menaces telles que:

— le recueil par des services de renseignement étrangers de données économiques essentielles concernant des firmes néerlandaises;

— le lancement de campagnes de presse calomnieuses dans le but de discréditer des entreprises néerlandaises.

Le ministre de l'Intérieur a établi une liste confidentielle des entreprises présentant un intérêt vital pour les Pays-Bas et dont le BVD doit assurer la protection.

Les Pays-Bas semblent donc avoir adopté une politique purement défensive mais qui associe de manière active le monde économique et le monde politique.

6.9. La Russie et les pays de la Communauté des États Indépendants.

En avril 1994, le président de la Fédération de Russie, M. Boris Eltsine a tenu un discours à l'intention des responsables et des collaborateurs des services de renseignement extérieur de son pays (SVR et GRU) dont l'extrait suivant est très clair au niveau des objectifs qui leur étaient assignés:

«Ce que nous attendons du Renseignement extérieur, ce sont des informations indispensables à l'adoption par l'État de décisions capitales touchant à la politique étrangère et intérieure de la Russie, à la mise en oeuvre de nos orientations économiques et du progrès scientifique et technique.»

Le rapport d'activités du service de renseignement allemand «Bundesamt für verfassungsschutz» (BfV) pour l'année 1999 donne quelques informations sur les activités de renseignement économique et scientifique auxquelles se livrent les services de renseignement russes, ukrainiens et bellarusses.

Selon ce rapport, la collecte de renseignements d'ordre économique, scientifique et technique occupe à présent la première place dans les priorités de ces services.

Le SVR, service de renseignement extérieur russe, occupe environ 15 000 personnes. Selon son attaché de presse, ce service a reçu pour mission de créer à l'étranger des conditions favorables pour les intérêts

Ruslands economische belangen, teneinde buitenlandse investeerders ervan te overtuigen naar Rusland te komen.

Bij het verzamelen van informatie gebruiken de Russische inlichtingendiensten open bronnen, maar ook clandestiene personele en technische middelen, zoals het intercepteren van communicatie.

Op het gebied van open bronnen maken ze gebruik van de literatuur, van bibliotheken, databanken, het internet, ze bezoeken handelsbeurzen, nemen deel aan colloquia en conferenties en proberen er interessante contacten te leggen.

Op het gebied van het clandestien verzamelen van inlichtingen, doen de Russische diensten een beroep op inlichtingenofficieren die ze onder een dekmantel naar hun ambassades en consulaten sturen, naar persagentschappen, naar overheidsbedrijven of naar ondernemingen waar het grootste deel van het kapitaal in handen is van Russische staatsburgers.

Nog steeds volgens het BfV houdt de interne inlichtingendienst (FSB) binnen de landsgrenzen de leden van buitenlandse ambassades en consulaten in het oog, alsook zakenlieden die naar Rusland komen en de kaderleden en het personeel van buitenlandse ondernemingen die in Rusland zijn gevestigd.

6.10. Andere landen (kort)

De Volksrepubliek China: de Chinese academie voor wetenschappen kent jaarlijks beurzen toe aan een groot aantal buitenlandse universiteitsprofessoren, directeuren van laboratoria en onderzoeksleiders, opdat zij zouden meewerken aan Chinese onderzoeksprogramma's. (*Bron*: «Le Monde du Renseignement» nr. 338, 2 juli 1998).

De sectie inlichtingen en economische en financiële contraspionage van het Chinese ministerie van Veiligheid («Guoanbu») heeft de opdracht gekregen te voorkomen dat buitenlanders in het bezit komen van economische «intelligence» die de overheid niet voorafgaandelijk heeft geselecteerd. Deze selectie wordt gezamenlijk verricht door Guoanbu, het ministerie van Buitenlandse Handel en Economische Samenwerking en het departement Propaganda van het Centraal Comité van de Chinese communistische partij. (*Bron*: «Le Monde du Renseignement» nr. 304, 30 januari 1997).

Ook Taiwan wordt beschouwd als een van de meest doeltreffende landen op het vlak van economische inlichtingen. (*Bron*: «Le Monde du Renseignement» nr. 356, 8 april 1999).

Zweden: sinds het begin van de 20ste eeuw zijn diverse Zweedse ondernemingen in alle discretie actief op het gebied van economische inlichtingen. Dit kan een verklaring zijn voor hun commerciële successen overal ter wereld. De universiteit van Lund heeft zich ter zake gespecialiseerd.

économiques russes en vue d'attirer des investisseurs étrangers vers ce pays.

Pour collecter leurs informations, les services de renseignement russes font usage aussi bien de sources ouvertes, que de moyens humains et techniques clandestins, tels que l'interception des communications.

Comme sources ouvertes, ils utilisent la littérature, les bibliothèques, les banques de données, l'internet, ils visitent des foires et missions commerciales, ils fréquentent des colloques et conférences et essayent d'y nouer des contacts intéressants.

Pour le recueil clandestin de renseignements, les services russes utilisent des officiers de renseignements envoyés sous couverture dans leurs ambassades et consulats, dans des agences de presse, dans des firmes d'État ou dont la majorité du capital est détenue pas des citoyens russes.

Toujours selon le BfV, le FSB (le service de renseignement intérieur) surveille à l'intérieur du pays les membres des ambassades et des postes consulaires étrangers, les hommes et femmes d'affaires venus en visite en Russie ainsi que les cadres et le personnel des firmes étrangères établies dans ce pays.

6.10. Autres pays (en bref).

La Chine populaire: l'académie des sciences chinoise offre chaque année des bourses à de nombreux professeurs d'universités, responsables de laboratoires et chefs de recherches de pays étrangers pour qu'ils s'associent à des plans de recherches chinois. (*Source*: «Le Monde du Renseignement» nº 338, 2 juillet 1998).

La section renseignement et contre-espionnage économique et financier du ministère de la sécurité chinoise (« Guoanbu «) a notamment reçu pour mission d'empêcher les étrangers de se procurer l'information économique qui n'a pas été préalablement triée par les autorités. Ce tri est effectué conjointement par le Guoanbu, le ministère du commerce extérieur et de la coopération économique et le département de propagande du Comité central du parti communiste chinois. (*Source*: LMR nº 304, 30 janvier 1997).

La Chine nationaliste est elle aussi considérée comme l'un des pays les plus efficaces en renseignement économique. (*Source*: LMR nº 356, 8 avril 1999).

La Suède: plusieurs entreprises suédoises pratiquent l'intelligence économique en toute discrétion depuis le début du siècle. Ceci peut expliquer leurs succès commerciaux dans le monde. L'université de Lund s'est spécialisée dans cette matière.

Israël : de Franse inlichtingendiensten zijn beducht voor de commerciële efficiëntie van Israëlische bedrijven die in Parijs zijn gevestigd en actief zijn op het gebied van economische inlichtingen of computerveiligheid. Onder de kaderleden van sommige van deze bedrijven vinden we voormalige leden van de Mossad (*Bron* : « Le Monde du Renseignement » nr. 392, 26 oktober 2000).

7. Commerciële vennootschappen gespecialiseerd in economische inlichtingen

7.1. Algemeen

Steeds meer private vennootschappen specialiseren zich, ten behoeve van grote industriële groepen (onder andere in de wapensector), in economische inlichtingen en financieel onderzoek. Sommige van die vennootschappen voeren echte veiligheidsonderzoeken voor rekening van hun klanten wanneer zij bepaalde personen willen rekruteren.

Ze voeren ook financiële onderzoeken wanneer hun klanten vermoedens hebben van fraude, verduistering, vijandelijke overnames, enzovoort. Vaak worden deze vennootschappen opgericht door exleden van politie- of inlichtingendiensten, die zich gaan specialiseren op het gebied van economische inlichtingen. In de Verenigde Staten hebben de NSA en de CIA een deel van hun personeel aangemoedigd zich om te scholen en in de privé-sector te gaan werken.

Er bestaat een « Annuaire Européen des Professionnels de l'Intelligence Economique », die wordt gepubliceerd door de « Société d'Intelligence Economique et Concurrentielle Appliquée » (SIECA). Deze publicatie streeft ernaar volledig te zijn, maar sommige ondernemingen weigeren erin te worden opgenomen.

We onderscheiden zeven categorieën van prestaties die verband houden met economische inlichtingen :

— privé-detectives;

— commerciële inlichtingen;

— auditbureaus;

— technologische bewakingsbureaus;

— bedrijven actief op het gebied van economische inlichtingen;

— tussenpersonen;

— lobbying.

Deze wereld van economische inlichtingenbureaus en -bedrijven is echter heel uiteenlopend en evolueert constant. We moeten ons er dan ook voor hoeden een al te formele definitie te geven van die organisaties. Immers, private onderzoeks- en veiligheidsondernemingen ondergaan dezelfde ontwikkeling als de grote auditbureaus.

Israël : les services de renseignement français redoutent l'efficacité commerciale des entreprises israéliennes d'intelligence économique ou de sécurité informatique implantées à Paris. Certaines de ces sociétés comptent parmi leurs cadres des anciens membres du Mossad (LMR nº 392, 26 octobre 2000).

7. Les sociétés commerciales spécialisées en intelligence économique

7.1. Généralités

De plus en plus nombreuses sont aussi les sociétés privées qui se spécialisent au profit de grands groupes industriels, (notamment de l'armement) dans l'intelligence économique ou dans l'investigation financière. Certaines d'entre elles procèdent pour le compte de leurs clients à de véritables enquêtes de sécurité préalables à l'embauche de personnes.

Elles peuvent aussi procéder à des enquêtes financières en cas de soupçons de fraudes, de détournements, d'OPA inamicale, etc. Les animateurs de ces sociétés ont, eux aussi, souvent appartenu à des services de police ou de renseignement avant de se reconvertir dans le renseignement économique. Aux États-Unis, la NSA et la CIA ont en effet encouragé la reconversion d'une partie de leur personnel vers le secteur privé.

Il existe un « Annuaire Européen des Professionnels de l'Intelligence Economique » édité par la « Société d'Intelligence Economique et Concurrentielle Appliquée » (SIECA). Ce manuel se veut exhaustif mais certaines sociétés ont néanmoins refusé d'y figurer.

On peut distinguer sept catégories de prestations en rapport avec l'intelligence économique :

— les détectives privés;

— le renseignement commercial;

— les cabinets d'audit

— les cabinets de veille technologique;

— les sociétés d'intelligence économique;

— les intermédiaires;

— le lobbying.

Néanmoins, ce monde des sociétés et cabinets d'intelligence économique est fort disparate et en constante évolution. Il convient donc d'éviter de donner aux sociétés ainsi désignées une définition trop formelle.

Ze breiden hun dienstengamma voortdurend uit, overschrijden de grenzen van hun vroegere activiteiten en voeren talrijke fusies, overnames of splitsingen uit. De grote groepen die zich vandaag duidelijk profileren, zijn vooral Amerikaans.

We noemen er een paar:

— Pinkerton, deel van de Zweedse groep Securitas AB,

— Kroll Associates, dat zich onlangs losmaakte van O'Gara en werd overgenomen door Blackstone Capital Partners III (BCPIII),

— Decision Strategy Fairfax Group (DSFX),

— de Britse firma Control Risks Group (CRG).

De meeste van deze firma's hebben een zetel in Europa (Parijs, Londen, enz.). De firma *Control Risks Group* heeft een kantoor in Antwerpen.

Sommige firma's stellen rapporten inzake risicoanalyse op, met heel specifieke informatie voor industriëlen die in het buitenland wensen te investeren. Die rapporten hebben betrekking op de politieke, sociale en economische toestand in de betrokken landen, op de belangen van rivaliserende groepen, terroristische bedreigingen, corruptiepraktijken, de invloed van criminele organisaties of van drukkingsgroepen.

In zijn rapport «2000 Outlook» buigt de firma «Control Risks Group» zich over de protestbewegingen tegen de globalisering, uitgaand van de veronderstelling dat een van die bewegingen op een dag zou kunnen overgaan tot gewelddadige acties tegen multinationals. Het rapport noemt zelfs mogelijke doelwitten en data waarop activisten tot actie zouden kunnen overgaan.

Andere bedrijven bieden diensten aan die gericht zijn op het identificeren en observeren van de auteurs van lastercampagnes op het internet, een nieuwe vorm van activisme die soms gericht is tegen industrieën of bepaalde activiteitensectoren. Een van die bedrijven, gevestigd in de USA, heeft zich uitgeroepen tot «the premier internet intelligence agency». Ze werken met onderzoekssoftware op het internet, waarbij ze een bezoek brengen aan «newsgroups» en aan sommige websites.

Een Franse firma, «Net Intelligenz», bewaakt, bestudeert en analyseert voor rekening van zijn klanten alle forums en gesprekken tussen internauten. Dankzij zijn bijzonder krachtige software kan deze firma, net als een zoekmotor, alle virtuele ontmoetingsplaatsen analyseren om er bepaalde sleutelwoorden of -uitdrukkingen terug te vinden. Deze enorme massa gegevens wordt verwerkt door wetenschappers, sociologen en semiologen die op verzoek van de klant een specifieke analyse verrichten.

Les sociétés privées d'investigation et de sécurité suivent en effet les mêmes évolutions que les grands cabinets d'audit. Elles élargissent leurs gamme de services, s'affranchissent des limites de leur métier d'origine et opèrent de multiples fusions, acquisitions ou séparations. Les groupes majeurs qui semblent se dessiner aujourd'hui sont pour la plupart américains.

On peut notamment citer:

— Pinkerton, détenu par le groupe suédois Securitas AB,

— Kroll Associates, qui s?est récemment séparé de O?Gara, et qui a été repris par Blackstone Capital Partners III (BCPIII),

— Decision Strategy Fairfax Group (DSFX),

— La firme britannique Control Risks Group (CRG).

La plupart de ces firmes ont leur siège en Europe (Paris, Londres, etc.). La firme *Control Risks Group* dispose d'une agence à Anvers.

Certaines firmes éditent des rapports d'analyse de risques contenant des informations pointues et précises pour les industriels qui désirent investir à l'étranger. Il s'agit de rapports portant sur la situation politique, sociale et économique des pays visés, sur les intérêts des groupes rivaux, sur les menaces terroristes, les pratiques de corruption, sur l'influence des groupes criminels ou celle des groupes de pression.

Ainsi, par exemple, le rapport «2000 Outlook» de la firme «Control Risks Group» se penche sur les mouvements de protestation contre la mondialisation, avec l'hypothèse que l'un d'eux pourrait basculer un jour dans l'action violente contre les multinationales. Ce rapport indique même des cibles potentielles ainsi que des dates auxquelles des activistes pourraient entrer en action.

Il existe également des sociétés qui offrent sur le marché des services destinés à identifier et à suivre tous les auteurs de campagnes de dénigrement sur l'internet, cette nouvelle forme d'activisme dirigée quelquefois contre des industries ou certains secteurs d'activités. L'une de ces sociétés, établie aux USA, s'est proclamée «the premier internet intelligence agency». Leurs prestations se basent sur des logiciels de recherche sur l'internet, effectuant des passages dans les «newsgroups» et sur certains sites.

Ainsi, une firme française «Net Intelligenz» surveille, étudie et analyse tous les forums et conversations entre internautes pour le compte de ses clients. Grâce à un logiciel très puissant, l'agence peut, tel un moteur de recherche, analyser l'ensemble des lieux de conversation virtuels pour y dénicher des mots ou des expressions-clés. Cette masse de données est traitée par des scientifiques, sociologues, sémiologues qui en font une analyse ciblée selon la demande du client.

Voorts zien we in het organigram van sommige multinationals, in het bijzonder in de voedingsmiddelenindustrie, in de energiesectoren (de oliesector, de nucleaire sector enz.), bij luchtvaartmaatschappijen enz., dat « war rooms » worden opgericht, d.i. speciale cellen waar belangrijke beslissingen worden genomen. Deze cellen krijgen de opdracht crisissen te beheren, gepast te reageren op de gevolgen van industriële ongevallen die steeds vaker voorkomen, aanvallen van concurrenten te counteren, alsook de strategische informatie van de onderneming te beheersen en nieuwe markten te gaan veroveren. Sommige van deze « war rooms » worden geleid door voormalige leden van politie- of inlichtingendiensten.

Tot slot ontstaat in de Verenigde Staten en Groot-Brittannië een nieuwe vorm van bewaking van het personeel op de werkvloer.

Grote bedrijven richten er teams van informaticainspecteurs op, die de opdracht krijgen de harde schijven van de werknemers, zonder hun medeweten, te kopiëren en grondig te onderzoeken om eventuele op het werk begane fouten op te sporen, of computerbewijzen te vinden betreffende de diefstal van bedrijfsgeheimen. Deze specialisten gebruiken informaticamiddelen en -technieken die oorspronkelijk werden ontworpen voor politie- en inlichtingendiensten.

Zowel in de Verenigde Staten als in Groot-Brittannië laat de wetgeving de werkgevers toe gebruik te maken van deze « legale computergeneeskunde », om redenen van de noodzaak zich te verweren.

7.2. De nood aan een juridisch debat en aan toezicht op de activiteiten van private inlichtingenbedrijven

In haar veiligheidsplan (1) stelt de federale regering vast dat er een tendens bestaat om steeds vaker een beroep te doen op private veiligheidsactoren (bewakingsondernemingen, interne bewakingsdiensten, beveiligingsondernemingen, privé-detectives enz.). Op sommige heel concrete gebieden van de veiligheid is er zelfs sprake van samenwerking en overleg tussen private actoren en de overheid.

Sommige aspecten van de activiteiten van economische inlichtingenbedrijven worden geregeld door de wet van 19 juli 1991 tot regeling van het beroep van privé-détective (deze wet beoogt met name het inwinnen door natuurlijke personen van informatie omtrent burgerlijke stand, gedrag, moraliteit en vermogenstoestand van personen, alsook het opsporen van bedrijfsspionage). Hoe staat het echter met, bijvoorbeeld, de systematische exploitatie van databanken? Er bestaat ook een wet van 10 april 1990 op de bewa-

(1) Senaat nr. 2-461/1 en Kamer van volksvertegenwoordigers (doc. 50 0716/001) — 13 juni 2000.

On voit aussi apparaître dans l'organigramme de certaines entreprises multinationales, notamment chez les industriels de l'agro-alimentaire, des secteurs énergétiques (pétrole, nucléaire, etc.), des compagnies aériennes, etc., des cellules de décisions appelées « war rooms ». Celles-ci sont chargées de gérer les crises, de répondre aux conséquences d'accidents industriels de plus en plus fréquents, de contrer les attaques de la concurrence, mais aussi de maîtriser l'information à caractère stratégique de l'entreprise et de s'attaquer à la conquête de nouveaux marchés. Certaines de ces « war rooms » sont animées par d'anciens membres de services de police ou de renseignement.

Une nouvelle forme de surveillance du personnel sur les lieux de travail apparaît enfin aux États-Unis et en Grande Bretagne.

L'on y voit en effet des grandes firmes mettre en place des équipes d'enquêteurs informatiques chargés de copier les disques durs des salariés, à leur insu, et de les passer au crible pour trouver, soit d'éventuelles fautes commises au travail, soit des preuves informatiques de vols de secrets industriels. Ces spécialistes se servent d'outils informatiques et de techniques conçus à l'origine pour l'usage des services de police ou de renseignement.

Les législations américaines et britannique permettent aux employeurs de recourir à cette « médecine légale informatique » qu'ils justifient par la nécessité de se défendre.

7.2. La nécessité d'un débat juridique et d'un contrôle sur l'activité des sociétés de renseignement privé

Dans son plan de sécurité (1), le gouvernement fédéral constate la tendance à de plus en plus faire appel à des acteurs privés dans le domaine de la sécurité (entreprises et services internes de gardiennage, de sécurité, détectives privés, etc.). Dans certains domaines de sécurité très concrets, il existe même une coopération et une concertation entre les acteurs privés et les autorités.

Si certains pans de l'activité des firmes de renseignement économique sont régis par la loi du 19 juillet 1991 organisant la profession de détective privé (cette loi vise notamment le recueil par des personnes physiques d'informations relatives à l'état civil, à la conduite, à la moralité et à la solvabilité de personnes, ainsi que la recherche d'activités d'espionnage industriel), qu'en est-il par exemple de l'exploitation systématique de banques de données? Il existe aussi une loi du 10 avril 1990 sur les entreprises de gardiennage et

(1) Sénat nº 2-461/1 et Chambre des représentants (doc 50 0716/001) — 13 juin 2000.

kings- en de beveiligingsondernemingen, maar ze betreft alleen hun activiteiten inzake de bewaking en fysieke bescherming van goederen en van personen.

De nood aan een juridisch debat en aan toezicht op de wettelijkheid van de inlichtingenactiviteiten van private bedrijven neemt voortdurend toe naarmate deze bedrijven hun aanbiedingen inzake economische inlichtingen vermenigvuldigen. Zelfs de exploitatie van de open bronnen, dit wil zeggen van informatie die toegankelijk is voor het grote publiek, sluit niet uit dat bepaalde rechtsregels moeten worden nageleefd(1).

Het federaal veiligheidsplan bepaalt: «Om de democratische controle op de private veiligheidsactoren te realiseren, is het opportuun te onderzoeken of de Vaste Comités van toezicht op de politiediensten en de inlichtingendiensten binnen hun wettelijke taak hiertoe kunnen bijdragen.»

Het Comité I is inderdaad van mening dat de overheid absoluut toezicht moet uitoefenen op de economische inlichtingenactiviteiten van private bedrijven. Volgens het Comité behoort deze controleopdracht in eerste aanleg tot de bevoegdheid van de diensten van de federale regering. De controle behoort ten dele tot de opdracht inzake de bescherming van het economisch en wetenschappelijk potentieel waarmee de Veiligheid van de Staat is belast.

Indien het Parlement het voornemen zou hebben het Comité I bij deze nieuwe opdracht te betrekken, zou dit een aanpassing vereisen van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, aangezien het Comité krachtens deze wet geen enkele bevoegdheid geniet om rechtstreeks toezicht uit te oefenen op de activiteiten van economische inlichtingenbedrijven.

8. De rol van de Belgische inlichtingendiensten inzake de bescherming van het wetenschappelijk en economisch potentieel: vaststellingen van het Comité I

8.1. Verwachtingen en voorstellen van de Belgische economische wereld

In 1986, kort na de aanslagen van de CCC, werd binnen het Verbond van Belgische ondernemingen

(1) Recent nog meende Commissie voor de bescherming van de persoonlijke levenssfeer dat de verwerking van persoonsgegevens, afkomstig van het raadplegen en systematisch exploiteren van jurisprudentiële informatie verspreid met behulp van elektronische middelen, onder de wet valt. «De mogelijkheid om, via gecentraliseerde, ja zelfs exhaustieve rechtspraakdatabanken, iemands gerechtelijk verleden terug te vinden, brengt voor de gegevensbescherming risico's met zich mee die veel groter zijn dan die verbonden aan de traditionele toegangswijzen of publicaties van rechtspraak» (beslissing nr. RZ97CN3-1 van 23 december 1997).

de sécurité, mais elle ne vise que leurs activités de surveillance et de protection physique des biens et des personnes.

La nécessité d'un débat juridique et d'un contrôle sur la légalité des activités privées d'intelligence se fait donc plus pressante à mesure que les offres de renseignement économique privé se multiplient. Même l'exploitation des sources ouvertes, c'est-à-dire celle pratiquée à partir d'informations accessibles au public, n'exclut pas le respect de certaines règles de droit(1).

Comme le souligne le plan fédéral de sécurité, «afin de soumettre les acteurs privés de la sécurité à un contrôle démocratique, il convient de voir si les Comités permanents de contrôle des services de police et de renseignements peuvent apporter leur contribution en la matière dans les limites de leur mission légale».

Le Comité R estime en effet qu'un contrôle de l'autorité est indispensable sur la pratique du renseignement économique par des firmes privées. Selon le Comité, cette mission de contrôle incombe en premier ressort aux services du gouvernement fédéral. Une part de ce contrôle entre notamment dans la mission de protection du potentiel économique et scientifique confiée à la Sûreté de l'État.

S'il entrait dans les intentions du Parlement d'associer le Comité R à cette nouvelle mission, cela nécessiterait une adaptation de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, car celle-ci ne lui donne aucune compétence pour contrôler directement l'activité des sociétés de renseignement économique.

8. Le rôle des services de renseignement belges en matière de protection du potentiel scientifique et économique: constatations du Comité R

8.1. Les attentes et les propositions des milieux économiques belges

En 1986, peu après les attentats des CCC, un groupe de travail de la Fédération des entreprises de

(1) Ainsi par exemple, la Commission de la protection de la vie privée a récemment estimé que le traitement de données personnelles tirées de la consultation et de l'exploitation systématique d'informations jurisprudentielles diffusées par des moyens électroniques tombait sous le coup de la loi. «La possibilité, à partir de banques de données jurisprudentielles centralisées, voire exhaustives, de retrouver l'historique judiciaire d'une personne, engendre des risques en matière de protection des données sans commune mesure avec ceux liés aux modes traditionnels d'accès ou de publication de la jurisprudence» (décision nº JZ97CN3-1 du 23 décembre 1997).

(VBO) een werkgroep opgericht die veiligheidsrichtlijnen opstelde voor de bedrijfsleiders. In 1994 creëerden veiligheidsexperts uit diverse industriële sectoren en van ondernemingen een « Permanent Overlegplatform Bedrijfsbeveiliging ». De sectoren die hierbij het meest waren betrokken, waren de distributiesector, de voedingsindustrie, de chemische nijverheid, Fabrimetal, Sabena, Belgacom, de petroleumsector, de banken, de verzekeringsmaatschappijen, de staalsector en de tabaksindustrie.

De veiligheidsexperts uit deze sectoren hebben zich gebogen over alle aspecten inzake de bescherming van de bedrijven tegen risico's van criminele oorsprong. Er werden contacten gelegd met de diverse overheden en met hun bevoegde diensten, in het bijzonder met de Veiligheid van de Staat en de SGR. In 1995 bezorgde het « Permanent Overlegplatform Bedrijfsbeveiliging » aan deze overheden een memorandum met een beschrijving van de verwachtingen en de voorstellen van de Belgische industriële kringen inzake de beveiliging van de bedrijven. Dit document werd in juni 2000 bijgewerkt.

Economische spionage wordt er beschreven als een van de hoofdbekommernissen van het VBO, naast gewapende overvallen, gewelddadige feiten van agressie en aanslagen.

Het VBO roept op om een nieuwe dynamiek te geven aan het overleg tussen de overheid en de privésector, het pleit voor een « integraal veiligheidsbeleid » en formuleert ook een aantal voorstellen. Twee van die voorstellen hebben direct betrekking op de inlichtingendiensten :

— het oprichten, binnen het ministerie van Justitie, van een vaste structuur voor contacten met de privé-sector : « Deze structuur, samengesteld uit vertegenwoordigers van de politiediensten, de inlichtingendiensten en de magistratuur, zou het VBO regelmatig moeten informeren over de bedreigingen die op de bedrijven wegen en samenwerkingsprojecten tussen de overheid en de privé-sector moeten ontwikkelen. » Het doel bestaat erin de vormen van criminaliteit die een bedreiging vormen voor de bedrijven onafgebroken te analyseren;

— « het organiseren van cursussen en vormingscycli voor het leidend personeel van de politiediensten, de inlichtingendiensten en de magistratuur, over de organisatie van de onderneming en de vormen van criminaliteit waarvan bedrijven het slachtoffer zijn. » Het VBO is immers van mening dat het personeel van deze diensten niet voldoende expertise bezit inzake de vormen van criminaliteit waarmee bedrijven te maken krijgen; dit personeel moet dus een passende opleiding kunnen krijgen, gericht op de realiteit van de bedrijven. « Het is ook aangewezen « technici » ter beschikking te stellen van de politiediensten en/of de

Belgique (FEB) s'est mis en place pour édicter des lignes directrices de sécurité aux chefs d'entreprises. En 1994, des experts en sécurité de divers secteurs industriels et d'entreprises ont créé une « Plate-forme de concertation permanente pour la protection des entreprises » (PCPE). Les secteurs les plus concernés étaient notamment la distribution, l'alimentation, la chimie, Fabrimetal, Sabena, Belgacom, le secteur pétrolier, les banques, les assurances, le secteur sidérurgique et l'industrie du tabac.

Les experts en sécurité de ces secteurs se sont penchés sur tous les aspects de la protection des entreprises contre les risques d'origine criminelle. Des contacts ont été établis avec les autorités publiques et leurs services compétents, notamment la Sûreté de l'État et le SGR. En 1995, la PCPE a adressé à ces autorités un mémorandum exprimant les attentes et les propositions des milieux industriels belges en matière de sécurité des entreprises. Ce document a été réactualisé en juin 2000.

L'espionnage économique y apparaît comme l'une des préoccupations majeures de la FEB parmi lesquelles on trouve aussi les attaques armées, les vols, les agressions violentes et les attentats.

La FEB appelle à une redynamisation de la concertation entre pouvoirs publics et secteur privé, elle plaide pour une « gestion intégrale de la sécurité » et formule des propositions, parmi lesquelles deux concernent directement les services de renseignement :

— la création au sein du ministère de la Justice d'une structure permanente de contact avec le secteur privé : « Cette structure, composées de représentants des services de police, des services de renseignement et de la magistrature, devrait informer régulièrement la FEB, quant aux menaces pesant sur les entreprises et définir les projets de coopération entre le public et le privé. » L'objectif est ici d'analyser en permanence les formes de criminalité qui constituent une menace contre les entreprises.

— « l'organisation de cours et cycles de formation pour le personnel dirigeant des services de police, des services de renseignement et de la magistrature, consacrés à l'organisation de l'entreprise et aux formes de criminalité dont les entreprises sont victimes. » Pour la FEB, le personnel de ces services manque en effet d'expertise dans les domaines de la criminalité touchant les entreprises; il doit donc pouvoir disposer d'une formation adéquate axée sur la réalité des entreprises. « Il s'indique, par ailleurs, de mettre des « techniciens » à la disposition des services de police et/ou des parquets pour des enquêtes spécifi-

parketten voor specifieke onderzoeken betreffende het technologisch en economisch potentieel van ons land.»

In haar veiligheidsplan van juni 2000 verklaart de federale regering dat de ministers van Justitie en Binnenlandse Zaken het overleg zullen voortzetten dat binnen het «Permanent Overlegplatform Bedrijfsbeveiliging» is ontstaan. Bovendien zal een gemengde werkgroep, belast met economische criminaliteit, aandacht besteden aan de volgende vormen van criminaliteit: computercriminaliteit, witwassen van geld, corruptie en economische spionage.

8.2. De Veiligheid van de Staat

Het Comité I stelde zich de vraag hoe de Veiligheid van de Staat haar nieuwe opdracht van bescherming van het wetenschappelijk of economisch potentieel opvatte en voorbereidde.

Gaat het voor deze dienst om een actieve benadering van de economische intelligentie ten bate van de Belgische ondernemingen (technologische en concurrentiële bewaking, lobbying, uitbating van open bronnen, ...) of daartegenover, om een methode van beveiliging met sensibilisering over het fenomeen van economische spionage met inbegrip van de veiligheidsmaatregelen om er zich tegen te beschermen?

In het ene geval of het andere, welke zijn de menselijke middelen die hiervoor worden ingezet, welke zijn de werkmethodes, de relaties van de Veiligheid van de Staat met de ondernemingen, met de universiteiten, enz.?

A. Historiek van het belang dat de Veiligheid van de Staat hecht aan de bescherming van het wetenschappelijk of economisch belang

Tijdens de Koude Oorlog beperkten de Belgische inlichtingendiensten zich tot de eventuele militaire implicaties van de transfer van spitstechnologie binnen het strikte kader van de richtlijnen, voorgeschreven door het COCOM-Comité (voorbeeld: de zaak Pégard).

In 1986 beginnen de besprekingen tussen vertegenwoordigers van de Veiligheid van de Staat en de directeur-generaal van het departement Wetenschappelijk Onderzoek van het ministerie van Economische Zaken. Van deze periode dateren de eerste contacten van de Veiligheid van de Staat met het Verbond van Belgische Ondernemingen (VBO). Daarop volgde een conferentie, gegeven door leden van de Veiligheid van de Staat aan enkele tientallen industriëlen. Deze eerste inspanning tot sensibilisering blijkt evenwel geen gevolgen gekend te hebben.

Tot in 1998 kwam de bescherming van het wetenschappelijk of economisch potentieel van het land

ques visant le potentiel technologique et économique de notre pays.»

Dans son plan de sécurité de juin 2000, le gouvernement fédéral déclare que les ministres de la Justice et de l'Intérieur poursuivront la concertation mise en place au sein de la PCPE et qu'un groupe de travail mixte chargé de la criminalité économique devra prêter attention aux modes criminels suivants: criminalité informatique, blanchiment d'argent, corruption et espionnage économique.

8.2. La Sûreté de l'État

Le Comité R s'est demandé comment la Sûreté de l'État concevait et préparait sa nouvelle mission de protection du potentiel scientifique et économique.

S'agit-il pour ce service d'une approche active de l'intelligence économique au profit des entreprises belges (veille technologique, concurrentielle, lobbying, exploitation des sources ouvertes, ...) ou bien d'une démarche sécuritaire avec sensibilisation au phénomène de l'espionnage économique ainsi qu'aux mesures de sécurité pour s'en prémunir.

Dans l'un ou l'autre cas, quels sont les moyens humains affectés à cette mission, les méthodes de travail mises en œuvre, les relations de la Sûreté de l'État avec les entreprises, avec les universités, etc.?

A. Historique de l'intérêt que porte la Sûreté de l'État à la protection du potentiel scientifique et économique

Pendant la guerre froide, les services de renseignement belges se sont cantonnés aux implications militaires éventuelles du transfert de hautes technologies dans le strict respect des directives prescrites par le comité COCOM (exemple, l'affaire Pégard).

C'est en 1986 que commencent des pourparlers entre des représentants de la Sûreté de l'État et le directeur général du département de la Recherche scientifique du ministère des Affaires économiques. C'est de cette époque que datent les premiers contacts de la Sûreté de l'État avec la Fédération des Entreprises de Belgique (FEB). Une conférence a alors été donnée par des membres de la Sûreté de l'État à quelques dizaines d'industriels. Ce premier effort de sensibilisation ne semble cependant pas avoir été suivi d'effets.

Jusqu'en 1998, la protection du patrimoine scientifique et économique du pays ne figurait pas comme

niet voor op de lijst met de onderwerpen waarvoor de Veiligheid van de Staat belangstelling heeft.

Toch heeft deze dienst, in het kader van de strijd tegen de proliferatie van NBC-wapens(1), altijd inlichtingen ingewonnen en geanalyseerd om de uitvoer van materiaal of de transfer van gevoelige technologie naar landen die geacht worden «risicovol» te zijn of naar criminele of terroristische organisaties.

In dit kader nam de Veiligheid van de Staat zijn eerste contacten met handelsondernemingen, universiteiten en onderzoekscentra.

Tussen 1995 en 1997 nam de Veiligheid van de Staat deel aan de werkzaamheden van het «Permanent Overlegplatform Bedrijfsbeveiliging» dat door het VBO werd opgezet in opvolging van het memorandum over de veiligheid van ondernemingen.

Meerdere officiële overlegvergaderingen tussen de publieke overheden en de wereld van de ondernemingen hadden plaats, meerbepaald twee rondetafelgesprekken waaraan vertegenwoordigers van het VBO en de ministers van Justitie en Binnenlandse Zaken deelnamen. De procureurs-generaal, de nationale magistraten en verantwoordelijken van politie en rijkswacht namen eveneens deel aan dit overleg. Het doel van deze vergaderingen was een verbeterde informatie-uitwisseling tot stand te brengen tussen private ondernemingen en bepaalde overheidsinstanties die gelast zijn met de veiligheid. Volgend op deze vergaderingen werden briefings gegeven door de Veiligheid van de Staat aan het VBO over de werking van de diensten over de sekten.

Bij gebrek aan personeel en middelen bleven deze contacten echter sporadisch en werd geen van de genomen initiatieven volledig uitgevoerd. Sedert 1997 hadden geen officiële contacten meer plaats tussen het VBO en de overheden in het kader van het voornoemde platform. Vergaderingen in dit kader werden voortgezet, maar enkel in bijzijn van privé-experten inzake de veiligheid van ondernemingen.

Op 9 oktober 1999 publiceerde het dagblad *De Financieel Economische Tijd* een interview met de nieuwe procureur-generaal des Konings te Antwerpen, waarin hij de economische en industriële spionage aanhaalt en deze betitelt als «de vergeten oorlog». Hij meent dat men in deze materie rekening moet houden met de buitenlandse inlichtingendiensten. Op dit tijdstip hebben de buitendiensten van de Veiligheid van de Staat reeds een tiental informatierapporten opgesteld, te rekenen vanaf het begin van dat jaar.

(1) NBC-wapens: Nucleaire, Bacteriologische en Chemische wapens.

telle parmi les sujets de préoccupation de la Sûreté de l'État.

Néanmoins, dans le cadre de la lutte contre la prolifération d'armes NBC(1), ce service a toujours recueilli et analysé des renseignements en vue d'empêcher l'exportation de matériel ou le transfert de technologies sensibles à destination de pays jugés «à risques», d'organisations maffieuses ou terroristes.

C'est dans ce cadre que la Sûreté de l'État a établi ses premiers contacts avec des firmes commerciales, des universités et des centres de recherche.

Entre 1995 et 1997, la Sûreté de l'État a pris part aux travaux de la «Plate-forme permanente de concertation pour la protection des entreprises» (PCPE) mise en place par la Fédération des Entreprises de Belgique (FEB) suite au mémorandum sur la sécurité des entreprises.

Plusieurs réunions officielles de concertation entre les autorités publiques et le monde des entreprises ont eu lieu, notamment deux tables rondes mettant en présence représentants de la FEB et les ministres de la Justice et de l'Intérieur. Ont également participé à cette concertation les procureurs généraux, les magistrats nationaux, ainsi que des responsables de la police et de la gendarmerie. Le but de ces réunions était de réaliser un échange d'informations amélioré entre les entreprises privées et certaines instances officielles en charge de la sécurité. À la suite de ces réunions, des briefings ont été donnés par la Sûreté de l'État à la FEB sur le fonctionnement de ce service et concernant les sectes.

Par manque de personnel et de moyens, ces contacts sont toutefois restés sporadiques et aucune des initiatives prises n'a vraiment été menée à son terme. Depuis 1997, les contacts officiels entre FEB et autorités ont cessé au sein de la PCPE. Des réunions se sont poursuivies dans ce cadre, mais seulement en présence d'experts privés de la sécurité des entreprises.

Le 9 octobre 1999, le journal «*De Financieel Economische Tijd*» publie une interview de M. B. Van Lijsebeth, devenu procureur du Roi à Anvers, dans lequel celui-ci évoque l'espionnage économique et industriel qu'il qualifie de «guerre oubliée». Il estime qu'il faut compter en cette matière avec les services de renseignement étrangers. À cette date, les services extérieurs de la Sûreté de l'État ont déjà produit une dizaine de rapports d'information depuis le début de l'année 1999.

(1) Armes NBC = armes nucléaires, bactériologiques et chimiques.

De minister van Justitie, hierover geïnterpelleerd, ondervroeg de Veiligheid van de Staat. Deze liet hem weten dat er geen enkel concreet bewijs voorlag dat aantoonde dat buitenlandse inlichtingen- en veiligheidsdiensten op dit moment in België actief zouden zijn op het vlak van economische of industriële spionage.

Evenwel maken open bronnen gewag van de heroriëntatie van de activiteiten van de inlichtingendiensten van de militaire spionage naar economische spionage.

In 1997 en 1998 lichtte de Veiligheid van de Staat de minister van Justitie in dat de Cubaanse ambassade te Brussel universitaire informaties zocht van economische aard en dat de ambassade voor deze opdracht zelfs personeel had aangeworven (1).

Op 28 oktober 1999 kondigde de minister van Justitie aan dat een kabinetsmedewerker zou deelnemen aan het « Permanent Overlegplatform Bedrijfsbeveiliging ». Dit forum zou een samenwerkingsplan moeten uitwerken tussen het VBO en de publieke overheden. Volgens de minister kan de Veiligheid van de Staat binnen dit kader een pro-actieve rol spelen.

B. De door de Veiligheid van de Staat ondernomen acties

De acties voorafgaand aan de wet van 30 november 1998

Een aantal documenten, gedateerd van vóór de goedkeuring van de wet van 30 november 1998, getuigen van de wil van de administrateur-generaal van de Veiligheid van de Staat om zijn dienst voor te bereiden op de uitoefening van de nieuwe opdracht ter bescherming van het wetenschappelijk en economisch potentieel.

Interessante documenten in dit verband zijn de volgende :

— In een nota, gericht aan de secretaris-generaal van het ministerie van Justitie op 25 maart 1997, evalueert de administrateur-generaal van de Veiligheid van de Staat de toekomstige noden van de buitendiensten voor de uitoefening van hun opdrachten, zoals beschreven in het wetsontwerp op de inlichtingen- en veiligheidsdiensten;

— een werknota van 5 februari 1998 van de Veiligheid van de Staat beschrijft de nieuwe opdracht van bescherming van het economisch en wetenschappe-

(1) *Cf.* Kamer van volksvertegenwoordigers van 28 oktober 1999 — Antwoord van de minister van Justitie op interpellatie nr. 84 van de heer Bourgeois.

Interpellé au sujet de l'interview précitée, le ministre de la Justice a questionné la Sûreté de l'État. Ce service lui a fait savoir qu'il n'existait aucune preuve concrète que des services de renseignement et de sécurité étrangers soient, en ce moment, actifs en Belgique sur le plan de l'espionnage économique ou industriel.

Néanmoins, des sources ouvertes font état de la réorientation de l'activité des services de renseignement de l'espionnage militaire vers l'espionnage économique.

En 1997 et 1998, la Sûreté de l'État a informé le ministre de la Justice que l'ambassade de Cuba à Bruxelles recherchait des informations universitaires de nature économique, mission pour laquelle cette ambassade avait même recruté du personnel (1).

Le 28 octobre 1999, le ministre de la Justice a annoncé qu'un membre de son cabinet participerait à la plate-forme de concertation permanente sur la sécurité industrielle. Cette intention a été confirmée par le plan fédéral de sécurité. Ce forum devrait pouvoir mettre en œuvre un plan de collaboration entre la Fédération des entreprises de Belgique et les pouvoirs publics. Selon le ministre, c'est dans ce cadre que la Sûreté de l'État pourra jouer un rôle proactif.

B. Les actions entreprises par la Sûreté de l'État

Les actions antérieures à la loi organique du 30 novembre 1998

Une série de documents préalables à l'adoption de la loi organique du 30 novembre 1998 témoignent de la volonté de l'administrateur général de la Sûreté de l'État de préparer son service à l'exercice de la nouvelle mission de protection du patrimoine scientifique et économique.

Les documents intéressants à cet égard sont les suivants :

— Dans une note adressée le 25 mars 1997 au secrétaire général du ministère de la Justice, M. Van Lijsebeth évalue les besoins futurs du cadre des services extérieurs pour l'exercice des missions décrites par le projet de loi organique des services de renseignement et de sécurité.

— Une note de travail datée du 5 février 1998 décrit la nouvelle mission de protection du potentiel économique et scientifique qu'entend confier à la

(1) Chambre des représentants du 28 octobre 1999 — Réponse du ministre de la Justice à l'interpellation nº 84 de M. Bourgeois.

lijk potentieel, die het wetsontwerp op de inlichtingen- en veiligheidsdiensten wenst op te dragen aan de Veiligheid van de Staat. (Dit document werd toegezonden aan het ministerie van Economische Zaken.)

De bedreiging door economische en wetenschappelijke spionage wordt als volgt omschreven:

« De gevolgen van economische en wetenschappelijke spionage vertonen zich zeer concreet in het verlies van belangrijke contracten, van markten, van werkplaatsen, door de diefstal van nieuwe technologie ...

De verliezen toe te schrijven aan spionage zijn moeilijk te berekenen want de slachtoffers aanvaarden zelden dat ze worden bekendgemaakt. Men kan evenwel bevestigen, meer bepaald op basis van wat in andere Europese landen werd ontdekt, dat de kost van economische spionage aanzienlijk is voor de ondernemingen en voor de economie van het land.

Belangrijke repercussies doen zich gevoelen in de sectoren van de defensie en de spitstechnologie, op het gebied van het onderzoek en op vlak van de buitenlandse politiek.

De economische en wetenschappelijke spionage, in de hand gewerkt door de toename van de economische concurrentie, vormt dus niet enkel een financiële en sociale bedreiging, maar eveneens een onbetwiste bedreiging wat de nationale veiligheid betreft. »

Op 28 november 1997 gaf het Ministerieel Comité inlichting en veiligheid aan het College voor de inlichting en veiligheid de opdracht om: « ... de analyse te verdiepen van de bedreigingen door aantasting, — met inbegrip van economische spionage —, van bepaalde socio-economische sectoren, om voorstellen te formuleren om deze bedreigingen te bestrijden en te onderzoeken in welke mate het ministerie van Economische Zaken kan betrokken worden bij deze werkzaamheden. »

Het College voor de inlichting en veiligheid vertrouwde deze opdracht toe aan de Veiligheid van de Staat, die op haar beurt de voorstellen van acties formuleerde in een nota van 5 februari 1998:

« 1. De inventaris opstellen van sectoren die dreigen geviseerd te worden:

— de ondernemingen die een bijzonder economisch of technologisch belang hebben of die vitaal zijn voor de tewerkstelling of de basisbehoeften van de bevolking;

— de instellingen voor wetenschappelijk onderzoek, belangrijke laboratoria, zowel privé als publiek, de universiteiten en bepaalde hogescholen, de departementen die verantwoordelijk zijn voor wetenschappen en economie.

Sûreté de l'État le projet de loi organique des services de renseignement et de sécurité. Ce document a été transmis au ministre des Affaires économiques.

La menace de l'espionnage économique et scientifique est décrite comme suit:

« Les effets de l'espionnage économique et scientifique se manifestent très concrètement par la perte de contrats importants, de marchés, d'emplois, par le vol de nouvelles technologies ...

Les pertes imputables à l'espionnage sont difficiles à chiffrer car les victimes de l'espionnage acceptent rarement de les dénoncer. On peut cependant affirmer, notamment sur la base de ce qui a été découvert dans d'autres pays européens, que le coût de l'espionnage économique est considérable pour les entreprises et pour l'économie du pays.

Des répercussions importantes se font sentir dans les secteurs de la défense et des technologies avancées, dans le domaine de la recherche et au niveau de la politique étrangère.

L'espionnage économique et scientifique, favorisé par la croissance de la concurrence économique, constitue donc non seulement une menace financière et sociale, mais également une menace certaine à l'égard de la sécurité nationale. »

Le 28 novembre 1997, le Comité ministériel du renseignement a chargé le Collège du renseignement et de la sécurité « d'approfondir l'analyse des menaces d'atteintes, en ce compris par l'espionnage économique, à certains secteurs socio-économiques, de formuler des propositions pour lutter contre ces menaces et d'examiner dans quelle mesure associer à ces travaux le département des Affaires économiques ».

Le Collège du renseignement et de la sécurité a confié cette mission à la Sûreté de l'État qui a elle-même formulé les propositions d'actions suivantes dans une note du 5 février 1998:

« 1. Faire l'inventaire des secteurs qui risquent d'être visés:

— les entreprises qui ont un intérêt, économique ou technologique particulier ou qui sont vitales pour l'emploi ou les besoins de base de la population;

— les instituts de recherches scientifiques, les laboratoires importants tant privés que publics, les universités et certaines écoles supérieures, les départements responsables pour les sciences et l'économie.

2. De bedreigingen en hun oorsprong bepalen en onderzoeken door contacten met de geviseerde sectoren en de organisatie van informatie-uitwisseling. (Verderop worden de bedreigingen als volgt omschreven: « Spionage door buitenlandse bedrijven, oneerlijke internationale concurrentie, pogingen tot onwettige overname van Belgische ondernemingen door buitenlandse tussenpersonen, enz., clandestiene onderzoeksactiviteiten door buitenlandse regeringen of -overheden of hun inlichtingendiensten, ... »).

(Volgens de Veiligheid van de Staat zou dus de industriële spionage, uitgeoefend door een onderneming tegen een andere op het niveau van de nationale privé-sector, niet tot haar opdrachten behoren.)

3. Het uitbreiden of aanpassen van de opzoekingen door de dienst in de klassieke domeinen (spionage (politieke), terrorisme, ideologisch extremisme, schadelijke sekten, georganiseerde criminaliteit, proliferatie van NBC-materiaal, bescherming van personen, talrijke taken van opzoekingen en adviezen van administratieve aard, ...) aan de noden op het vlak van de economische en wetenschappelijke bescherming.

4. Sensibilisering en raadgeving aan economische en wetenschappelijke instellingen inzake de te nemen veiligheidsmaatregelen (personeel, bescherming van gegevens, fysieke bescherming, communicatieverbindingen, enz.).

5. Het deelnemen aan of organiseren van overlegvergaderingen met de betrokken officiële instanties.

6. Aan de overheden analyses verschaffen over de dreigingen en maatregelen voorstellen.

7. De Belgische regering verwittigen wanneer de spelregels eigen aan de markteconomie opzettelijk vervalst worden in het nadeel van de Belgische belangen.

8. Studie van de buitenlandse wetgeving en de juridische aspecten in deze materie » (1).

De nota van 5 februari 1998 gaat verder en raamt op minimale wijze de bijkomende personeelsbehoefte bij de veiligheid van de Staat om deze nieuwe opdracht uit te voeren.

Gezien de omvang van deze opdracht wordt de voorlopige raming van 25 maart 1997 als kennelijk onvoldoende beoordeeld.

Als bijlage vindt men een — niet exhautieve — lijst van departementen en overheidsdiensten die betrokken zijn bij de nieuwe opdracht.

(1) Vrije vertaling.

2. Déterminer et enquêter sur les menaces et leurs origines par des contacts avec les secteurs visés, et organisation d'échanges d'informations ». (Plus loin, les menaces sont ainsi décrites: « Espionnage par des entreprises étrangères, concurrence déloyale internationale, tentative d'OPA illicite d'entreprises belges par des intervenants étrangers, etc. Recherches d'activités clandestines de gouvernements ou administrations étrangers et leurs services de renseignement »).

Selon la Sûreté de l'État, ne seraient donc pas inclus dans sa mission, l'espionnage industriel développé par une firme contre une autre au niveau du secteur privé national.

3. Elargir ou adapter les recherches dans les domaines classiques (espionnage (politique), terrorisme, extrémisme idéologique, sectes nuisibles, crime organisé, prolifération de matières NBC, protection de personnes, nombreuses tâches de recherche et d'avis administratifs, ...) couverts par le service aux besoins de la protection économique et scientifique.

4. Sensibilisation et conseils aux institutions économiques et scientifiques quant aux mesures de sécurité à prendre (personnel, protection des données, protection physique, communications, etc.).

5. Assister à ou organiser des réunions de concertation avec les instances officielles concernées.

6. Fournir des analyses de la menace et proposer des mesures à prendre aux autorités.

7. Prévenir le gouvernement belge lorsque les règles du jeu propre à l'économie de marché sont délibérément faussées au détriment des intérêts belges.

8. Étude des législations étrangères et des aspects juridiques liés à la matière (1).

La note du 5 février 1998 se poursuit en estimant de manière minimale le besoin en personnel supplémentaire à la Sûreté de l'État pour réaliser cette nouvelle mission.

Vu l'ampleur de la nouvelle mission, l'estimation provisoire du 25 mars 1997 est jugée manifestement insuffisante.

En annexe, on trouve une liste — non exhaustive — des départements et services de l'État concernés par la nouvelle mission de protection du potentiel économique et scientifique.

(1) Traduction libre.

De acties navolgend op de wet van 30 november 1998

De «bescherming van het wetenschappelijk of economisch potentieel» komt vanaf nu wel degelijk voor in de opdrachten bepaald in de interne richtlijnen van de Veiligheid van de Staat. De opdracht werd zelfs uitgebreid tot de «bescherming van het industrieel patrimonium», opgevat als een deel van het economisch potentieel en dat het geheel van de economische activiteiten tot productie van goederen omvat.

Een nieuwe sectie die werd opgericht, is specifiek belast met de nieuwe opdracht.

Op 28 maart 2000 deelt de administrateur aan de nieuwe minister van Justitie mee op welke wijze zij de uitvoering van deze nieuwe opdracht opvat. De bewoordingen van deze nota zijn vrij gelijklopend met deze van de nota van 5 februari 1998. De vraag om personeel slaat op 50 eenheden voor de buitendiensten en voor 28 eenheden voor de administratieve diensten (wetenschappers, economisten, ingenieurs, enz.). De minister verleent zijn goedkeuring op 11 april 2000 om deze voorstellen voor te leggen aan het ministerieel Comité Inlichting en veiligheid.

Het ministerieel Comité inlichting en veiligheid bereidt de richtlijnen voor, teneinde het economisch en wetenschappelijk potentieel te definiëren ter uitvoering van artikel 7 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Het Comité I heeft nog geen kennis van het resultaat van de werkzaamheden.

Intussen nam het kabinet van de minister van Justitie deel aan verschillende vergaderingen van het «Permanent overlegplatform bedrijfsbeveiliging» in aanwezigheid van vertegenwoordigers van het VBO.

De voorstellen die voortvloeiden uit dit platform van het VBO werden in juli 2000 daadwerkelijk door de Veiligheid van de Staat onderzocht, en deze gaf haar advies hieromtrent aan de minister van Justitie op 1 augustus 2000.

Dit advies beveelt onder meer aan om:

«1. de inrichting van een preventieactie door het VBO en de Staatsveiligheid, *in concreto* door de voorstelling van sensibiliserings-uiteenzettingen voor ondernemingen die behoren tot de geviseerde sectoren;

2. de opstelling en her-actualisering van een prioriteitenlijst van sectoren met activiteiten en spitstechnologie die een doeltreffende en snelle bescherming van de betrokken ondernemingen toelaten;

3. de inzameling van inlichtingen die in het bijzonder betrekking hebben — binnen de economische wereld — tot sektaire organisaties, georganiseerde criminaliteit of spionnage door buitenlandse mach-

Les actions postérieures à la loi organique du 30 novembre 1998

La «protection du potentiel scientifique et économique» figure bien à présent dans les missions définies par les directives internes de la Sûreté de l'État. La mission est même étendue à la «protection du patrimoine industriel» conçu comme une part du potentiel économique et qui comprend l'ensemble des activités économiques de production de biens.

Une nouvelle section a été créée spécifiquement chargée de la protection du potentiel économique et scientifique.

Le 28 mars 2000, l'administrateur général *ad interim* a fait part au nouveau ministre de la Justice de la manière dont elle concevait l'exécution de cette nouvelle mission. Les termes de cette note sont assez semblables à ceux de la note du 5 février 1998. La demande de personnel pour la nouvelle mission porte sur 50 unités pour les services extérieurs et 28 unités pour les services administratifs (scientifiques, économistes, ingénieurs, etc.). Le 11 avril 2000, le ministre a marqué son accord avec ces propositions à soumettre au CMRS.

Le Conseil ministériel du renseignement et de la sécurité prépare des directives afin de définir le potentiel scientifique et économique à protéger en application de l'article 7 de la loi organique des services de renseignement et de sécurité. Le Comité R n'a pas encore connaissance du résultat de ses travaux.

Entre-temps, le cabinet du ministre de la Justice a participé à plusieurs réunions de la «Plate-forme de concertation permanente sur la sécurité industrielle» en présence de représentants de la FEB.

Les propositions issues de cette plate-forme de concertation ont effectivement été examinées en juillet 2000 par la Sûreté de l'État laquelle a transmis son avis au ministre de la Justice le 1er août 2000.

Cet avis préconise notamment:

1. «la mise en place d'une action de prévention conjointe FEB/SE, concrétisée par la présentation d'exposés de sensibilisation auprès d'entreprises appartenant à des secteurs exposés;

2. la constitution et la réactualisation d'une liste prioritaire de secteurs d'activités et de technologies de pointe permettant une protection efficace et rapide des entreprises concernées;

3. le recueil de renseignements plus spécifiquement relatifs aux activités, au sein du monde économique, d'organisations sectaires, de la criminalité organisée ou d'espionnage par des puissances étrangères. Cette

ten. Deze informatiegaring zal het mogelijk maken om de verborgen dreiging te analyseren en om eventueel beschermende maatregelen te nemen.»

De Veiligheid van de Staat vraagt trouwens dat haar agenten zouden kunnen deelnemen aan vormingsprogramma's over de ondernemingsorganisatie en de criminaliteitsvormen waarvan de onderneming het slachtoffer is.

Zij dringt aan op de oprichting van een cel «Informatica- en telecommunicatiecriminaliteit» binnen een federaal agentschap voor de bescherming van de informatica en de vercijfering.

De administrateur-generaal van de Veiligheid van de Staat stelde deze nota voor aan het kabinet van de minister van Justitie tijdens twee vergaderingen die plaatsvonden op 2 augustus en 6 september 2000.

De sectie belast met het wetenschappelijk en economisch potentieel nam reeds een aantal contacten met verantwoordelijken van private en publieke ondernemingen, patroonsorganisaties, universiteiten , ministeries en andere overheidsadministraties.

De andere secties van de buitendiensten zijn bovendien gemachtigd om gegevens in te zamelen in verband met dit onderwerp indien bedreigingen uitgaan van landen of extremistische, sektarische of criminele milieus die zij behandelen.

De analysedienst die gelast is met de criminele organisaties en de contraspionage (die onder meer «ontwrichtende gevolgen op politiek en socio-economisch gebied» kunnen hebben) werd in eerste instantie belast met het ontvangen en behandelen van de rapporten inzake de bescherming van het wetenschappelijk en economisch potentieel. Sedert september 2000 werd deze nieuwe bevoegdheid toevertrouwd aan de analysedienst die eveneens verantwoordelijk is op het gebied van wapens en proliferatie.

Op 30 november 2000 werden reeds een zeventigtal informatieverslagen, evenals vijf analyserapporten opgesteld over het economisch en wetenschappelijk potentieel. De Veiligheid van de Staat toont zich onder meer gevoelig voor de occulte invloed die een sekte zou kunnen pogen uit te oefenen op de grote economische beleidsvormers van het land.

In afwachting van noodzakelijke richtlijnen van het ministerieel Comité inlichting en veiligheid, gebruikt de Veiligheid van de Staat deze rapporten uitsluitend strikt intern.

Er hebben eveneens gesprekken van algemeen aard plaats over dit onderwerp met de Algemene Dienst inlichting en veiligheid, maar er werd nog niet overgegaan tot een uitwisseling van gegevens. Er werden

collecte d'information permettra d'analyser la menace latente et la mise en place éventuelle de mesures protectrices».

La Sûreté de l'État demande par ailleurs que ses agents puissent prendre part à des formations au sujet de l'organisation de l'entreprise et des formes de criminalité dont celle-ci est victime.

Elle préconise la mise en place d'une cellule «criminalité informatique et télécommunications» au sein d'une agence fédérale pour la protection informatique et le cryptage.

L'administrateur général de la Sûreté de l'État a présenté cette note au cabinet du ministre de la Justice au cours de deux réunions qui se sont tenues les 2 août et 6 septembre 2000.

La section chargée du potentiel scientifique et économique a déjà établi une série de contacts avec des responsables d'entreprises privées et publiques, de fédérations patronales, d'universités, de ministères et autres administrations publiques.

Les autres sections des services extérieurs de la Sûreté de l'État sont en outre habilitées à recueillir des informations en rapport avec le potentiel scientifique et économique lorsque les menaces émanent soit des pays, soit des milieux extrémiste, sectaire ou criminel qu'elles traitent.

Le service d'analyse chargé des organisations criminelles et du contre-espionnage (qui peuvent notamment avoir des «conséquences déstabilisatrices sur le plan politique ou socio-économique») a d'abord été chargé de recevoir et de traiter les rapports relatifs à la protection du potentiel scientifique et économique. Depuis septembre 2000, cette nouvelle compétence est confiée au service d'analyse qui est également compétent en matière d'armes et de prolifération. L'espionnage est également traité par les services d'étude de certaines régions du monde selon l'origine géographique des activités d'espionnage détectées.

Au 30 novembre 2000, une septantaine de rapports d'information ainsi que cinq rapports d'analyse concernant la protection du potentiel scientifique et économique ont déjà été rédigés. La Sûreté de l'État s'y montre notamment sensible à l'influence occulte qu'une secte pourrait tenter d'exercer sur les grands décideurs économiques du pays.

En attendant de recevoir les directives nécessaires du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'État n'utilise ces rapports qu'à des fins purement internes.

De même, des discussions d'ordre général ont eu lieu sur le sujet avec le SGR mais il n'a encore été procédé à aucun échange d'informations. Quelques contacts préparatoires ont été établis avec des services

voorbereidende contacten gelegd met buitenlandse inlichtingendiensten, maar niet onder vorm van officiële samenwerking.

Bij herhaling heeft de administrateur-generaal van de veiligheid van de Staat aan het ministerieel Comité inlichting en veiligheid verzocht om zich uit te spreken over de wijze waarop de dienst inlichtingen moest doorgeven aan ministeries, administratieve en gerechtelijke overheden, aan politiediensten en bevoegde personen overeenkomstig artikel 19, eerste lid, van de organieke wet op de inlichtingen- en veiligheidsdiensten.

8.3. De Algemene Dienst inlichting en veiligheid

In 1997 verklaarde de toenmalige administrateur-generaal van de Veiligheid van de Staat aan het Comité I dat de vrijwaring van het economisch en wetenschappelijk potentieel een nieuwe opdracht zou zijn die de Veiligheid van de Staat alleen zou moeten vervullen dit wil zeggen met uitsluiting van de Algemene Dienst inlichting en veiligheid. Inderdaad, de organieke wet op de inlichtingen- en veiligheidsdiensten gaf aan de Algemene Dienst inlichting en veiligheid geen taak tot opzoeken, analyseren en behandelen van inlichtingen over activiteiten die het wetenschappelijk of economisch potentieel van het land bedreigen.

Niettemin beheert de sectie verantwoordelijk voor de militaire en industriële veiligheid van de Algemene Dienst inlichting en veiligheid, in het kader van de wet van 10 januari 1955 op de industriële eigendom en in samenwerking met het ministerie van Economische Zaken, de informaties en geclassificeerde brevetten teneinde de exploitatievoorwaarden van uitvindingen en de uitwerking van fabrieksgeheimen die ter kennis komen van commerciële ondernemingen te controleren, en dit in het kader van hun specifieke activiteiten te voordele van landsverdediging of van de NAVO.

Het gaat *in casu* om het toepassen van de procedures die eigen zijn aan het indienen, het beheer en het opheffen van het geheim van geclassificeerde brevetten, — uitvindingen en — gegevens die, overeenkomstig de wet, niet verspreid mogen worden.

De ADIV stelt voorschriften voor industriële veiligheid op, verspreidt ze en controleert hun toepassing bij de industriële ondernemingen die in België gevestigd zijn. Indien de installatie in een ander land gevestigd is, draagt de Algemene Dienst inlichting en veiligheid er zorg voor dat de controle in het betrokken land door de bevoegde nationale overheid wordt uitgevoerd.

Op eigen grondgebied handelt de Algemene Dienst inlichting en veiligheid op eenzelfde wijze voor geclassificeerde brevetten van een buitenlandse mogendheid, binnen het kader van artikel 12 van de bovengenoemde wet.

de renseignement étrangers, mais aucune collaboration officielle.

À plusieurs reprises, l'administrateur général de la Sûreté de l'État a demandé que le Comité ministériel du renseignement et de la sécurité (CMRS) se prononce sur la manière dont son service devait communiquer des renseignements aux ministres, aux autorités administratives et judiciaires, aux services de police, aux instances et personnes compétentes conformément à l'article 19, alinéa 1er, de la loi organique des services de renseignement et de sécurité.

8.3. Le SGR

En 1997, M. Van Lijsebeth, alors administrateur général de la Sûreté de l'État, avait déclaré au Comité R que la sauvegarde du potentiel scientifique et économique du pays serait une mission toute nouvelle que la Sûreté devrait accomplir seule, c'est-à-dire en excluant le SGR. En effet, la loi organique des services de renseignement et de sécurité n'a pas donné au SGR la mission de rechercher, d'analyser et de traiter le renseignement relatif aux activités qui menacent le potentiel scientifique et économique du pays.

Cependant, dans le cadre de la loi du 10 janvier 1955 sur la propriété industrielle, la section du SGR chargée de la sécurité militaire et industrielle assure la gestion des informations et brevets «classifiés» conjointement avec le ministre des Affaires économiques pour contrôler les conditions d'exploitation, d'inventions et de mise en œuvre des secrets de fabrique portés à la connaissance de sociétés commerciales, dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l'OTAN.

Il s'agit en l'occurrence d'appliquer les procédures inhérentes au dépôt, à la gestion et la levée du secret des brevets, des inventions et des informations «classifiés» qui, à ce titre, ne peuvent être divulgués conformément à la loi.

Le SGR établit et diffuse des directives de sécurité industrielle et contrôle leur application auprès des sociétés industrielles installées sur le territoire national. Si l'installation est située dans un autre pays, le SGR veille à ce que ce contrôle se fasse dans le pays concerné par l'autorité nationale compétente de ce pays.

Le SGR agit de la même manière sur le territoire national pour les brevets «classifiés» par un État étranger, dans le cadre de l'article 12 de la loi en question.

De Algemene Dienst inlichting en veiligheid voert eveneens onderzoeken uit met het oog op het toekennen van veiligheidsmachtigingen aan ondernemingen, hun zaakvoerders en hun personeel in het kader van hun specifieke activiteiten ten voordele van de landsverdediging of van de NAVO. De bedoeling van deze onderzoeken is het nagaan van de integriteit van de zaakvoerders en het personeel van die firma's, zowel op het vlak van betrouwbaarheid, loyaliteit en discretie als op het financieel en commercieel gebied.

9. Besluiten en aanbevelingen

Twee jaar nadat aan de Veiligheid van de Staat de opdracht werd toevertrouwd om het wetenschappelijk en economisch potentieel te beschermen, geeft deze dienst blijk van sensibilisering voor dit onderwerp bij wijze van meerdere interne nota's en voorbereidende documenten gericht aan de minister van Justitie.

Toch is de Veiligheid van de Staat van oordeel dat het nog niet in staat is om deze nieuwe taak op operationele wijze uit te voeren.

Deze situatie is het gevolg van het feit dat de dienst:

— nog geen richtlijnen heeft ontvangen van het Ministerieel Comité inlichting en veiligheid die de bescherming van het wetenschappelijk en economisch potentieel vastleggen zoals voorgeschreven in artikel 7, 1º, van de wet van 30 november 1998;

— geen bijkomende en noodzakelijke menselijke middelen kreeg.

Het Comité I beveelt aan dat deze twee obstakels worden weggeruimd om de Veiligheid van de Staat toe te laten haar opdracht uit te voeren.

In afwachting bereidt een sectie het terrein voor, door het leggen van een aantal contacten die bedoeld zijn om de economische en wetenschappelijke milieus te sensibiliseren.

Het Comité I is overtuigd van de moeilijkheid om de wetenschappelijke en economische geheimen te beschermen in de huidige context van de informatiemaatschappij, die gedomineerd wordt door technologische vooruitgang, gekenmerkt door mondialisering en wetenschappelijke openheid van geest. De mondialisering van de ondernemingen en de globalisering van procédés op wereldschaal maken het trouwens moeilijk om een nationaliteit toe te kennen aan een wetenschappelijk of economisch potentieel.

Het is vooral om deze reden dat het Comité I meent dat het criterium van de nationaliteit van de opdrachtgevers van de spionage, niet relevant is. Dit criterium wordt gebezigd door de Veiligheid van de Staat om de economische spionage (waarvoor ze zou

Le SGR effectue également les enquêtes en vue de l'octroi des habilitations de sécurité aux firmes, à leurs administrateurs et à leur personnel dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l'OTAN. La finalité de ces enquêtes est de vérifier l'intégrité des administrateurs et du personnel de ces firmes, aussi bien sur le plan de la fiabilité, de la loyauté et de la discrétion que sur les plans financier et commercial.

9. Conclusions et recommandations

Deux ans après que lui ait été attribuée la mission de protéger le potentiel scientifique et économique du pays, la Sûreté de l'État se montre sensibilisée à ce sujet à travers différentes notes internes et documents préparatoires adressés au ministre de la Justice.

Toutefois, la Sûreté de l'État n'estime pas être encore en mesure de remplir cette nouvelle tâche de manière opérationnelle.

Cette situation est due au fait que la Sûreté de l'État:

— n'a pas encore reçu les directives du Comité ministériel du renseignement et de la sécurité définissant le potentiel scientifique et économique à protéger ainsi que le prescrit l'article 7, 1º, de la loi du 30 novembre 1998;

— n'a pas reçu les moyens humains supplémentaires nécessaires.

Le Comité R recommande que ces deux obstacles soient levés pour permettre à la Sûreté de l'État de remplir sa nouvelle mission.

En attendant, une section prépare le terrain en établissant une série de contacts destinés à sensibiliser les milieux économiques et scientifiques à la problématique.

Le Comité R est conscient de la difficulté de protéger les secrets scientifiques et économiques dans le contexte actuel de la société de l'information dominée par les progrès technologiques et caractérisée autant par son mondialisme que par son ouverture d'esprit scientifique. La mondialisation des entreprises et la globalisation des procédés au niveau mondial rendent d'ailleurs difficile l'attribution d'une nationalité à un potentiel scientifique et/ou économique.

C'est notamment la raison pour laquelle le Comité R estime non pertinent le critère de nationalité du mandant de l'espion retenu par la Sûreté de l'État pour distinguer l'espionnage économique (pour lequel elle serait compétente) de l'espionnage indus-

bevoegd zijn) te onderscheiden van de industriële spionage (private affaire waarvoor ze niet bevoegd zou zijn).

In navolging van het VBO, neigt het Comité I er naar om te beschouwen als behorend tot het wetenschappelijk en economisch potentieel van het land, elke onderneming, elk laboratorium of onderzoeksinstelling die of dat een activiteit uitoefent in het land en hierbij een toegevoegde waarde ontwikkelt. Het Comité I heeft de administrateur generaal van de Veiligheid van de Staat in kennis gesteld van dit standpunt.

Het komt aan het Ministerieel Comité inlichting en veiligheid toe om te beslissen.

De belangrijkheid van de private sector en de belangen die verbonden zijn met het wetenschappelijk en economisch potentieel creëren nieuwe veiligheidsbehoeften in de wereld van de wetenschappen en ondernemingen. In ons land werden deze behoeften gedefinieerd door het VBO.

De bescherming van voornoemd potentieel moet een aandachtsonderwerp zijn van het Parlement en de regering, in de mate dat ons land vele, vaak kleinere ondernemingen telt die betrokken zijn in onderzoek en ontwikkeling van spitstechnologie. Indien aan de veiligheidsbehoeften onvoldoende beantwoord wordt door de overheden en onze inlichtingendiensten, zullen de ondernemingen en de onderzoekslaboratoria ofwel de risico's die zij lopen blijven onderschatten of zich tot private inlichtingen- en veiligheidsfirma's richten.

In deze is de sterke groei van private inlichtingenondernemingen in economische zaken een bron van bezorgdheid en vraagstelling wat hun ethiek, juridisch kader en de democratische controle betreft.

triel (affaire privée pour laquelle elle ne serait pas compétente).

À l'instar de la FEB, le Comité R tend à considérer comme appartenant au potentiel scientifique et économique du pays, toute entreprise, tout laboratoire ou tout centre de recherche exerçant son activité sur le territoire national et y développant une valeur ajoutée. Le Comité R a fait part de ce point de vue à l'administrateur général de la Sûreté de l'État.

C'est au Comité ministériel du renseignement et de la sécurité qu'il appartiendra de trancher.

L'importance prise par le secteur privé et les enjeux liés au patrimoine scientifique et économique du pays créent en effet de nouveaux besoins de sécurité dans le monde scientifique et celui des entreprises. Dans notre pays, certains de ces besoins ont été définis par la Fédération des entreprises de Belgique.

Ceci doit être un sujet d'attention pour le Parlement et le gouvernement dans la mesure où notre pays compte nombre d'entreprises, souvent de petites dimensions, impliquées dans la recherche et le développement de technologies de pointe. Si les besoins de sécurité ne sont pas suffisamment pris en compte par les autorités publiques et par nos services de renseignement, soit les entreprises et les laboratoires de recherche continueront à sous-estimer les risques qu'ils courent, soit ils se tourneront vers les firmes privées de renseignement et de sécurité.

À cet égard, la montée en puissance des sociétés de renseignement privées en matière économique suscite des interrogations profondes quant à leur éthique, leur cadre juridique et leur contrôle démocratique.

C. Onderzoeken op initiatief van de Dienst enquêtes

ONDERZOEK NAAR DE INTERVENTIE VAN DE ADIV NAAR AANLEIDING VAN EEN EVENTUEEL VEILIGHEIDSINCIDENT BINNEN EEN MILITAIRE BASIS

1. Procedure

In februari 1999 ontving het Comité I een schrijven van zijn Dienst enquêtes. Deze dienst wilde een mogelijke provocatie van neonazistische aard onderzoeken die zich had voorgedaan ter gelegenheid van een vliegmeeting op 5 en 6 september 1998 op de basis van Kleine Brogel.

Voor zover het Comité I weet hebben twee persorganen over de feiten verslag uitgebracht en daarbij een of meer foto's gepubliceerd.

Op 10 februari 1999 verleende het Comité I aan het hoofd van de Dienst enquêtes de toestemming om een onderzoek te voeren naar de feiten. Dezelfde dag gaf het Comité I de voorzitters van Kamer en Senaat kennis van de opening van het onderzoek, overeenkomstig artikel 46, § 3, van zijn huishoudelijk reglement en de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, zoals deze wet in die tijd van toepassing was.

Op 12 februari 1999 bracht het hoofd van de Dienst enquêtes op zijn beurt de minister van Landsverdediging op de hoogte van dit onderzoek, krachtens artikel 43.1 van dezelfde organieke wet.

Op 31 maart 1999 legde de Dienst enquêtes van het Comité I een rapport neer.

Een aanvullend kantschrift werd op 21 december 1999 verzonden aan de Dienst enquêtes, die zijn eindrapport indiende op 11 september 2000.

Het Comité I heeft dit onderzoeksrapport goedgekeurd op 12 maart 2001.

Op 12 april 2001 heeft de minister van Landsverdediging schriftelijk laten weten dat hij geen commentaar had op het verslag.

De minister vermeldt tevens: «Verwijzend naar mijn antwoorden op vroeger gestelde parlementaire vragen, maak ik hierbij van de gelegenheid gebruik mijn eerder uitgedrukt standpunt te bevestigen dat extreemrechtse organisaties helemaal niet thuishoren op massa-evenementen die door Landsverdediging worden georganiseerd.»

2. De belangstelling van het Parlement

Het Comité I heeft vastgesteld dat in verband met deze zaak een aantal parlementaire vragen werden

C. Enquêtes à l'initiative du Service d'enquêtes

ENQUÊTE SUR L'INTERVENTION DU SGR À PROPOSD'UNÉVENTUELINCIDENTDESÉCURITÉ À L'INTÉRIEUR D'UNE ENCEINTE MILITAIRE

1. Procédure

Au mois de février 1999, le Comité R réceptionne un courrier de son Service d'enquêtes. Ce dernier souhaite en effet prendre en considération l'éventualité d'une provocation à caractère néo-nazi s'étant déroulée à l'occasion d'un meeting aérien organisé les 5 et 6 septembre 1998 sur la base de Kleine Brogel.

Deux organes de presse, à la connaissance du Comité R, en ont fait une relation, photo(s) à l'appui.

Le 10 février 1999, le Comité R fait donc parvenir son accord au chef du Service d'enquêtes et se charge, à la même date, de notifier l'ouverture de cette enquête aux présidents respectifs de la Chambre et du Sénat, en conformité avec l'article 46, § 3, de son règlement d'ordre intérieur et la loi organique de contrôle des services de police et de renseignement du 18 juillet 1991, telle qu'elle était en vigueur à cette époque.

Le 12 février 1999, le chef du Service d'enquêtes adresse à son tour notification de l'ouverture de cette enquête au ministre de la Défense nationale, en exécution de l'article 43.1 de la même loi organique.

Le Service d'enquêtes du Comité R dépose un rapport en date du 31 mars 1999.

Une apostille complémentaire lui est adressée le 21 décembre 1999 et le rapport d'enquête final sera déposé le 11 septembre 2000.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 12 mars 2001.

Le 12 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas de commentaire à formuler au sujet de ce rapport.

Toutefois, il a souligné que: «Faisant référence à mes réponses aux questions parlementaires antérieures, je saisis l'occasion de confirmer mon point de vue, déjà exprimé antérieurement, que des organisations d'extrême droite ne sont pas du tout à leur place lors d'événements organisés par la Défense nationale.»

2. L'intérêt parlementaire

Sans prétendre à l'exhaustivité, le Comité R a relevé l'existence de questions parlementaires à ce

gesteld aan de vice-eerste minister en aan de minister van Landsverdediging. Zonder een volledige opsomming daarvan te willen geven, ging het onder meer om de vragen van 30 oktober 1998 van volksvertegenwoordigers Rony Cuyt en Lode Vanoost, en om de vraag van 27 oktober 1998 van senator Erdman.

In die vragen is er vooral sprake van een organisatie die « Soldiers of fortune » heet en die banden zou hebben met extreem-rechtse elementen in de Verenigde Staten.

In antwoord op deze vragen verklaarde de minister dat aan een man, afkomstig uit Wales, die zich had bekendgemaakt onder de benaming « Soldiers of fortune », de toestemming was verleend om een stand te houden.

Op dat ogenblik wist niemand iets af van zijn eventuele banden met extreem-rechts, en de controles die vóór en tijdens het evenement plaatsvonden hadden geen abnormale zaken aan het licht gebracht. Voorts verklaarde de minister dat extreem-rechtse organisaties niet mogen worden toegelaten tot massa-evenementen die het leger organiseert.

3. Vaststellingen

De Dienst enquêtes van het Comité I heeft contact opgenomen met de ADIV en heeft om te beginnen een onderhoud gehad met de hoofdcommissaris belast met problemen inzake terrorisme en subversie.

De betrokkene verklaarde dat de militaire overheid die het evenement organiseert in hoofdzaak bevoegd is voor de veiligheid. Bijgevolg is de korpschef van de organiserende eenheid aansprakelijk voor de aanwezigheid van particulieren en bedrijven die op het terrein een of andere bedrijvigheid beoefenen.

De meeting van Kleine Brogel vormt echter een uitzondering op deze regel.

In het kader van deze specifieke opvolging en naar aanleiding van de belangstelling waarvan de minister van Landsverdediging naderhand blijk heeft gegeven, kon de ADIV bij toeval bepaalde inlichtingen verstrekken betreffende de stand « Soldiers of fortune ».

Uit de verklaringen aan de onderzoekers van het Comité I is gebleken dat de organisator gekend was bij de militaire overheden van Kleine Brogel, aangezien hij ter gelegenheid van een vroegere show in 1995 reeds de toestemming had gevraagd, — en gekregen —, om diverse zaken te verkopen, zoals : « British army berets, cap badges, clothing, boots, coffee mugs and zippo lighters with military crests on, enz. ».

In de uitgereikte toestemming werd de aandacht van de betrokkene erop gevestigd dat de basis van Kleine Brogel noch de Belgische regering aansprakelijk konden worden gesteld voor ongevallen of incidenten waarbij personeelsleden van de stand betrokken zouden zijn.

sujet, à l'adresse du vice-premier ministre et ministre de la Défense nationale, soit celles du 30 octobre 1998 des députés Rony Cuyt et Lode Vanoost ainsi que celle du 27 octobre 1998 du sénateur Erdman.

Il y est essentiellement question d'une organisation nommée « Soldiers of fortune » qui serait liée à l'extrême droite américaine.

Le ministre a porté à la connaissance des intervenants qu'une autorisation de tenir un stand a été délivrée à un homme originaire du pays de Galles s'étant fait connaître sous l'appellation de « Soldiers of fortune ».

À ce moment personne ne savait rien de ses éventuels liens avec l'extrême droite et les contrôles organisés avant et pendant la manifestation n'avaient rien révélé d'anormal. Le ministre a en outre déclaré que les organisations d'extrême droite ne peuvent être tolérées aux manifestations de masse organisées par l'armée.

3. Constatations

Le Service d'Enquêtes du Comité R a pris contact avec le SGR et s'est d'abord entretenu avec le commissaire principal chargé de la problématique du terrorisme et de la subversion.

Ce dernier précise que la sécurité est essentiellement du ressort de l'autorité militaire qui organise la manifestation. La responsabilité de la présence de particuliers et de sociétés exerçant une activité sur le site incombe donc au chef de corps de l'unité organisatrice.

Le meeting de Kleine Brogel représente toutefois une exception.

C'est donc à l'occasion de ce suivi spécifique et de l'intérêt ultérieurement manifesté par le ministre de la Défense nationale que le SGR a pu fournir incidemment quelques éléments d'information relatifs au stand « Soldiers of fortune ».

Selon les déclarations faites aux enquêteurs du Comité R, l'organisateur était connu des autorités militaires de Kleine Brogel dans la mesure où il avait déjà sollicité, et obtenu, lors d'un air show antérieur en 1995, l'autorisation de vendre divers colifichets, style; « british army berets, cap badges, clothing, boots, coffee mugs and zippo lighters with military crets on, etc. ».

L'autorisation délivrée attirait l'attention du candidat sur le fait que ni la base de Kleine Brogel, ni le gouvernement belge, ne sauraient être tenus pour responsables d'accidents ou d'incidents dans lesquels seraient impliqués les membres du personnel de ce stand.

Aangezien de betrokkene geen onbekende was, werd de aanvraag tot toestemming van « Soldiers of fortune », die in 1998 werd ingediend, niet aan de ADIV bezorgd. Het ging immers om een « habitué », wiens stand in het verleden geen incidenten had uitgelokt.

Een controle *a posteriori* heeft aangetoond dat de standhouder niet voorkwam in de documentatie van de ADIV. Evenmin is bij een later contact met een geallieerde dienst gebleken dat de betrokkene banden zou hebben gehad met extreem-rechts.

De Veiligheid van de Staat werd echter niet geraadpleegd met betrekking tot de standhouder of tot de organisatie « Soldiers of fortune ».

De ADIV heeft met nadruk verklaard dat zijn agenten niet hadden vastgesteld dat er op de stand voorwerpen waren aangetroffen die voorzien waren van neonazistische symbolen. Dit is in tegenspraak met de voorstelling van een foto die in de pers verscheen en waarop een persoon met een bivakmuts is te zien die een bierpul met een hakenkruis voor zich uit houdt.

Aangezien geen dergelijke zaken werden vastgesteld, werd geen enkel rapport opgemaakt betreffende dit type van activisme.

Bovendien was er rond de stand geen grote menigte aanwezig. Volgens de ADIV kan het incident dan ook weinig opschudding hebben veroorzaakt. Deze dienst sluit niet uit dat het enkel om een provocatie ging.

De ADIV heeft pas kennis genomen van het bestaan van de betwiste foto na de publicatie ervan in de pers. Deze dienst is opgetreden op verzoek van de toezichthoudende minister, die daarmee op zijn beurt gevolg gaf aan een aantal parlementaire vragen.

4. Samenvatting van het onderzoek

Het onderzoek heeft aangetoond dat de ADIV — uitzonderlijk — aanwezig was op een zogenaamd « open » evenement dat door een eenheid van Landsverdediging werd georganiseerd.

Het blijkt dat de ADIV de vliegmeeting bijwoonde om andere redenen dan om toezicht te houden op de stand « Soldiers of fortune ».

De beide agenten van de ADIV hebben niets opgemerkt met betrekking tot de aanwezigheid van betwiste voorwerpen of een samenscholing als gevolg van een incident. Ze sluiten echter niet uit dat er kortstondig opschudding is geweest. Wat hen betreft is het mogelijk voorkomen van een of andere manipulatie een werkhypothese, die echter niet door enige concrete elementen wordt gestaafd.

Eens ze *a posteriori* en via de pers kennis hadden gekregen van de feiten, en na de ondervraging van de minister van Landsverdediging, hebben ze niet alleen

Cette connaissance a fait que la demande d'autorisation de « Soldiers of fortune » introduite en 1998 n'a pas été relayée vers le SGR, puisqu'il s'agissait d'un « habitué » dont le stand n'avait précédemment provoqué aucun incident.

Vérification faite *a posteriori*, le responsable du stand n'était pas connu de la documentation du SGR, pas plus qu'il n'est ressorti d'une consultation ultérieure d'un service allié que l'intéressé aurait été en liaison avec l'extrême droite.

Il n'y a toutefois pas eu, à ce niveau, de consultation de la Sûreté de l'État, qu'il s'agisse du gérant du stand ou de l'organisation « Soldiers of fortune ».

Le SGR s'est montré catégorique sur l'absence de toute constatation par ses agents de la présence d'objets revêtus de sigles néo-nazis, contrairement au contenu d'une photo publiée dans la presse, montrant une personne cagoulée tendant une chope sur laquelle apparaît une croix gammée.

C'est cette absence de constatation qui explique pourquoi aucun rapport n'a été dressé quant à la présence d'activisme de ce type.

Il n'y a pas non plus eu de mouvement de foule aux abords du stand, de telle sorte que le SGR forme l'hypothèse que l'incident n'a pu en tout état de cause qu'être furtif, et n'exclut pas qu'il se soit agi d'une provocation.

Le SGR n'a pris connaissance de la photographie litigieuse qu'en raison de sa publication dans la presse et est intervenu à la suite de la demande du ministre de tutelle, résultant elle-même des questions parlementaires.

4. Synthèse de l'enquête

L'enquête a révélé que le SGR était — exceptionnellement — présent lors de l'une des manifestations « ouvertes » organisées par une unité de la Défense nationale.

Il appert que les raisons de la présence du SGR au meeting show étaient d'un autre ordre que la surveillance du stand « Soldiers of fortune ».

Les deux agents du SGR n'ont rien remarqué, qu'il s'agisse d'objets litigieux ou d'attroupement consécutif à un incident, mais ils n'excluent pas une survenance furtive. Pour leur part l'éventualité d'une manipulation reste une hypothèse de travail, que rien de concret n'a cependant étayé.

Informés *a posteriori* par la presse et à la suite de l'interrogation du ministre de la Défense nationale, ils ont cherché des informations tant internes qu'auprès

intern maar ook bij een geallieerde dienst inlichtingen ingewonnen over de standhouder en over de organisatie «Soldiers of fortune». Ze hebben echter geen elementen gekregen volgens dewelke de betrokkene of de organisatie met extreem-rechts in verband kunnen worden gebracht.

Voor het overige heeft het Comité I eind 1999 uit eigen initiatief een kort onderzoek gevoerd op het internet. Daarbij heeft het op het adres «http://www.sofmag.com» een site aangetroffen met een dertigtal pagina's, die een officiële vitrine lijkt te zijn van de «beweging» «Soldiers of fortune» maar die verder geen informatie geeft. Bij een snel onderzoek van de site in dezelfde periode werden er geen nazistische emblemen aangetroffen.

5. Conclusies

De ADIV heeft geen rapport opgemaakt over een mogelijk incident dat deze dienst niet persoonlijk heeft vastgesteld. Geen enkel element laat toe de informatie die in de pers verscheen te bevestigen of te ontkrachten.

De inlichtingen die de Dienst enquêtes van het Comité I heeft verzameld, zijn afkomstig van het verhoor van de agenten die ter plaatse een opdracht uitvoerden, alsook van de opzoekingen verricht naar aanleiding van de publicatie van foto's in de pers en van het verzoek daartoe van de minister van Landsverdediging.

Het onderzoek van het Comité I heeft aangetoond dat de ADIV slechts uitzonderlijk was betrokken bij de veiligheid van de activiteiten op de site van een «open» militaire eenheid, namelijk indien een of meer potentiële deelnemers voorkomen op de lijst van de organisaties die deze dienst in het oog houdt. Door twee agenten naar de basis van Kleine Brogel te sturen, heeft de ADIV zijn algemene opdracht vervuld.

Het Comité I stelt echter vast dat de ADIV in dit dossier noch de Veiligheid van de Staat noch de gerechtelijke overheden heeft geraadpleegd. Zonder daarom te beweren dat de inhoud van dit dossier dit contact met beide instanties noodzakelijk maakte, wil het Comité I er niettemin op wijzen, voor zover dienstig, dat de wet van 30 november 1998 het principe van een «zo doeltreffend mogelijke onderlinge samenwerking» heeft ingevoerd.

d'un service allié, à la fois sur le gérant du stand et sur l'organisation nommée «Soldiers of fortune» mais n'ont recueilli aucun élément susceptible de relier l'un ou l'autre à l'extrême droite.

Pour le surplus le Comité R a, fin 1999, brièvement parcouru d'initiative le web et a ainsi pu constater qu'à l'adresse suivante: «http://www.sofmag.com» résidait un site abritant une trentaine de pages et semblant constituer une vitrine officielle du «mouvement» «Soldiers of fortune» sans pour autant informer davantage. À l'époque un examen rapide du site n'avait pas permis d'y déceler la présence d'emblèmes à caractère nazi.

5. Conclusions

Le SGR n'a rédigé aucun rapport relatif à un possible incident qu'il n'a pas personnellement constaté. Rien ne permet donc de confirmer ni d'infirmer l'information véhiculée par la presse.

Les renseignements recueillis par le Service d'enquêtes du Comité R proviennent de l'audition des agents qui étaient en mission sur place et des quelques recherches effectuées à la suite de la parution de photos dans la presse et de la demande en ce sens formulée par le ministre de la Défense nationale.

L'enquête menée par le Comité R a permis d'apprendre que le SGR n'était qu'exceptionnellement concerné par la sécurité des activités s'exerçant sur le site d'une unité militaire «ouverte», soit lorsqu'un ou plusieurs participants potentiels appartiennent à la liste des organisations suivies par ce service. En dépêchant deux agents à Kleine Brogel, le SGR a donc satisfait à sa mission générale.

Le Comité R constate toutefois qu'en ce dossier, ni la Sûreté de l'État ni les autorités judiciaires n'ont été consultées par le SGR. Sans aller jusqu'à prétendre que le contenu de celui-ci rendait cette double démarche indispensable, il tient à rappeler ici, à toutes fins utiles, que la loi du 30 novembre 1998 a instauré le principe de «coopération mutuelle aussi efficace que possible».

D. Klachten en aangiften van en door particulieren

HOOFDSTUK 1

VERSLAG VAN HET TOEZICHTSONDERZOEK BETREFFENDE DE ADIV NAAR AANLEIDING VAN EEN KLACHT VAN EEN PARTICULIER

Krachtens artikel 37 van de wet van 18 juli 1991 houdende regeling van toezicht op de politie- en inlichtingendiensten en omwille van redenen van vertrouwelijkheidenbeschermingvanhetprivé-levenvanpersonen,heeftheVastComitéIbeslotenslechts een beknopt gedeelte te publiceren van het verslag (21 pagina's) dat aan de Senaat en aan de bevoegde minister werd toegezonden, zoals door voornoemde wet wordt voorzien in artikel 33, § 3.

1. Procédure

Op 29 april 1999 ontving het Vast Comité I een brief met een klacht van een lid van de Belgische Strijdkrachten.

De betrokkene schreef dat hij meende het slachtoffer te zijn geworden van misbruik door de Algemene Dienst inlichting en veiligheid van de Strijdkrachten (ADIV), ter gelegenheid van een controle van de veiligheid van het informaticasysteem bij de dienst waar hij was gedetacheerd.

De klager was ervan overtuigd dat zijn rechten niet waren gerespecteerd in een context waarin hij ertoe was gebracht ontslag te nemen uit zijn functies onder voorwaarden die hij onaanvaardbaar noemde.

Op 5 mei 1999 werd de klager uitvoerig verhoord door het Hoofd van de Dienst enquêtes van het Comité I, in het bijzijn van de Voorzitter van het Comité I. De klager bevestigde zijn klacht en verschafte daarbij heel wat toelichting.

Aangezien aanwijzingen van strafrechtelijke inbreuken naar voren leken te komen uit de feiten zoals de klager ze had beschreven, werd beslist de gerechtelijke overheden op de hoogte te brengen overeenkomstig artikel 29 van het Wetboek van strafvordering en artikel 46, lid 1 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten.

In deze fase, — er rekening mee houdend dat de feiten ter kennis waren gebracht van de gerechtelijke overheden — achtte het Comité I het niet opportuun, — teneinde niet tussen te komen in het strafonderzoek —, om al onmiddellijk een toezichtsonderzoek te openen. Het gaf er de voorkeur aan de resultaten van het gerechtelijk onderzoek af te wachten.

D. Plaintes de particuliers et dénonciations

CHAPITRE 1er

RAPPORT RELATIF À L'ENQUÊTE DE CONTRÔLE CONCERNANT LE SGR SUITE À LA PLAINTE D'UN PARTICULIER

En vertu de l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et pour des raisons tenant à la confidentialité ainsi qu'au respect de la vie privée des personnes, le Comité permanent R a décidé de ne publier ici qu'une partie succincte du rapport (21 pages) qui a été adressé au ministre compétent ainsi qu'au Sénat, comme la loi précitée le prévoit en son article 33, 3º alinéa.

1. Procédure

Le Comité R a reçu, le 29 avril 1999, une lettre contenant une dénonciation émanant d'un membre des Forces armées.

Dans cet écrit l'intéressé estimait avoir été abusé par le Service général de renseignement et de la sécurité des Forces armées (SGR) à l'occasion d'un contrôle de la sécurité du système informatique dans le service où il était détaché.

Il était convaincu que ses droits n'avaient pas été respectés dans un contexte où il avait été amené à démissionner de cette fonction particulière sous des conditions qu'il qualifiait d'inacceptables.

Le 5 mai 1999, le plaignant était entendu de manière circonstanciée par le chef du Service d'enquêtes du Comité R, en présence du président de celui-ci. À cette occasion, il a confirmé sa plainte en y apportant de nombreuses précisions.

Des indices d'infractions pénales semblant apparaître des faits tels que décrits par le plaignant, la décision fut prise d'en aviser les autorités judiciaires en application des articles 29 du Code d'instruction criminelle et 46, 1er alinéa, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

À ce stade, et vu cette transmission aux autorités judiciaires, le Comité R a estimé opportun, dans le but de ne pas interférer dans l'enquête pénale, de ne pas ouvrir immédiatement une enquête de contrôle et d'attendre pour ce faire les résultats des investigations judiciaires.

Krachtens artikel 40, derde lid, van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten werd dit onderzoek aan de Dienst enquêtes van het Comité I toevertrouwd. Dit gebeurde buiten elke controlebevoegdheid van het Vast Comité I, dat geen toegang kreeg tot de gegevens van het gerechtelijk dossier tijdens het onderzoek.

In augustus 1999 werd het strafonderzoek afgerond met « een beslissing van sepot bij gebrek aan elementen die een inbreuk vormen ».

Nadat de klager kennis had gekregen van het sepot van het gerechtelijk onderzoek, diende hij op 27 oktober 1999 opnieuw een vraag tot onderzoek in bij het Comité I. Daarbij herhaalde hij de aantijgingen van zijn eerste klacht (1).

Op 28 oktober 1999 besliste het Comité I dus een toezichtsonderzoek te openen.

Krachtens artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten kreeg de voorzitter van de Senaat op 29 oktober 1999 kennis van de opening van dit onderzoek.

Op dezelfde datum werd met een schrijven aan de bevoegde overheden, overeenkomstig artikel 38, § 2, van de voornoemde organieke wet van 18 juli 1991, de toelating gevraagd om het gerechtelijk dossier in te zien en stukken van dat dossier te kopiëren.

Deze toelating werd verleend per brief van 3 november 1999.

Overeenkomstig artikel 43.1 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten bracht het hoofd van de Dienst enquêtes van het Comité I de minister van Landsverdediging schriftelijk op de hoogte op 8 november 1999.

Op 15 maart 2000 bezorgde de Dienst enquêtes de resultaten van zijn onderzoeksverrichtingen, samen met het volledige dossier en de aanverwante stukken, aan het Comité I, dat aldus kennis kon nemen van de gerechtelijke kant van het onderzoek.

Op 30 november 2000 hadden twee leden van het Comité I een onderhoud met de klager.

Het Comité I heeft de openbare versie van dit verslag goedgekeurd op zijn plenaire vergadering van 6 maart 2001.

Het integrale verslag werd op 15 februari 2001 toegezonden aan de voorzitter van de Senaat en aan de bevoegde minister; het huidig verslag werd op 13 maart 2001 opgestuurd.

(1) Teneinde elk misverstand te voorkomen wijst het Comité I erop dat het niet de minste gerechtelijke bevoegdheid bezit en dat het verzoek van de klager bijgevolg niet kan worden geïnterpreteerd als een verzoek tot herziening van de beslissing van de gerechtelijke overheden.

Ces dernières furent confiées au Service d'enquêtes du Comité R en application de l'article 40, 3e alinéa, de la loi du 18 juillet 1991, organique du contrôle des Services de police et de renseignements, en dehors de toute compétence de contrôle du Comité R, qui n'a pas eu accès aux données du dossier judiciaire en cours de traitement.

L'information pénale aboutit en août 1999 à « une décision de classement sans suite par défaut d'éléments constitutifs d'infraction ».

Ayant été informé du classement sans suite de l'enquête judiciaire, le plaignant déposa, le 27 octobre 1999, une nouvelle demande d'enquête auprès du Comité R reprenant les mêmes termes que ceux de sa plainte initiale (1).

Par décision du 28 octobre 1999, le Comité R a donc ouvert une enquête de contrôle.

Conformément à l'article 32 de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991, l'ouverture de cette enquête a été notifiée, le 29 octobre 1999 à M. A. De Decker, président du Sénat.

Par courrier du même jour, et en application de l'article 38, § 2, de la loi organique du 18 juillet 1991 précitée, l'autorisation de consultation et de prise de copies des pièces du dossier judiciaire a été demandée aux autorités compétentes.

Cette autorisation a été accordée par courrier du 3 novembre 1999.

Le chef du Service d'enquêtes du Comité R a averti M. le ministre de la Défense nationale par courrier du 8 novembre 1999, conformément à l'article 43.1 de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements.

Le Service d'enquêtes a transmis le 15 mars 2000 les résultats de ses investigations, ainsi que l'ensemble du dossier contenant les pièces y afférentes, au Comité R qui a ainsi pu prendre connaissance du versant judiciaire de l'enquête.

Deux membres du Comité R ont eu un entretien avec le plaignant en date du 30 novembre 2000.

La version publique du présent rapport a été approuvée par le Comité R lors de sa réunion plénière du 6 mars 2001.

La version intégrale du rapport a été envoyée au ministre de la Défense nationale et au président du Sénat le 15 février 2001. Le présent rapport leur a été envoyé le 13 mars 2001.

(1) Pour éviter toute confusion, le Comité R rappelle qu'il n'a aucune compétence judiciaire et que la requête du plaignant ne peut donc s'entendre comme une demande de révision de la décision des autorités judiciaires.

Op 25 april 2001 heeft de minister van Landsverdediging het Comité I laten weten dat hij akkoord ging met de publicatie van dit verslag.

2. Besluiten en aanbevelingen

2.1. Het Comité I wijst er op dat, voorafgaand aan de opening van het toezichtsonderzoek, de gerechtelijke overheden oordeelden dat de in de klacht beschreven feiten geen strafrechtelijke inbreuken vormden ten laste van leden van de Algemene Dienst inlichting en veiligheid, en dat, op basis van deze en navolgende vaststellingen die werden gedaan door het toezichtsorgaan, geen enkele inbreuk kon worden vastgesteld op de rechten die de Grondwet en de wet aan de personen waarborgen (1).

2.2. De organieke wet van 30 november 1998 voorziet voor de ADIV een aantal opdrachten waartoe, naast het aspect inlichtingen, ook behoort: «de bescherming van de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert».

Voor het Vast Comité I en voor de huidige leiding van de ADIV is het duidelijk dat al deze opdrachten, teneinde tegelijk de doeltreffende werking van de diensten en de bescherming van de fundamentele rechten van de burgers te verzekeren, nood hebben aan het uitwerken van een aanvullend wettelijk kader dat voldoende duidelijk en precies is om het mogelijk te maken, met name in de context van de veiligheid inzake informatica, elke poging van indringing in de computersystemen van de Strijdkrachten en van het ministerie van Landsverdediging te identificeren en te neutraliseren, zonder daarbij op enige wijze inbreuk te maken op de bevoegdheden van de gerechtelijke overheden.

Het Vast Comité I wijst regelmatig op de noodzaak de inlichtingen- en veiligheidsdiensten ruimere wettelijke bevoegdheden toe te kennen, uit te rusten met performant materieel en met meer gespecialiseerd personeel.

De enige reden daarvoor is de betrokken diensten toe te laten een hoger niveau van efficiëntie te bereiken dan het niveau waarop ze zich vandaag bevinden. Dit dossier, waarin het Comité I op elke regel heeft gepoogd een onderscheid te maken tussen subjectieve verklaringen enerzijds en bewijzen anderzijds, zonder ooit partij te kiezen voor een van de aangevoerde stellingen, heeft de grote verdienste gehad de aandacht van het Comité I te vestigen op de risico's die kunnen opduiken wanneer de zaken uit de hand lopen bij het

(1) *Cf.* artikel 1 van de wet van 18 juli 1991 houdende regeling van het toezicht op de politie- en inlichtingendiensten.

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il était d'accord pour la publication de ce rapport.

2. Conclusions et recommandations

2.1. Le Comité R souligne que les autorités judiciaires n'ont décelé aucun élément constitutif d'infraction pénale dans les faits rapportés par le plaignant à charge des membres du SGR et que, sur cette base ainsi que sur celles des constatations ultérieures de l'organe de contrôle, aucune violation par ce service des droits que la Constitution et la loi confèrent aux personnes n'a été relevée (1).

2.2. La loi organique du 30 novembre 1998 prévoit pour le SGR une série de missions parmi lesquelles, outre l'aspect du renseignement, on trouve: «la protection des systèmes informatiques et de communications militaires ou ceux que le ministre de la défense nationale gère».

Il est clair pour le Comité R, comme pour l'actuelle direction du SGR, que toutes ces missions nécessitent, pour garantir à la fois l'efficacité des services et la protection des droits fondamentaux des citoyens l'élaboration d'un cadre légal complémentaire suffisamment clair et précis pour permettre, notamment dans le contexte de la sécurité informatique, d'identifier et de neutraliser toute tentative d'intrusion dans les systèmes des Forces armées ou du ministère de la Défense nationale, sans empiéter, d'aucune manière sur les compétences propres des autorités judiciaires.

Le Comité R rappelle régulièrement la nécessité de doter les services de renseignement et de sécurité de compétences légales élargies, de matériel performant et de davantage de personnel spécialisé.

La raison n'est autre que de permettre à ces services de se hisser à un niveau d'efficacité supérieur à celui qu'ils sont actuellement susceptibles de mettre en œuvre. Le présent dossier, pour lequel le Comité R a cherché à chaque ligne à faire la part du subjectif et de l'avéré, sans jamais prendre parti pour l'une ou l'autre des thèses en présence, a eu le grand mérite d'attirer son attention sur les risques liés à des dérapages potentiels dans l'utilisation de méthodes de travail proches de celles de la police et qui pourraient mettre

(1) *Cf.* l'article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

gebruik van werkmethodes nauwverwant met deze van de politie en die de vrijheden en de fundamentele rechten van de burgers in gevaar zouden kunnen brengen.

Natuurlijk moet de perfectionering van de middelen gepaard gaan met een perfectionering van de controle op het gebruik van die middelen. Men kan immers niet betwisten dat inbreuken en de schade aangericht door de eventuele slechte werking van performante middelen nog veel ergere gevolgen kunnen hebben.

In deze optiek raadt het Vast Comité I aan de toekenning door de wetgever van bijkomende middelen aan de inlichtingen- en veiligheidsdiensten te laten samenvallen met een passende en doeltreffende controle op het gebruik van die middelen.

2.3. Tot slot kan het Comité I niet anders dan vaststellen dat geen enkel dossier van dit onderzoek werd bewaard in het archief van de ADIV. Een dergelijke procedure is zeker strijdig met de geest van de wet van 18 juli 1991 en komt er in de praktijk op neer dat elke latere controle wordt belemmerd of zelfs verhinderd.

Bij gebrek aan een volledig en geïnventariseerd dossier kan het Comité I er zich *a posteriori* niet van vergewissen dat, *in tempore non suspecto*, de handelwijze van de leden van de inlichtingendiensten paste binnen het wettelijk kader van de specifieke opdrachten van een dergelijke dienst.

HOOFDSTUK 2

Verslag betreffende de aangifte door een particulier van vermeende disfuncties bij de Veiligheid van de Staat

1. De procedure

Op zijn verzoek werd de klager verhoord door de Dienst enquêtes van het Comité I op 24 januari 2000.

In essentie deelde hij mee dat hij sedert begin 1998 informatie had gegeven aan een van de locale secties van de Veiligheid van de Staat en dat na ongeveer twee jaar van samenwerking hieraan een einde werd gesteld op bevel van de centrale zetel van deze administratie te Brussel. Hij meende dat deze beslissing het gevolg was van het hinderend karakter van bepaalde door hem geleverde gegevens.

In opvolging van deze aangifte besloot het Vast Comité I op 26 januari 2000 een toezichtsonderzoek te openen.

Bij toepassing van artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten, werd de voorzitter van de Senaat op 4 februari 2000 op de hoogte gebracht van de opening van het onderhavig onderzoek.

en péril les libertés et les droits fondamentaux des citoyens.

Il va de soi que le perfectionnement de l'outil doit aller de pair avec un perfectionnement du contrôle de l'usage de celui-ci. Il est en effet incontestable que les atteintes et les dommages occasionnés par un éventuel dysfonctionnement d'un outil performant seront d'autant plus conséquents.

Dans cette optique, le Comité R recommande dès lors de doubler l'attribution par le législateur de moyens complémentaires aux services de renseignement et de sécurité d'un contrôle adéquat et effectif en matière d'usage de ces moyens.

2.3. Enfin, le Comité R ne peut que constater qu'aucun dossier de cette enquête informatique n'était conservé dans les archives du SGR. Une telle procédure est bien certainement contraire à l'esprit de la loi du 18 juillet 1991 et est en pratique de nature à entraver et même à empêcher tout contrôle ultérieur.

En l'absence d'un dossier complet et inventorié, le Comité R ne peut en effet s'assurer *a posteriori* qu'*in tempore non suspecto* le comportement des membres des services de renseignement s'inscrivaient bien dans le cadre légal des missions spécifiques d'un tel service.

CHAPITRE 2

Rapport concernant la dénonciation par un particulier de dysfonctionnements présumés à la Sûreté de l'État

1. Procédure

À sa demande le plaignant fut entendu par le Service d'enquêtes du Comité R le 24 janvier 2000.

Il relata en substance que depuis le début de 1998, il avait fourni occasionnellement des informations à l'une des sections locales de la Sûreté de l'État et qu'après environ deux années de collaboration, il venait d'être mis fin à cette dernière sur ordre du siège central de cette administration à Bruxelles. Il estimait que cette décision résultait du contenu de certaines informations dérangeantes qu'il avait transmises.

Suite à cette déposition, le Comité R a décidé le 26 janvier 2000 d'ouvrir une enquête de contrôle.

En application de l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le président du Sénat a été averti de l'ouverture de la présente enquête par courrier du 4 février 2000.

Op dezelfde datum werd eveneens een kantschrift gericht aan het hoofd van de Dienst enquêtes van het Comité I.

In toepassing van artikel 43, § 1, van voornoemde wet, bracht het diensthoofd op 7 februari 2000 de minister van Justitie op de hoogte van de opening van het toezichtsonderzoek.

De Dienst enquêtes van het Comité I sloot zijn onderzoek af door middel van een verslag van zijn vaststellingen op 30 maart 2000.

Het Comité I gaf zijn goedkeuring aan het onderhavige verslag op 23 januari 2001.

Op 1 februari 2001 werd het advies van de minister van Justitie gevraagd.

Op 4 april 2001 liet de minister van Justitie weten dat hij, op basis van een nota van de Veiligheid van de Staat, niet instemt met de aanbeveling van het Comité I om het gebruik van informanten door de Veiligheid van de Staat te regelen door een algemene wetgeving.

Le même jour une apostille était adressée au chef du Service d'enquêtes du Comité R.

Celui-ci, en application de l'article 43, § 1, de la loi précitée, a avisé le ministre de la Justice de l'ouverture de l'enquête de contrôle en date du 7 février 2000.

Le Service d'enquêtes du Comité R a clôturé son enquête par un compte-rendu de ses constatations dressé le 30 mars 2000.

Le Comité R a approuvé le présent rapport en date du 23 janvier 2001.

Le 4 avril 2001, le ministre de la Justice, se basant sur une note de la Sûreté de l'État, faisait savoir qu'il ne partageait pas la recommandation du Comité R de réglementer par une législation générale l'utilisation d'informateurs par la Sûreté de l'État.

2. De elementen van de aangifte

De klager, die actief is binnen de georganiseerde misdaad, zou bepaalde recente gegevens hebben geleverd aan een buitenlandse inlichtingendienst. Bij die gelegenheid zou hij hebben vernomen dat hij in België in een slecht daglicht stond. Nadere gegevens werden hem niet meegedeeld.

Enige tijd later moest hij evenwel vaststellen dat de leden van de Veiligheid van de Staat, waarmee hij gewoonlijk in contact stond, hem ervan verwittigden dat ze een einde moesten maken aan de samenwerking, vermits de betrokkene geen goede reputatie genoot op de zetel van de Veiligheid van de Staat te Brussel.

De betrokkene veronderstelt dat deze beslissing het gevolg was van gegevens die hij had meegedeeld, en die betrekking hadden op verdachte banden tussen verschillende personen waarvan bepaalde volgens hem behoorden tot de zakenwereld en tot de wereld van de inlichtingendiensten.

Hij had overwogen zich tot de pers te wenden doch besloot uiteindelijk het Comité I op de hoogte te stellen van de feiten die, volgens hem, wezen op een disfunctie bij de Veiligheid van de Staat.

Verder preciseerde hij in het bezit te zijn van nieuwe, belangwekkende informatie voor de dienst, maar deze niet meer aan zijn normale contactpersonen te kunnen doorgeven, gezien zij het risico liepen een sanctie te krijgen of zelfs overgeplaatst te worden.

2. Les éléments de la plainte

Le plaignant, qui situe son action dans la sphère des activités de la criminalité organisée, aurait fourni certaines informations récentes à un service étranger. Il aurait appris à cette occasion qu'il était présenté sous un jour négatif en Belgique. Il ne lui fut pas fourni davantage de précision.

Il dut toutefois constater que, quelque temps plus tard, les membres de la Sûreté avec lesquels il était normalement en contact l'avertissaient qu'il devait mettre un terme à leur relation, étant donné que l'intéressé ne jouissait pas d'une bonne réputation au siège de la Sûreté de l'État à Bruxelles.

Le plaignant supposait que cette décision était la conséquence d'informations qu'il avait communiquées et qui mettaient en lumière des relations suspectes entre diverses personnes dont certaines appartenant, d'après lui, au monde des affaires et au monde du renseignement.

Il avait pensé s'adresser à la presse, mais finalement avait décidé d'informer le Comité R s'agissant pour lui de faits qui montraient des dysfonctionnements au sein de la Sûreté de l'État.

Il précisait encore être en possession de nouvelles informations intéressantes pour ce service, mais ne pouvoir les transmettre à ses contacts habituels sous peine de leur faire courir le risque d'être sanctionnés ou même déplacés.

3. Het onderzoek

3.1. Bepaalde algemene regels met betrekking tot het omgaan met informanten

In het kader van dit onderzoek werden er gesprekken gevoerd tussen de Dienst enquêtes van het Comité I, de directeur operaties van de Veiligheid van de Staat, de verantwoordelijke van de betreffende locale sectie van de Veiligheid van de Staat en de twee betrokken leden van deze dienst.

Bij deze gelegenheden werden bepaalde, algemene regels aangaande de omgang met informanten in herinnering gebracht.

Aldus kan een persoon geen informant zijn, indien hij een gerechtelijk verleden heeft, hij voor een andere inlichtingendienst werkt, of als blijkt dat de door deze persoon geleverde informatie onbetrouwbaar is.

Deze drie criteria staan niet expliciet vermeld in een dienstnota. Wel dient men hier te benadrukken dat ze dateren uit een periode dat de Veiligheid van de Staat niet uitdrukkelijk als taak had zich bezig te houden met de georganiseerde misdaad, en daardoor dus — per definitie —, niet in contact stond met het misdaadmilieu.

Heden is deze toestand gewijzigd, vermits artikel 7 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten de Veiligheid van de Staat belast heeft met de opdracht van «(...) 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 bedreigt of zou kunnen bedreigen (...)».

Artikel 8 van dezelfde wet definieert op zijn beurt «(...) een activiteit die bedreigt of zou kunnen bedreigen (...)» als: «(...) elke individuele of collectieve activiteit ontplooid in het land of vanuit het buitenland die verband kan houden met (...), criminele organisaties, (...)».

Binnen deze nieuwe context leek het dus essentieel voor de hiërarchie van de Veiligheid van de Staat om het criterium aangaande het gerechtelijk verleden soepeler toe te passen. Desalniettemin wordt er nog steeds voorgehouden om personen met gerechtelijke antecedenten niet officieel in te schrijven als betaalde informanten, maar — naar gelang het geval —, te erkennen dat dergelijke personen occasionele informatie kunnen doorgeven.

De beoordelingscriteria en de modaliteiten voor de behandeling van dit soort occasionele informaties, maken het voorwerp uit van een volgend onderzoek.

3. L'enquête

3.1. Certaines règles générales concernant l'utilisation d'informateurs

Dans le cadre de cette enquête des échanges de vue ont eu lieu entre le Service d'enquêtes du Comité R, le directeur des opérations de la Sûreté de l'État, le responsable de la section locale de la Sûreté de l'État et les deux membres concernés de ce service.

À ces occasions, certaines règles générales concernant le recours à des informateurs ont été rappelées.

C'est ainsi qu'une personne ne peut être informateur répertorié si elle a des antécédents judiciaires, si elle travaille pour un autre service de renseignements, s'il apparaît que les informations fournies par cette personne ne sont pas fiables.

Ces trois critères ne se trouvent pas repris explicitement dans une note de service. Il faut souligner qu'ils datent d'une période où la Sûreté de l'État n'avait pas pour mission explicite de s'occuper de la criminalité organisée et n'était donc pas, par définition, en contact avec le milieu délinquant.

Cette situation est différente aujourd'hui, en ce sens que l'article 7 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité a attribué à la Sûreté de l'État la mission «de rechercher, d'analyser et de 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 ...».

L'article 8 de la même loi définit pour sa part «l'activité qui menace ou pourrait menacer (...)» comme étant notamment «toute activité individuelle ou collective, déployée à l'intérieur du pays ou à partir de l'étranger, qui peut avoir un rapport avec (...) les organisations criminelles, (...)».

Dans ce nouveau contexte, il apparaissait donc essentiel pour la hiérarchie de la Sûreté de l'État d'assouplir l'application du critère relatif aux antécédents judiciaires. Il est toutefois toujours proposé de ne pas inscrire officiellement comme informateur rémunéré les personnes ayant des antécédents judiciaires, mais d'admettre éventuellement, en fonction du cas, que ces personnes puissent fournir des informations occasionnelles.

Les critères d'appréciation et les modalités de traitement de ces informations occasionnelles de cette espèce feront l'objet d'une prochaine enquête.

3.2. De toepassing van deze criteria op het onderhavige geval

3.2.1. De context

De eerste contacten van de Veiligheid van de Staat met deze informant dateren van maart 1998. Ze kwamen tot stand ingevolge informaties die aan onze inlichtingendienst werden overgemaakt door de inlichtingendienst van een ander Europees land. Deze informaties sloegen op activiteiten van wapenhandel die in verband stonden met een terroristische groepering.

Bij deze gelegenheid maakte de betrokkene gewag van zijn talrijke contacten, zowel met inlichtingendiensten als politiediensten doorheen gans Europa en de rest van de wereld. Hij onthulde tevens contacten gehad te hebben in het misdaadmilieu en problemen te kennen op gerechtelijk vlak.

Deze laatsten waren volgens hem te wijten «aan zijn inlichtingsactiviteiten». In verband met de genoemde feiten van wapenhandel, verklaarde de betrokkene dat men hem had verzocht op te treden als tussenpersoon. Daartoe moest hij kunnen beschikken over middelen om zich naar het buitenland te begeven en er een contactpersoon te ontmoeten.

Gezien zijn problemen met het gerecht, diende hij eveneens te kunnen beschikken over een nieuwe identiteit en een nieuw paspoort. Hij vroeg dus aan de Veiligheid van de Staat om hem daarbij te helpen.

Blijkbaar had hij zijn verhaal reeds bij andere inlichtingendiensten gedaan, maar zonder al te veel succes. Dit had hem ertoe gebracht zich te wenden tot de ambassade van het land waarvan de inlichtingendienst de Veiligheid van de Staat op de hoogte had gebracht.

3.2.2. De eerste controles uitgevoerd door de Veiligheid van de Staat

Uit de gerechtelijke antecedenten van de betrokkene bleek dat hij van 1993 tot 1998 verscheidene veroordelingen had opgelopen voor financiële delicten (valsheid in geschrifte, afpersing, misbruik van vertrouwen, ...).

Uit controles, die werden uitgevoerd bij buitenlandse inlichtingendiensten en nationale politiediensten, kwam aan het licht dat de gegevens die door de betrokkene waren overgemaakt grotendeels onjuist bleken en voor een ander gedeelte reeds bij de autoriteiten bekend waren.

3.2. L'application de ces critères au cas d'espèce

3.2.1. Le contexte

Les premiers contacts de la Sûreté de l'État avec l'informateur remontent au mois de mars 1998. Ces contacts ont été initiés suite à des informations communiquées à notre service de renseignement par le service d'un autre pays européen concernant des activités de trafic d'armes en relation avec un groupement terroriste.

À cette occasion, l'intéressé a fait état de ses nombreux contacts aussi bien avec des services de renseignement qu'avec des services de police, dans toute l'Europe et dans le reste du monde.

Il a révélé avoir également des contacts au sein du milieu criminel et connaître des problèmes sur le plan judiciaire à attribuer d'après lui, «à ses activités de renseignement». En rapport avec les faits précis de trafic, l'intervenant déclara avoir été sollicité pour servir d'intermédiaire. Pour cela, il devait disposer de moyens pour se rendre à l'étranger et rencontrer une personne de contact.

Vu ses problèmes judiciaires, il devait également disposer d'une nouvelle identité et d'un nouveau passeport. Il demandait donc l'aide de la Sûreté de l'État.

Il avait apparemment fait le même récit à d'autres services de renseignement, mais sans grand succès. Cela l'avait amené à s'adresser à l'ambassade du pays dont le service de renseignement avait averti la Sûreté de l'État.

3.2.2. Les premières vérifications faites par la Sûreté de l'État

Les antécédents judiciaires de l'intervenant ont montré qu'il avait encouru, de 1993 à 1998, de nombreuses condamnations principalement pour des faits de délinquance financière (faux en écritures, escroquerie, abus de confiance, ...).

Des vérifications faites auprès de services de renseignement étrangers et auprès des services de police nationaux, il est apparu que les informations fournies par le plaignant étaient pour une grande partie inexactes et pour une autre partie déjà connues des autorités.

In één geval moesten deze gegevens de betrokkene voornamelijk helpen aan een visum om naar België te kunnen terugkeren (1).

Door het natrekken van deze gegevens kon de Veiligheid van de Staat in verband met deze zaak op 12 maart 1998 een gedetailleerd verslag voorleggen aan de minister van Justitie en de nationale magistraat.

In de conclusie van haar nota vermeldde de Veiligheid van de Staat het volgende:

«Gelet op de voorgeschiedenis van E. kunnen we ervan uitgaan dat hij een aantal elementen verbonden heeft tot een verhaal. Hij poogt op grond hiervan een aantal dingen te bekomen: geld, een wagen en vervalste identiteitsbewijzen. Deze zouden door de Veiligheid van de Staat of een politiedienst ter beschikking moeten gesteld worden.

De Veiligheid van de Staat zal hierop niet ingaan; deelt U wat voorafgaat tot alle nuttige doeleinden mee en zal, indien zich geen nieuwe elementen aandienen, ter zake geen verder gevolg eraan geven.»

De Veiligheid van de Staat vernam vervolgens dat de buitenlandse zusterdienst (2) uiteindelijk de reis van de informant had kunnen organiseren opdat hij de contactpersoon zou kunnen ontmoeten. Tijdens dat verblijf in het buitenland was er geen enkele ontmoeting. Het dossier werd door de Veiligheid van de Staat derhalve niet meer opgevolgd.

Op 16 april 1998 werd aan de locale sectie het verbod opgelegd om nog verder contact te onderhouden met de betrokkene.

3.2.3. De andere informaties en het gevolg dat door de Veiligheid van de Staat aan de zaak werd gegeven

De betrokkene poogde niettemin bij herhaling opnieuw contact te leggen met de lokale sectie van de Veiligheid van de Staat, door op eigen initiatief en occasioneel gegevens over verschillende zaken in verband met de georganiseerde misdaad door te spelen.

Telkens bleken deze bij de Veiligheid van de Staat reeds bekend of ongegrond te zijn.

(1) Deze informatie sloeg op een handel in kinderen en een zekere «Marc» uit Charleroi.

(2) Zie onder punt 3.2.1.

Dans un cas, ces informations devaient principalement permettre à l'intéressé d'obtenir un visa pour pouvoir revenir en Belgique (1).

Ces vérifications ont permis à la Sûreté de l'État d'adresser, le 12 mars 1998, un rapport circonstancié au ministre de la Justice, ainsi qu'au magistrat national concernant cette affaire.

En conclusion de cette note la Sûreté de l'État mentionnait ce qui suit:

«Vu les antécédents de E., nous pouvons conclure qu'à l'aide de plusieurs éléments il construit un récit. Au départ de ce dernier, il tente alors d'obtenir certaines choses: de l'argent, un véhicule et de faux documents d'identité. Ceux-ci devraient être mis à sa disposition par la Sûreté de l'État ou par un service de police.

La Sûreté de l'État ne va pas s'engager plus avant dans cette affaire; ce qui précède est communiqué à toutes fins utiles et restera sans aucune suite, sauf survenance d'éléments nouveaux.»

La Sûreté de l'État apprit par la suite que le service homologue étranger mentionné (2) avait finalement pu organiser le voyage de l'informateur, dans le but qu'il puisse rencontrer la personne de contact. Durant le séjour de l'intéressé, aucune rencontre ne se réalisa. Ce dossier ne fut donc pas davantage suivi par la Sûreté de l'État.

Le 16 avril 1998 l'interdiction d'entretenir le suivi des contacts avec le plaignant était signifiée à la section locale.

3.2.3. Les autres informations et le suivi de l'affaire par la hiérarchie de la Sûreté de l'État.

Le plaignant tenta cependant à plusieurs reprises de renouer les contacts avec la section locale de la Sûreté de l'État, en fournissant d'initiative et occasionnellement des informations concernant plusieurs affaires en relation avec la criminalité organisée.

À chaque fois celles-ci se révélèrent déjà connues de la Sûreté ou bien sans fondement.

(1) Ces dernières informations faisaient état de trafic d'enfants et d'un certain «Marc» de Charleroi.

(2) Voir point 3.2.1.

De minister van Justitie, de nationale magistraat en de territoriaal bevoegde procureur-generaal werden van deze nieuwe inlichtingen op de hoogte gesteld door middel van een verslag van de Veiligheid van de Staat daterend van 1 oktober 1999.

De conclusie van dit verslag maakt melding van het weinig betrouwbare karakter van de bron en onderstreept zijn gevaarlijk karakter. Men had zich inderdaad rekenschap gegeven van het feit dat de betrokkene valselijk gegevens had bevestigd die indirect reeds van hemzelf afkomstig waren, en die dus reeds via een andere persoon ter ore van de agenten van de Veiligheid van de Staat waren gekomen. Er worden twee concrete voorbeelden gegeven om het gevaar van dergelijke manipulaties te illustreren.

De Veiligheid van de Staat bevestigt derhalve haar intentie om definitief een einde te stellen aan alle contacten met de heer E.

Op 25 februari 2000 werd evenwel een nieuwe informatienota toegezonden aan de minister van Justitie, de Nationale Magistraat en aan de territoriaal bevoegde procureur-generaal, aangaande door de betrokkene aangebrachte feiten die dateerden van mei 1999, en die verband hielden met georganiseerde criminaliteit. Opnieuw werd de nadruk gelegd op het weinig betrouwbare karakter van de informant.

In verband met deze aangelegenheid dient tevens vermeld te worden dat het hoofd van de locale sectie een vermaning kreeg wegens het niet strikt navolgen van de inhoud van de nota van 16 april 1998, die hem opdroeg «geen verder contact met de heer E. meer te zoeken, zelfs niet onder het mom van occasionele informaties.»

3.2.4. Het standpunt van de agenten op het terrein

Deze agenten werden gehoord door de Dienst Enquêtes van het Comité I aangaande hun persoonlijke indruk over de informant.

Zij bevestigden zeker te zijn dat de betrokkene niet 100 % betrouwbaar was, maar voegden er evenwel aan toe dat hij ook nuttige informatie had overgemaakt.

Volgens hen was het niet ondenkbaar dat deze informatie aan de basis had gelegen van goede resultaten die door andere nationale diensten waren geboekt. Ze haalden in dit verband een voorbeeld aan.

Ze zijn dus nog steeds geneigd om te denken dat de betrokkene op termijn zijn nut voor de dienst had kunnen bewijzen op het vlak van de georganiseerde misdaad, op voorwaarde dat hij zou zijn behandeld en gevolgd door ervaren personen, en dat de door hem geleverde informatie aan een rigoureuze controle zou zijn onderworpen.

Le ministre de la Justice, le magistrat national, ainsi que le procureur général territorialement compétent ont été mis au courant de ces nouveaux renseignements par un rapport de la Sûreté de l'État du 1er octobre 1999.

En conclusion, ce rapport rappelle le caractère peu fiable de la source et souligne son caractère dangereux. On s'est en effet aperçu à ce moment que l'intéressé confirmait faussement des informations qui provenaient déjà indirectement de lui-même et qui avaient ainsi déjà été portées à la connaissance des agents de la Sûreté par une autre personne. Deux exemples concrets sont donnés pour illustrer le danger de telles manipulations.

La Sûreté de l'État confirme donc son intention de mettre définitivement un terme à tous les contacts avec monsieur E.

Le 25 février 2000, une nouvelle note d'information fut toutefois adressée au ministre de la Justice, au magistrat national ainsi qu'au procureur général territorialement compétent concernant des informations communiquées en mai 1999 par le plaignant relativement à des faits de criminalité organisée. Une nouvelle fois, le peu de confiance que l'on pouvait accorder à l'informateur était souligné.

Il faut noter à ce sujet que le chef de la section locale reçut une réprimande pour ne pas avoir tenu strictement compte du contenu de la note du 16 avril 1998 qui donnait comme instruction «de ne plus chercher à avoir de contacts avec monsieur E. même dans le contexte d'informations occasionnelles».

3.2.4. Le point de vue des agents sur le terrain

Ces agents furent entendus par le Service d'enquêtes du Comité R concernant leur impression personnelle au sujet de l'informateur.

Il confirmèrent certes que l'intéressé n'était pas fiable à 100 % tout en ajoutant cependant que le plaignant avait aussi apporté des informations utiles.

Il n'était pas impensable d'après eux que celles-ci aient d'ailleurs été à l'origine des résultats positifs enregistrés par d'autres services nationaux. Ils citent un exemple à ce sujet.

Ils continuent donc de penser que l'intéressé aurait pu démontrer à terme son utilité pour le service en matière de criminalité organisée, à condition qu'il ait été traité et suivi par des personnes expérimentées et que ses informations aient été soumises à un contrôle très approfondi.

Het is dus duidelijk dat er in het onderhavige geval een verschil van mening bestaat tussen de agenten van het terrein en de directie «Operaties».

4. Conclusies en aanbevelingen

4.1. Uit het onderzoek bleek dat in het onderhavige geval de drie criteria die gewoonlijk door de Veiligheid van de Staat worden gehanteerd om een einde te stellen aan contacten met informanten waren vervuld.

De betrokkene had niet enkel een geladen gerechtelijk verleden maar werkte bovendien, en naar eigen zeggen, voor andere inlichtingendiensten en had informatie geleverd die ofwel weinig waardevol was gebleken omdat ze reeds gekend was, ofwel weinig betrouwbaar en waarschijnlijk gebruikt met het oog op manipulatie.

De beslissing om elk contact met de informant te verbreken werd voornamelijk genomen om toekomstige problemen te vermijden. Georganiseerde misdaad is voor de Veiligheid van de Staat een nieuwe materie en men kan begrijpen dat op dit vlak de grootste voorzichtigheid geboden is.

De aanwerving van informanten uit het misdaadmilieu heeft reeds tot ernstige disfuncties geleid binnen andere, gespecialiseerde diensten in het kader van recente zaken (onder andere door corruptie). De risico's die hieraan zijn verbonden versterken deze benadering dus nog.

4.2. Het is evenwel ook zo dat, geconfronteerd met de nieuwe opdracht die artikel 8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten oplegt aan de Veiligheid van de Staat, de hiërarchie van deze dienst er zich van bewust is dat de strikte toepassing van het criterium aangaande het bestaan van een gerechtelijk verleden om de samenwerking met een informant uit te sluiten, dient te worden herzien en versoepeld.

Ze stelt ongetwijfeld ook hoge eisen aan het aanpassingsvermogen van de met het inwinnen van informatie belaste agenten.

Op het principiële vlak getuigt het inderdaad niet van veel realisme om te pogen op een efficiënte wijze de nieuwe opdracht uit te voeren door enkel informatie te zoeken en in te winnen bij personen zonder een gerechtelijk verleden. Dergelijke informatie zou slechts veelal op het randgebeuren slaan.

Overigens zal de afwezigheid van een gerechtelijk verleden slechts een zwakke garantie bieden, gezien het zuiver formele karakter hiervan. Kan men, per definitie, de informant met een blanco strafregister beschouwen als een onberispelijk persoon? Is hij volkomen te vertrouwen? Is hij in wezen de «ideale»

Il est donc évident qu'une divergence de conception se manifeste au travers du cas d'espèce entre les agents du terrain et la direction des opérations.

4. Conclusions et recommandations

4.1. Il est apparu de l'enquête qu'en l'espèce les trois critères habituels pris en compte par la Sûreté de l'État pour mettre fin à tous les contacts avec l'informateur étaient rencontrés.

L'intéressé avait non seulement un passé judiciaire chargé, mais il travaillait de surcroît — d'après ses dires — pour d'autres services de renseignement et ses informations s'étaient révélées soit de peu de valeur parce que déjà connues, soit peu fiables et suspectes d'être utilisées à des fins de manipulation.

La décision de mettre fin à tout contact avec l'informateur a été prise principalement pour éviter des problèmes dans l'avenir. La matière concernant la criminalité organisée est neuve pour la Sûreté de l'État et l'on peut comprendre que la plus grande prudence en ce domaine se soit imposée.

Les risques liés au recrutement d'informateurs appartenant au milieu délinquant qui a déjà entraîné de très graves dysfonctionnements dans d'autres services spécialisés à l'occasion d'affaires récentes (entre autres des faits de corruption), renforcent bien certainement cette approche.

4.2. Il n'en reste pas moins vrai que face à la mission nouvelle que l'article 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité attribue à la Sûreté de l'État, la hiérarchie de ce service est consciente que l'application stricte du critère relatif à l'existence d'antécédents judiciaires pour exclure le travail avec un informateur doit être revue et assouplie.

Elle impose sans doute également dans le chef des agents chargés de recueillir l'information une grande capacité d'adaptation.

Sur le plan des principes, il est peu réaliste en effet d'envisager de répondre le plus efficacement possible à cette nouvelle mission en ne recherchant et en ne recueillant seulement que des informations provenant de personnes sans antécédent judiciaire. De tels renseignements ne pourraient concerner le plus souvent que des informations périphériques.

Par ailleurs, l'absence d'antécédent judiciaire ne constitue qu'une ébauche de garantie, eu égard à son caractère purement formel. Peut-on, par définition, considérer l'informateur dont le casier judiciaire est vierge comme une personne exempte de reproche? Sa fiabilité est-elle totale? Est-il par essence l'infor-

informant? Een persoon zal als informant enkel van nut blijken door zijn connecties met het milieu.

Criteria die enkel en alleen gebaseerd zijn op het voorzichtigheidsprincipe kunnen derhalve niet worden weerhouden zonder het risico te lopen zich af te sluiten van belangrijke informatiebronnen in deze zeer gevoelige materie rond criminele organisaties.

Er dient overigens op gewezen dat in andere, meer traditionele actievelden van de agenten van de buitendiensten van de Veiligheid van de Staat, dezelfde risico's die inherent zijn aan het aanwerven van informanten, reeds bestonden. Denken we hierbij maar aan de materie van het extremisme en die van het terrorisme.

Anderzijds is het niet steeds gemakkelijk om een duidelijke en precieze lijn te trekken tussen de andere wettelijke opdrachten die aan de inlichtingendiensten werden toevertrouwd en deze die specifiek aan de Veiligheid van de Staat werden toebedeeld betreffende de bedreiging op verschillende vlakken vanwege misdaadorganisaties.

Artikel 8, *f)*, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten stelt aangaande dit onderwerp duidelijk «die destabiliserende gevolgen kunnen hebben op het politiek- en sociaal-economische vlak(1).»

Het staat vast dat de activiteiten van criminele organisaties inderdaad talrijk en veelzijdig zijn en dat deze in aanraking kunnen komen met gevoelige sectoren, zoals diegene met betrekking tot het economisch potentieel van het land (bijvoorbeeld: het infiltreren in economische bedrijven via het witwassen van misdaadkapitalen, corruptie, mensenhandel en clandestiene arbeid), het terrorisme, de proliferatie, kortom al de betrokken onderwerpen die de Veiligheid van de Staat als opdrachten kreeg toegewezen.

4.3. De Veiligheid van de Staat dient zich ook te plaatsen ten opzichte van andere diensten die meestrijden tegen de georganiseerde misdaad(2), en dient op dit vlak ook deel te nemen aan een zo goed

(1) Artikel 8, *f)*, definieert de criminele organisatie als «(...) iedere gestructureerde vereniging van meer dan twee personen die duurt in de tijd, met als oogmerk het in onderling overleg plegen van misdaden en wanbedrijven, om direct of indirect vermogensvoordelen te verkrijgen, waarbij gebruik gemaakt wordt van intimidatie, bedreiging, geweld, listige kunstgrepen of corruptie, of waarbij commerciële of andere structuren worden aangewend om het plegen van misdrijven te verbergen of te vergemakkelijken(...)».

(1) Volgens het jaarverslag van 1999 over de georganiseerde misdaad ligt de Veiligheid van de Staat voor 1 % aan de basis van informatie die toegelaten heeft een gerechtelijk onderzoek op te starten (*cf.* voornoemd jaarverslag — blz. 72, pt. 9.2 — tabel 13).

(2) EEG-verordening nr. 3381/94 van de Raad van 19 december 1994 tot instelling van een communautaire regeling voor controle op de uitvoer van goederen voor tweeërlei gebruik.

mateur idéal? Il ne sera un informateur utile que par ses accointances avec le milieu.

Des critères basés exclusivement sur le principe de prudence ne peuvent donc être retenus sans prendre un autre risque qui est de se couper de sources importantes d'informations dans cette matière très sensible des organisations criminelles.

Il faut relever par ailleurs que dans d'autres domaines plus traditionnels de l'action des agents extérieurs de la Sûreté de l'État, le même type de dangers inhérents au recrutement d'informateurs existait déjà. Pensons notamment à la matière de l'extrémisme et à celle du terrorisme.

D'autre part, il n'est pas toujours facile de tracer une limite nette et précise entre les autres missions légales qui sont confiées aux services de renseignement et celle attribuée spécifiquement à la Sûreté de l'État concernant les menaces que font peser dans différents domaines les organisations criminelles.

L'article 8, *f)*, de la loi organique des services de renseignement du 30 novembre 1998 vise spécialement à ce sujet «les conséquences déstabilisantes sur le plan politique ou socio-économique» susceptibles d'être causées par les organisations criminelles(1).

Il est un fait que les activités de celles-ci sont en effet multiples et diversifiées et qu'elles peuvent toucher des secteurs sensibles comme ceux relatifs au potentiel économique du pays (citons entre autres à ce sujet la prise de participation dans des entreprises économiques via le blanchiment de capitaux d'origine criminelle, la corruption, les trafics d'êtres humains et ceux de la main-d'œuvre clandestine), au terrorisme, à la prolifération, autant de matières concernées par les missions de la Sûreté de l'État.

4.3. La Sûreté de l'État doit aussi se positionner par rapport aux autres services qui participent à la lutte contre la criminalité organisée(2) et participer dans ce domaine à la meilleure collaboration possible

(1) L'article 8, *f)*, définit d'autre part l'organisation criminelle comme «(...) toute association structurée de plus de deux personnes, établies dans le temps, en vue de commettre de façon concertée des crimes et des délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions (...)».

(1) Selon le rapport annuel 1999 sur le crime organisé la Sûreté de l'État est à concurrence de 1 % à l'origine des informations qui ont permis de démarrer une enquête judiciaire (*cf.* rapport — p. 71, pt. 9.2 — tableau nº 13).

(2) Règlement CE nº 3381/94 du Conseil, du 19 décembre 1994 instituant un régime communautaire de contrôle des exportations de biens à double usage.

mogelijke samenwerking met de andere administratieve en gerechtelijke diensten en politiediensten (1).

Het gaat trouwens over deze samenwerking in de wet op de inlichtingen- en veiligheidsdiensten, zoals trouwens in diezelfde wet de mogelijkheid erkent wordt dat de inlichtingendiensten een beroep kunnen doen op «menselijke bronnen» voor het inwinnen van inlichtingen (2).

Het verslag van 1999 van de ministers van Justitie en Binnenlandse Zaken aangaande «georganiseerde misdaad in België in 1998», vermeldt:

«Gelet op de specifieke doelstelling van de dienst en het ontbreken van politiële bevoegdheden, kan de Veiligheid van de Staat alleen «zachte» informatie geven (de Veiligheid van de Staat voert immers geen enkel gerechtelijk onderzoeken uit en stelt geen processen-verbaal op).

Bovendien voert de Veiligheid van de Staat geen enkel onderzoek uit naar afzonderlijke strafbare feiten, maar tracht de structuren in kaart te brengen. Ten slotte wordt getracht dubbel tellingen te voorkomen (een gedeelte van de informatie van de Veiligheid van de Staat wordt door de politiediensten in harde informatie omgezet). De werking van de Veiligheid van de Staat is niet gericht op de omzetting van dat soort inlichtingen in kwantitatieve gegevens. Derhalve geeft de Veiligheid van de Staat een kwalitatieve omschrijving van het verschijnsel. »(3)

In «Het Federaal Veiligheids- en Detentieplan»(4) wordt bij herhaling de rol van de Veiligheid van de Staat binnen de veiligheidscontext (meer bepaald in de strijd tegen de georganiseerde misdaad) beklemtoond, in het bijzonder wat betreft het uitwerken van strategische analyses.

4.4. Volgens de voormalige administrateur-generaal van de Veiligheid van de Staat blijft het beroep doen op informanten nog steeds het belang-

(1) Een rondschrijven van het College van procureurs-generaal bij de hoven van beroep van juni 1999, geclassificeerd als «vertrouwelijk», regelt de samenwerking tussen de inlichtingen- en veiligheidsdiensten, het openbaar ministerie en de onderzoeksrechters. Zie eveneens het verslag over «De toepassing van het protocolakkoord tussen de minister van Justitie en de minister van Landsverdediging over de samenwerking en de uitwisseling van informatie tussen de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid», Activiteitenverslag 1999 van het Comité I, blz. 62 tot 65.

(1) *Cf.* respectievelijk de artikelen 18 en 20 van de wet van november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

(2) *La Libre Belgique*, van 16 januari 2001, blz. 15: «Que les espions lèvent le doigt ...».

(3) Zie voornoemd jaarverslag — blz. 38, *cf.* voetnoot 21.

(4) Zie Belgische Senaat en Kamer van volksvertegenwoordiging, zitting 1999-2000 — Doc. nr. 2-461/1, Senaat en doc. nr. 50 0716/001, Kamer van 13 juni 2000, blz. 44-45: project 27.

avec les autres services administratifs, policiers et judiciaires (1).

Cette coopération est d'ailleurs visée par la loi organique des services de renseignement et de sécurité, comme d'ailleurs la possibilité reconnue par cette même loi aux services de renseignement de recourir à «des sources humaines» pour le recueil d'informations (2).

Selon le rapport 1999 des ministres de la Justice et de l'intérieur sur le crime organisé en 1998:

«Étant donné la finalité spécifique de la Sûreté de l'État et l'absence de compétences policières, ce service peut uniquement soumettre l'information qualifiée de «douce» (la Sûreté de l'État n'effectue aucune enquête judiciaire et ne rédige pas de procès-verbaux).

De plus, la Sûreté de l'État ne mène aucune enquête sur des faits punissables isolés mais tente de dresser une carte des structures. Enfin, on vise à éviter ainsi des doubles comptages (une partie des informations provenant de la Sûreté de l'État est transformée par les services de police en information dure). Le fonctionnement de la Sûreté de l'État n'est pas axé sur la conversion de ce type de renseignements en données quantitatives. Par conséquent, elle donne une description qualitative du phénomène. »(3)

Dans le plan fédéral de sécurité et de politique pénitentiaire (4), à plusieurs reprises, le rôle de la Sûreté de l'État dans la chaîne de sécurité et plus particulièrement dans la lutte contre la criminalité organisée, est souligné, notamment dans l'établissement d'analyses stratégiques.

4.4. Selon l'ancien administrateur général de la Sûreté de l'État, le recours à des informateurs reste également le moyen principal pour obtenir des rensei-

(1) Une circulaire du Collège des procureurs généraux près les cours d'appel de juin 1999, classifiée «confidentielle» règle la collaboration entre les services de renseignement et de sécurité, le ministère public et les juges d'instruction. Voir également «Le rapport sur la mise en application du protocole d'accord entre le ministre de la justice et le ministre de la défense nationale règlant la coopération et l'échange d'informations entre la Sûreté de l'État et le Service général du renseignement et de la sécurité« (Rapport d'activités 1999 du Comité R, pp. 55 à 58).

(1) *Cf.* respectivement les articles 18 et 20 de la loi organique des services de renseignement et de sécurité du 30 novembre 1998.

(2) *La Libre Belgique*, du 16 janvier 2001, p. 15: « Que les espions lèvent le doigt ... ».

(3) Voir rapport — p. 36, *cf.* note de base nº 21.

(4) *Cf.* Sénat et Chambre des représentants de Belgique — session 1999-2000 — Doc. nº. 2-461/1, Sénat et doc. nº 50 0716/001, Chambre du 13 juin 2000 — pp. 44 à 45 — projet 27.

rijkste middel om aan inlichtingen te komen (onderhoud met het Vast Comité I op 2 februari 1999).

4.5. In 1995 heeft het Comité I reeds een theoretisch onderzoek uitgevoerd aangaande de informanten van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid. De resultaten van dit onderzoek werden gepubliceerd in het activiteitenverslag van het Vast Comité I — 1997 (zie pagina 141 tot 173).

Dit onderzoek had tot doel de problemen die zich kunnen stellen naar aanleiding van het gebruik van informanten te identificeren, en daaruit volgend de nodige aanbevelingen te formuleren.

In zijn algemeen besluit onderlijnde het Comité I dat «(...) verdient deze materie in verband met de inlichtingendiensten verder onderzoek (...)» en «(...) Het risico bestaat immers in de materies zoals georganiseerde misdaad, terrorisme, (...) het verschil tussen informanten van politie- en inlichtingendiensten vervaagt en beide diensten voor vergelijkbare problemen zullen komen te staan.»

Het Comité I deed de aanbeveling dat een wettekst zou worden uitgevaardigd die het gebruik van informanten door inlichtingendiensten zou regelen volgens de principes van subsidiariteit, proportionaliteit en externe bescherming van de informant, met inbegrip van zijn fysieke bescherming.

4.6. Indien de beslissing om een einde te stellen aan de contacten met een informant gerechtvaardigd lijkt, blijkt daaruit duidelijk dat men, wanneer een specifieke geval in een bredere context wordt geplaatst en er rekening wordt gehouden met het verschil in appreciatie van de situatie tussen de mensen van het terrein en de directie van de dienst, geconfronteerd wordt met een voldoende belangrijke problematiek, die in de toekomst in al haar aspecten dient geregeld te worden, en dit op zulk een wijze dat er een zo goed mogelijk evenwicht ontstaat tussen de vereisten op het vlak van efficiëntie bij het onderkennen van bedreigingen zoals geformuleerd door de wet op de inlichtingendiensten, en de vereisten op het vlak van de bescherming van personen, met inbegrip van de informanten en de agenten van de betrokken diensten.

Het Comité I herhaalt derhalve haar aanbeveling om aangaande deze materie de nodige wetgevende initiatieven te ontplooien.

Wat deze aanbeveling betreft verwijst de minister van Justitie in zijn brief van 4 april 2001 (1) naar de opmerking geformuleerd door de Veiligheid van de Staat volgens dewelke «de organieke wet (artikelen 18, 38, 39, 40, 41 en 43) de wettelijke basis

(1) Zie *infra* blz. 171.

gnements (entretien du 2 février 1999 avec le Comité R).

4.5. En 1995, le Comité R avait déjà effectué une enquête théorique de contrôle sur l'utilisation d'informateurs par la Sûreté de l'État et le SGR. Les résultats de cette enquête ont été publiés dans le rapport général d'activités de 1997 (voir pages 134 à 164).

Cette enquête visait à identifier les problèmes qui peuvent se poser à l'occasion de l'utilisation d'informateurs et d'en dégager des premières recommandations.

Dans sa conclusion générale le Comité R soulignait que la matière méritait «d'être traitée en ce qui concernait les services de renseignement» et qu'il y avait un risque «dans les domaines de la criminalité organisée et du terrorisme, que la différence entre informateur des services de police et de renseignement ne s'estompe et que les deux services aient à faire face à des problèmes comparables».

Le Comité R avait recommandé à cette occasion qu'un texte légal soit édicté qui règlerait l'utilisation d'informateurs par les services de renseignement, selon les principes de subsidiarité, de proportionnalité et de protection externe de l'informateur, en ce compris sa protection physique.

4.6. Si la décision prise en l'espèce de mettre fin aux contacts avec l'informateur apparaît comme justifiée, la mise en perspective du cas particulier dans un contexte actuel plus élargi, ainsi que la divergence d'appréciation de la situation par les agents du terrain et par la direction du service montrent que l'on se trouve en présence d'une problématique suffisamment importante pour qu'elle soit réglée dans l'avenir et dans toutes ses composantes, de manière à établir le meilleur équilibre possible entre les exigences d'efficacité dans l'identification des menaces telles qu'elles sont définies par la loi organique des services de renseignement et celles de la protection des personnes, en ce compris les informateurs eux-mêmes et les agents des services concernés.

Le Comité R réitère donc sa recommandation de mettre en place une législation générale en la matière.

À propos de cette recommandation, le ministre de la Justice se réfère, dans son courrier du 4 avril 2001 (1), à la remarque formulée par la Sûreté de l'État selon laquelle «la loi organique (articles 18, 38, 39, 40, 41 et 43) contient les bases légales quant au

(1) Voir *infra* p. 158.

behoudt om beroep te doen op informanten voor het inwinnen van inlichtingen, de veiligheid van de gegevens die op de menselijke bronnen betrekking hebben en de inlichtingen die ze meedelen; de bescherming van geclassificeerde gegevens (waaronder deze toevertrouwd door deze bronnen) alsook de garantie van hun anonimiteit met name door middel van geldboetes in geval van openbaarmaking van de identiteit van een persoon die de anonimiteit vraagt of in de veronderstelling van de verspreiding door de agenten van de Veiligheid van de Staat van geheimen toevertrouwd bij de uitoefening van hun opdrachten (inbegrepen de identiteit van een informant indien ze toevertrouwd wordt onder het zegel van geheimhouding).

Rekening houdend met deze teksten, lijkt het niet nodig eventuele andere regels te voorzien inzake informanten. Het past inderdaad zich te beperken tot de zeer algemene regels in het kader van de wet teneinde het operationeel werk van de dienst niet te hinderen. De andere regels inzake informanten daarentegen zouden kunnen hernomen worden in de interne richtlijnen met een controle.»

recours aux informateurs pour le recueil du renseignement, la sécurité des données les concernant et les informations qu'elles communiquent, la protection des données classifiées (dont celles qui seraient confiées par ces sources) et la garantie de leur anonymat notamment par le biais de la sanction pénale en cas de révélation de l'identité d'une personne qui demande l'anonymat ou dans l'hypothèse de la divulgation par les agents de la Sûreté de l'État des secrets confiés dans l'exercice de leurs missions (en ce compris l'identité d'un informateur si celle-ci est confiée sous le sceau du secret).

Compte tenu de ces textes, il ne paraît pas nécessaire de prévoir d'éventuelles autres règles relatives aux informateurs. Il convient en effet de se limiter à des règles très générales dans le cadre de la loi afin de ne pas compromettre le travail opérationnel du service. Par contre, les autres règles concernant les informateurs pourraient être reprises dans des directives internes avec un contrôle.»

HOOFDSTUK 3

TOEZICHTSONDERZOEK ALS GEVOLG VAN EEN KLACHT INGEDIEND DOOR EEN PARTICULIER

1. Procedure

Op 13 maart 2000 ontving het Comité I een schrijven van een gedetineerde. De betrokkene vroeg het Comité I een onderzoek te openen tegen de Belgische (en buitenlandse) inlichtingendiensten wegens bepaalde omstandigheden waarvan hij had vastgesteld dat ze in zijn nadeel bestonden en die verband hielden met de vrijmetselarij. Hij stelde de voornoemde diensten aansprakelijk voor deze omstandigheden. In zijn brief schreef hij ook dat hij contact had opgenomen met de «politieke sectie» van de Amerikaanse ambassade.

Bijgevolg stuurde het Comité I op 27 maart 2000 een kantschrift naar het hoofd van zijn Dienst enquêtes met het verzoek de klager te verhoren en hem te vragen zijn klacht te bevestigen. Tegelijk deelde het Comité I mee dat deze klacht opnieuw zou worden onderzocht na kennisname van dit verhoor.

Op 28 maart 2000 gaf de voorzitter van het Comité I kennis van de opening van dit onderzoek aan de voorzitter van de Senaat, overeenkomstig artikel 32 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten. Het onderzoek kreeg de titel «klacht van een particulier over vermeende activiteiten van de inlichtingendiensten».

CHAPITRE 3

ENQUÊTE DE CONTRÔLE SUITE À LA PLAINTE D'UN PARTICULIER

1. Procédure

Le 13 mars 2000, le Comité R réceptionne un courrier d'une personne détenue, laquelle souhaite voir le Comité R initier une enquête à charge des services de renseignement belges (et étrangers) en raison des circonstances qu'il a constatées à l'encontre de sa personne et en rapport avec la franc-maçonnerie et dont il leur prête la responsabilité. Il signale par ailleurs avoir pris contact avec la «section politique» de l'ambassade américaine.

Le 27 mars 2000, le Comité R fait donc parvenir au chef de son Service d'enquêtes une apostille par laquelle il invite ce dernier à entendre le plaignant en confirmation de sa plainte, tout en signalant qu'une réévaluation de cette plainte sera faite après prise de connaissance de cette audition.

En date du 28 mars 2000 le président du Comité R notifie l'ouverture de cette enquête au président du Sénat, en conformité avec l'article 32 de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991, sous l'intitulé «plainte d'un particulier au sujet d'activités supposées des services de renseignement».

Per brief van 30 maart 2000 gaf het hoofd van de Dienst enquêtes van het Comité I op zijn beurt kennis van de opening van dit onderzoek aan de ministers van Landsverdediging en Justitie, overeenkomstig artikel 43.1 van dezelfde organieke wet.

Op 7 april 2000 diende de Dienst enquêtes van het Comité I een rapport in.

Op 7 juni 2000 ontving de Dienst enquêtes een aanvullend verzoekschrift. Het definitieve onderzoeksrapport werd ingediend op 20 juni 2000.

Het Comité I heeft dit rapport goedgekeurd op 26 maart 2001.

Op 4 april 2001 liet de minister van Justitie schriftelijk weten dat hij geen opmerkingen had over dit verslag.

Op 25 april 2001 liet de minister van Landsverdediging schriftelijk weten dat hij geen bezwaar had tegen de publicatie van dit verslag.

2. Vaststellingen

Op 5 april 2000 heeft de Dienst enquêtes van het Comité I dus een onderhoud gehad met de klager. Van zijn verklaringen werd een proces-verbaal opgesteld. Hoewel de betrokkene de inhoud van zijn bovengenoemd schrijven bevestigde, kwam zijn verklaring erop neer dat hij geen elementen tot staving van zijn beweringen kon aanvoeren. Ondanks het aandringen van de onderzoekers kon geen enkele precieze grief of geen enkel bijkomend element aan zijn schrijven worden toegevoegd.

Onmiddellijk na ontvangst van het kantschrift met het verzoek bijkomende zaken te verifiëren, heeft het hoofd van de Dienst enquêtes inlichtingen ingewonnen over de omstandigheden waarin de klager werd opgesloten.

Hieruit is gebleken dat de betrokkene het voorwerp was geweest van een bevel tot internering, verleend door een raadkamer en kort nadien bevestigd door een kamer van inbeschuldigingstelling. Overigens meldde de verzoeker dat hij tegen deze laatste beslissing voorziening in cassatie had aangetekend.

Enkele dagen later hebben de onderzoekers van het Comité I de Veiligheid van de Staat ondervraagd teneinde na te gaan of deze dienst eventueel over inlichtingen beschikte met betrekking tot de klager. Ze kregen echter te horen dat de betrokkene niet gekend was bij de Veiligheid van de Staat.

3. Besluiten

De hierboven beschreven activiteiten van de Dienst enquêtes van het Comité I hebben het niet mogelijk gemaakt enig tastbaar element aan te brengen dat kan worden gecontroleerd. Ze hebben echter aangetoond

Par courrier du 30 mars 2000, le chef du Service d'enquêtes du Comité R avise à son tour de l'ouverture de cette enquête les ministres de la Défense nationale et de la Justice, en exécution de l'article 43.1 de la même loi organique.

Le Service d'enquêtes du Comité R dépose un rapport en date du 7 avril 2000.

Une apostille complémentaire lui est adressée le 7 juin 2000 et le rapport d'enquête final sera déposé le 20 juin 2000.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 26 mars 2001.

Le 4 avril 2001, le ministre de la Justice a fait savoir au Comité R qu'il n'avait aucune remarque quant à la publication de ce rapport.

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas d'objection à la publication de ce rapport.

2. Constatations

Le Service d'enquêtes du Comité R s'est donc entretenu avec le plaignant en date du 5 avril 2000 et un procès-verbal a été dressé des propos recueillis. Celui-ci, quoique maintenant le contenu de son courrier précité, déclare en substance ne pouvoir y apporter d'éléments contributifs. Aucun grief précis, aucun élément complémentaire ne seront ajoutés, nonobstant les insistances des enquêteurs.

Dès réception de l'apostille l'invitant à procéder à des vérifications supplémentaires, le chef du Service d'enquêtes s'est enquis des circonstances de la détention du plaignant.

Il est apparu de cette vérification que l'intéressé avait fait l'objet d'une ordonnance d'internement rendue par une chambre du conseil et confirmée peu après par une chambre des mises en accusation. Le requérant a en outre signalé avoir formé un pourvoi en cassation contre cette dernière décision.

Quelques jours plus tard les enquêteurs du Comité R ont interrogé la Sûreté de l'État sur l'éventualité d'informations disponibles au sein du service relativement à la personne du plaignant, mais il leur a été répondu que l'intéressé était inconnu de la Sûreté de l'État.

3. Conclusions

Les démarches préalables opérées par le Service d'enquêtes du Comité R n'ont pas permis d'apporter le moindre élément matériel susceptible de vérifications, mais ont révélé que le plaignant avait fait l'objet

dat de klager het voorwerp was geweest van een gerechtelijke maatregel tot internering in een psychiatrische inrichting, die in hoger beroep werd bevestigd.

Gelet op deze dubbele omstandigheid heeft het Comité I beslist dit onderzoek te sluiten in de staat waarin het zich bevindt.

HOOFDSTUK 4

TOEZICHTSONDERZOEK ALS GEVOLG VAN EEN KLACHT INGEDIEND DOOR EEN PARTICULIER

1. Procedure

Op 10 mei 2000 ontving het Comité I een schrijven van iemand die meldde dat hij het slachtoffer was geworden van feiten van agressie. Deze feiten werden gepleegd door twee personen, van wie de ene volgens de klager « een schurk is van wie bekend staat dat hij wordt betaald door een gewestelijk bureau van de inlichtingendiensten ». De feiten zouden een vorm van intimidatie zijn geweest.

De klager voegde bij zijn schrijven een kopie van een proces-verbaal van 6 mei 2000 betreffende het indienen van een klacht. Voorts kondigde hij aan dat hij zinnens was eender welke rechtsvordering in te stellen die hij passend achtte. Tevens behield hij zich de mogelijkheid voor de pers in te lichten. Voor het overige hield hij zich zo nodig ter beschikking van het Comité I.

Dezelfde dag bezorgde het Comité I aan het hoofd van zijn Dienst enquêtes een kantschrift met het verzoek de klager te verhoren en hem te vragen zijn klacht te bevestigen. Tegelijk deelde het Comité I mee dat deze klacht opnieuw zou worden onderzocht na kennisname van dit verhoor.

Op 25 mei 2000 diende de Dienst enquêtes van het Comité I een evaluatieverslag in.

Op 7 juni 2000 ontving deze dienst een aanvullend kantschrift met het verzoek de opsporingen voort te zetten in het kader van een toezichtsonderzoek.

Per brief met dezelfde datum bracht het hoofd van de Dienst enquêtes van het Comité I de minister van Justitie op de hoogte van de opening van dit onderzoek, overeenkomstig artikel 43.1 van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten.

Op 8 juni 2000 gaf de voorzitter van het Comité I kennis van de opening van dit onderzoek aan de voorzitter van de Senaat, overeenkomstig artikel 32 van dezelfde organieke wet. Dit onderzoek kreeg de titel « toezichtsonderzoek naar aanleiding van een klacht

d'une mesure judiciaire d'internement psychiatrique, confirmée en degré d'appel.

En raison de cette double circonstance le Comité R a décidé de clôturer l'enquête en l'état.

CHAPITRE 4

ENQUÊTE DE CONTRÔLE SUITE À LA PLAINTE D'UN PARTICULIER

1. Procédure

Le 10 mai 2000, le Comité R réceptionne un courrier d'une personne qui souhaite faire part d'une agression dont il a fait l'objet de la part de deux individus dont l'un serait d'après le plaignant « un voyou notoirement à la solde d'un bureau régional d'un des services de renseignement ». Cet acte constituerait en fait une intimidation.

Le plaignant joint à son courrier une copie d'un procès-verbal de dépôt de plainte du 6 mai 2000 et annonce son intention d'intenter toute action en justice qu'il estimera appropriée, de même qu'il se réserve la possibilité d'en référer à la presse. Pour le surplus, il se tient à la disposition du Comité R, s'il échet.

Le même jour, le Comité R fait donc parvenir au chef de son Service d'enquêtes une apostille par laquelle il invite ce dernier à entendre le plaignant en confirmation de sa plainte, tout en signalant qu'une réévaluation de cette plainte sera opérée après prise de connaissance de cette audition.

Le service d'enquêtes du Comité R dépose un rapport d'évaluation en date du 25 mai 2000.

Une apostille complémentaire lui est adressée le 7 juin 2000, l'invitant à poursuivre les investigations dans le cadre d'une enquête de contrôle.

Par courrier du même jour, le chef du Service d'enquêtes du Comité R avise le ministre de la Justice de l'ouverture de cette enquête, en exécution de l'article 43.1 de la même loi organique.

En date du 8 juin 2000, le président du Comité R notifie l'ouverture de cette enquête au président du Sénat, en conformité avec l'article 32 de la loi organique de contrôle des services de police et de renseignement du 18 juillet 1991, sous l'intitulé « enquête de

ingediend door een particulier over de Veiligheid van de Staat».

Op 19 juli 2000 werd het definitieve onderzoeksrapport ingediend.

Nadien bezorgde de klager aan het hoofd van de Dienst enquêtes van het Comité I de kopieën van 20 december 2000 en 16 januari 2001 van nieuwe klachten die hij had verzonden naar de administrateur-generaal van de Veiligheid van de Staat en die betrekking hadden op de intimidaties waarover hij zich beklaagde.

Het Comité I heeft dit rapport goedgekeurd op 26 maart 2001.

Op 4 april 2001 liet de minister van Justitie schriftelijk weten dat hij geen opmerkingen te formuleren had nopens dit verslag.

2. Vaststellingen

Op 23 mei 2000 heeft de Dienst enquêtes van het Comité I een onderhoud gehad met de klager. Van zijn verklaringen werd een proces-verbaal opgemaakt.

Uit de verklaring van de betrokkene blijkt dat het bewuste incident in werkelijkheid de zoveelste episode is in een reeks die een aanvang zou hebben genomen in 1993-1994. Alles begon naar aanleiding van een banaal misverstand. Dit was het gevolg van het feit dat de klager in die tijd werd opgemerkt in het gezelschap van leden van de GP. Hij zou dan de vergissing hebben begaan het gerucht te verspreiden — «voor de lol» — dat hij voor het ministerie van Justitie werkte. Als gevolg daarvan zou hij herhaaldelijk zijn geschaduwd en zijn geïnterpelleerd in de cafés die hij regelmatig bezoekt.

De betrokkene, wiens vader een Bask is, verklaarde dat hij speciaal in het oog was gehouden ter gelegenheid van het bezoek van de Spaanse koning. Zo zou een Puma-helikopter van de rijkswacht een tijdlang zijn blijven hangen voor het raam van zijn woonkamer, «om hem te observeren met een grote camera». De rijkswacht zou ook zijn bankrekeningen hebben gecontroleerd.

De betrokkene kent geen leden van de inlichtingendiensten en de intimidaties worden steeds gepleegd door «kleine schurken» die daartoe de opdracht krijgen.

Hij heeft gewerkt in Frankrijk, in Zuid-Afrika en in Israël en hij is van mening dat men hem — ten onrechte — aanziet voor «een grote vis».

Hij wil slechts één ding: met rust gelaten worden.

Op 26 juni 2000 werd een commissaris van de GP ondervraagd over de betrokkene. Deze commissaris

contrôle suite à la plainte d'un particulier concernant la Sûreté de l'État».

Le rapport d'enquête final sera déposé le 19 juillet 2000.

Le plaignant a ultérieurement adressé au chef du Service d'enquêtes du Comité R les copies respectivement datées des 20 décembre 2000 et 16 janvier 2001 de nouvelles doléances qu'il a adressées à l'administrateur général de la Sûreté de l'État en relation avec le harcèlement dont il se plaint.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 26 mars 2001.

Le 4 avril 2001, le ministre de la Justice a fait savoir au Comité R qu'il n'avait pas de remarque à formuler au sujet de la publication de ce rapport.

2. Constatations

Le Service d'enquêtes du Comité R s'est donc entretenu avec le plaignant en date du 23 mai 2000 et un procès-verbal a été dressé des propos recueillis.

Il ressort de la déclaration que l'incident dénoncé serait en fait la «énième» péripétie d'une série qui aurait débuté en 1993-1994, à l'issue d'un malentendu banal, le plaignant ayant à cette époque été vu en compagnie de membres de la PJ. Il aurait eu le tort de laisser circuler — par amusement — la rumeur selon laquelle il travaillait pour le ministère de la Justice, ce qui aurait fini par provoquer des filatures répétées et des interpellations dans les débits de boissons qu'il fréquente.

Basque par son père, il relate avoir fait l'objet d'une surveillance spécifique lors de la visite du roi d'Espagne, et notamment par un hélicoptère «Puma» de la gendarmerie qui aurait effectué un vol stationnaire devant la fenêtre de son living, «pour l'observer avec sa grosse caméra». Ses comptes bancaires auraient aussi été vérifiés par la gendarmerie.

Il ne connaît aucun membre de services de renseignement et le harcèlement est toujours effectué par l'entremise de «petits voyous» mandatés à cette fin.

Il a travaillé en France, en Afrique du Sud et en Israël et son hypothèse est qu'il serait — à tort — pris pour «un gros poisson».

Il ne souhaite qu'une chose: récupérer sa tranquillité.

Interrogé à son propos le 26 juin 2000, un commissaire de la PJ a déclaré le connaître et le considérer

verklaarde dat hij de betrokkene kent en hem beschouwt als een erudiet persoon. Na het vertrek van de betrokkene naar het buitenland, was hij uit het zicht verdwenen. Hij is bij de politiediensten niet gekend om ongunstige feiten.

Op 4 juli 2000 werd een commissaris van de Veiligheid van de Staat verhoord. Hij verklaarde dat de betrokkene niet gekend was bij zijn dienst en ook niet persoonlijk door een of meer van zijn medewerkers. Hij sluit echter niet uit dat agenten van de Veiligheid van de Staat de betrokkene hebben ontmoet, zonder hem evenwel te identificeren, bij een toevallig bezoek aan een café.

3. Besluiten

Op basis van het voorafgaand verhoor van de klager kon het Comité I zich niet onmiddellijk een mening vormen. Bijgevolg heeft het Comité I een toezichtsonderzoek uitgevoerd. Dit onderzoek heeft echter geen omstandigheden aan het licht gebracht die de Veiligheid van de Staat kunnen interesseren, *a fortiori* aanleiding kunnen geven tot de aangeklaagde intimidaties. Daarentegen is gebleken dat de klager een trouw cafébezoeker is en niets heeft ondernomen om te beletten dat een waas van geheimzinnigheid rond zijn activiteiten bleef hangen, niet alleen als gevolg van zijn omgang met leden van politiediensten, maar ook tengevolge van zijn afkomst of zijn professionele activiteiten in het buitenland.

Zonder de feiten van agressie in twijfel te trekken die de klager ter staving van zijn stelling aanvoert, is het Comité I niettemin van mening, op grond van de inhoud van het onderzoek en bij gebrek aan enige aanwijzingen van het tegendeel, dat deze feiten eerder zijn gepleegd door personen die dezelfde cafés bezoeken, maar die niet de minste band hebben met de Veiligheid van de Staat.

Rekening houdend met het feit dat er momenteel geen overtuigende elementen voorhanden zijn die de klacht lijken te staven, besliste het Comité I het onderzoek te sluiten in de staat waarin het zich bevindt.

comme un érudit, puis l'avoir perdu de vue à la suite de son départ à l'étranger. Il n'est pas connu défavorablement des services de police.

Interrogé à son tour en date du 4 juillet 2000, un commissaire de la Sûreté de l'État a déclaré que l'intéressé n'était pas connu de son service, ni même à titre personnel par ses collaborateurs. Il n'exclut toutefois pas l'éventualité d'une rencontre, sans identification de l'intéressé, au hasard de la fréquentation de débits de boissons par des agents de la Sûreté de l'État.

3. Conclusions

L'audition préalable du plaignant n'a pas permis au Comité R de se faire une opinion immédiate. Il a donc entamé une enquête de contrôle. Celle-ci n'a révélé aucune circonstance susceptible d'intéresser la Sûreté de l'État, *a fortiori* de provoquer le comportement de harcèlement dénoncé. Il en est par contre apparu que le plaignant fréquente assidûment les débits de boissons et y a laissé s'installer un hâlo de mystère autour de ses activités, tant en raison de sa fréquentation de policiers que de ses origines ou de ses occupations professionnelles à l'étranger.

Sans mettre en doute l'agression que le plaignant invoque à l'appui de sa thèse, le Comité R estime cependant à la lecture du contenu de son enquête et à défaut de la moindre indication contraire, que celle-ci serait plutôt imputable à des mauvais garçons fréquentant les mêmes établissements, sans la moindre liaison avec la Sûreté de l'État.

En raison de cette absence actuelle d'éléments de conviction allant dans le sens de la plainte, le Comité R a décidé de clôturer l'enquête en l'état.

E. Opvolging van de onderzoeken van voorafgaande jaren

EINDVERSLAG OVER HET GEZAMENLIJK ONDERZOEK NAAR DE VEILIGHEIDSMAATREGELEN DIE BINNEN DE ALGEMENE POLITIESTEUNDIENST (1) (APSD) WERDEN GENOMEN OM HET WELSLAGEN VAN DE GERECHTELIJKE ONDERZOEKEN TE WAARBORGEN EN MEER IN HET ALGEMEEN NAAR DE DOELMATIGHEID VAN DEZE DIENST

1. Inleiding

1.1. Het eerste deel van dit toezichtsonderzoek werd op 18 december 1997 door het Comité I geopend, ingevolge een aangifte gedaan door een lid van de «Commissie Sirene» van de APSD, omdat de veiligheid van de Staat een veiligheidscertificaat had afgeleverd aan een personeelslid van deze commissie, dat later in het kader van een gerechtelijk onderzoek werd vervolgd omdat hij inlichtingen aan het misdaadmilieu had doorgespeeld. Toen onderhavig verslag werd opgesteld, was dit gerechtelijk onderzoek nog aan de gang.

1.2. Het Parlement was duidelijk in deze zaak geïnteresseerd, zoals uit verschillende interpellaties die uit die periode dateren, blijkt (zie pagina's 4 en 5 van het tussentijds verslag van 10 augustus 1998 waarvan sprake in punt 1.4 hieronder).

1.3. Op 3 februari 1998 werd het toezichtsonderzoek uitgebreid tot een gezamenlijk onderzoek met het Comité P, in toepassing van de artikelen 52 en volgende van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten. De opdrachten van de gezamenlijke Dienst Enquêtes bestonden erin de normen en richtlijnen die op deze problematiek van toepassing zijn, vast te leggen, om daarna de structuren, de samenstelling en de aanwervingsprocedure van de leden van de APSD te omschrijven, alsook het begrip «veiligheid» dat geldt in deze dienst, waartoe de afdeling «Sirene» belast met de toepassing van de Overeenkomst ter uitvoering van het Schengenakkoord behoort.

1.4. Op 10 augustus 1998 werd een eerste tussentijds verslag respectievelijk aan de voorzitters van de Senaat, de Kamer van volksvertegenwoordigers en de Bijzondere commissie belast met de parlementaire begeleiding van de Comités P en I toegezonden, alsook aan de ministers van Justitie en Binnenlandse

(1) Sinds 1 januari 2001 en ingevolge de politiehervorming bestaat de APSD als dusdanig niet meer. De taken van deze dienst werden overgenomen door de algemene directie voor operationele steun, «algemene directie III».

E. Suivi des enquêtes des années précédentes

RAPPORT FINAL CONCERNANT L'ENQUÊTE COMMUNE SUR LES MESURES DE SECURITÉ PRISES AU SEIN DU SERVICE GÉNÉRAL D'APPUI POLICIER (1) (SGAP) EN VUE D'ASSURER LE SUCCÈS DES ENQUÊTES JUDICIAIRES ET DE MANIÈRE PLUS GÉNÉRALE SUR L'EFFICACITÉ DE CE SERVICE

1. Préambule

1.1. La première partie de cette enquête de contrôle a été ouverte par le Comité R le 18 décembre 1997, suite à une dénonciation faite par un membre de la «Commission Sirène» du SGAP, relative au fait que la Sûreté de l'État avait accordé un certificat de sécurité à un membre du personnel de cette commission, ultérieurement poursuivi dans le cadre d'une instruction judiciaire pour avoir fourni des renseignements au milieu criminel. Ce dossier judiciaire est toujours en cours au moment de la rédaction du présent rapport.

1.2. L'intérêt parlementaire pour la question était manifeste, comme en témoignent les diverses interpellations relevées à l'époque (voir les pages 4 et 5 du rapport intermédiaire du 10 août 1998 dont question au point 1.4 ci-dessous).

1.3. Le 3 février 1998, en application des articles 52 et suivants de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, l'enquête de contrôle a été élargie à une investigation commune avec le Comité P. Les devoirs à exécuter par le Service d'enquêtes commun consistaient à relever les normes et directives applicables à la problématique pour ensuite en décrire les structures, la composition, la procédure d'engagement des membres du SGAP, et enfin le concept de sécurité en vigueur dans ce service dans lequel était incorporée la section «Sirène», chargée de l'application de la Convention d'Application de l'Accord de Schengen.

1.4. Un premier rapport intermédiaire retraçant les grandes tendances du fonctionnement du SGAP «en ce qui concerne les mesures de sécurité prises au sein de ce service en vue d'assurer le succès des enquêtes judiciaires et de manière plus générale sur l'efficacité de ce service» a été transmis, le 10 août 1998, respecti-

(1) Depuis le 1er janvier 2001 et suite à la réforme des polices, le SGAP n'existe plus en tant que tel. Ses missions ont été reprises par la direction générale de l'appui opérationnel, «la direction générale III».

Zaken. Dit verslag schetst in grote lijnen de werking van de APSD « wat de veiligheidsmaatregelen betreft die binnen deze dienst werden genomen om het welslagen van de gerechtelijke onderzoeken te waarborgen en meer in het algemeen het onderzoek naar de doelmatigheid van deze dienst ».

Eén van de doelstellingen van dit verslag was een antwoord te formuleren op de vraag wie verantwoordelijk was voor het definiëren en implementeren van de veiligheidsmaatregelen op het niveau van de divisie internationale politiesamenwerking van de APSD (afgekort IPS), daar het hoofd van deze divisie in de praktijk geleidelijk aan de eigenlijke controle van de « Commissie Sirene » had overgenomen, ten nadele van de directeur en later ook van de directeur *ad interim* van deze commissie.

Het tussentijds verslag maakte eveneens melding van de talrijke moeilijkheden die men tijdens de zoektocht naar het antwoord op deze vraag had ondervonden.

Problemen zoals persoonlijke tegenstellingen en rivaliteit tussen personen uit verschillende politiekorpsen leken inderdaad vaste vorm te hebben gekregen in de werking van de commissie « Sirene ».

Deze werkingsproblemen hadden geleid tot een bevriezing van de uitwisseling van informatie over de bescherming van gegevens en waarborgden niet langer het behoud van het veiligheidsniveau; dit werd sinds 1995 door de directeur van de « Commissie Sirene »aangeklaagd. Deze moeilijkheden hadden eveneens geleid tot een minder duidelijke bepaling van de verantwoordelijkheden in geval van « informatielekken ».

De gerechtelijke zaak (zie 1.1) bracht al deze problemen, waarmee de Algemene Politiesteundienst sinds 1995 kampte, aan het licht.

Na op die manier een hele reeks van disfuncties die duidelijk het klimaat van politieoorlog, met als inzet het beheer van informatie, weergeven, aan het licht te hebben gebracht, beval het tussentijds verslag in hoofdzaak aan de veiligheidsproblemen op te lossen door de voorschriften voorzien in artikel 118-1º, 2º, 3º en 4º van de Overeenkomst ter uitvoering van het Schengenakkoord (* Zie volgende paragrafen) ter bescherming van de persoonlijke levenssfeer in dit systeem feitelijk en nauwgezet na te leven.

(*) Artikel 118

1. Elk der overeenkomstsluitende partijen verbindt zich ertoe om voor haar nationale deel van het Schengen- informatiesysteem passende maatregelen te treffen opdat :

a. onbevoegden de toegang tot de voor de persoonsregistraties gebezigde automatiseringsapparatuur wordt ontzegd (controle op de toegang);

b. wordt voorkomen dat gegevensdragers door onbevoegden kunnen worden gelezen, gekopieerd, veranderd of verwijderd (controle op de gegevensdragers);

vement aux présidents du Sénat, de la Chambre des représentants, et de la Commission spéciale chargée de l'accompagnement parlementaire des Comités P et R, ainsi qu'aux ministres de la Justice et de l'Intérieur.

Un des buts de ce rapport était notamment de répondre à la question de savoir qui était responsable de la conception et de la mise en œuvre des mesures de sécurité au niveau de la division coopération policière internationale du SGAP (en abrégé CPI), le chef de cette division ayant acquis progressivement dans les faits le contrôle réel de la « Commission Sirène », au détriment du Directeur et ensuite du Directeur *ad interim* de celle-ci.

Le rapport intermédiaire rendait compte des nombreuses difficultés rencontrées dans la recherche de la réponse à cette question.

Des problèmes d'antagonismes personnels, de rivalité entre personnes provenant de différents corps de police semblaient en effet s'être concrétisés au niveau du fonctionnement de la commission « Sirène ».

Ces difficultés de fonctionnement avaient rendu stériles des échanges d'informations concernant la protection des données et la garantie du maintien du niveau de sécurité dont l'absence était dénoncée depuis 1995 par le directeur de la « Commission Sirène ». Ces difficultés avaient provoqué également une dilution dans la détermination des responsabilités en cas de « fuites d'informations ».

L'affaire judiciaire (voir 1.1) fut le révélateur de ces problèmes auxquels était confronté le Service général d'appui policier depuis 1995.

Après avoir ainsi mis en exergue une série de dysfonctionnements illustrant un climat avéré de guerre des polices, dont l'enjeu était la gestion de l'information, le rapport intermédiaire recommandait en substance de résoudre les problèmes de sécurité en respectant concrètement et scrupuleusement les règles prévues à l'article 118-1º, 2º, 3º et 4º de la Convention d'Application de l'Accord de Schengen (* Voir paragraphes suivants) destinées à assurer la protection de la vie privée dans ce système.

(*) Article 118

1. Chacune des Parties Contractantes s'engage à prendre, pour la partie nationale du Système d'information Schengen, les mesures qui sont propres :

a. à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations);

b. à empêcher que des supports de données ne puissent être lus, copiés, modifiés ou éloignés par une personne non autorisée (contrôle des supports de données);

c. onbevoegde opslag in het geheugen, alsmede onbevoegde kennisneming, wijziging of verwijdering van opgeslagen persoonsgegevens wordt voorkomen (controle op de opslag);

d. wordt voorkomen dat geautomatiseerde registratiesystemen door middel van datatransmissieapparatuur door onbevoegden kunnen worden gebruikt (controle op de gebruikers);

e. wordt gewaarborgd dat de personen die tot gebruik van een geautomatiseerd registratiesysteem gemachtigd zijn, uitsluitend toegang hebben tot gegevens waarop hun machtiging betrekking heeft (controle op de toegang);

f. wordt gewaarborgd dat naderhand kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in een geautomatiseerd registratiesysteem zijn opgenomen (controle op de opneming);

g. wordt gewaarborgd dat naderhand kan worden nagegaan en vastgesteld welke persoonsgegevens wanneer en door wie in een geautomatiseerd registratiesysteem zijn opgenomen (controle op de opneming);

h. wordt voorkomen dat bij de overdracht van persoonsgegevens, alsmede bij transport van gegevensdragers de gegevens op onbevoegde wijze worden gelezen, gekopieerd, gewijzigd of verwijderd (controle op het transport).

2. Iedere overeenkomstsluitende partij dient bij overdracht van gegevens aan buiten het grondgebied van de overeenkomstsluitende partijen gevestigde instanties bijzondere voorzieningen inzake gegevensbeveiliging te treffen. Hiervan dient aan de gemeenschappelijke controle-autoriteit mededeling te worden gedaan.

3. Iedere overeenkomstsluitende partij wijst ten behoeve van de gegevensverwerking in het nationale deel van het Schengeninformatiesysteem slechts personen aan die een passende opleiding hebben genoten en een veiligheidsonderzoek hebben ondergaan.

4. De voor de technisch ondersteunende functie verantwoordelijke overeenkomstsluitende partij treft voor deze functie de in de leden 1 tot en met 3 genoemde maatregelen.

In zijn brief van 24 augustus 1998 drukte de minister van Justitie zijn terughoudendheid uit over de mogelijkheid om het verslag van het gezamenlijk toezichtsonderzoek in de jaarverslagen 1998 van de Vaste Comités P en I op te nemen.

Om zijn standpunt kracht bij te zetten, wees de minister van Justitie op de aan gang zijnde politiehervorming en, in dat opzicht, op het voorstel om de APSD op te nemen in de algemene directie belast met de operationele steun binnen de toekomstige federale politie. Hij maakte anderzijds gewag van de wijzigingen die net waren aangebracht(1) aan de structuur en de werking van de beheerorganen van de APSD om

(1) Zie hiervoor de overwegingen van het koninklijk besluit van 11 juni 1998 tot wijziging van het koninklijk besluit van 11 juli 1994 over de APSD (*Belgisch Staatsblad* van 2 juli 1998) dat voorziet in de uitbreiding van de raad van bestuur met twee leden, met name een vertegenwoordiger van de bestuurlijke overheden en een vertegenwoordiger van de gerechtelijke overheden, het nemen van beslissingen bij meerderheid in plaats van bij consensus en ten slotte de vervanging van het driekoppige directiecomité door een directeur.

c. à empêcher l'introduction non autorisée dans le fichier ainsi que toute prise de connaissance, modification ou effacement non autorisés de données à caractère personnel intégrées (contrôle de l'intégration);

d. à empêcher que des systèmes de traitement automatisé de données ne puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);

e. à garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);

f. à garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission);

g. à garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);

h. à empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données ne puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport).

2. Chaque Partie Contractante doit prendre des mesures particulières en vue d'assurer la sécurité des données lors de la transmission de données à des services situés en-dehors des territoires des Parties Contractantes. Ces mesures doivent être communiquées à l'autorité de contrôle commune.

3. Chaque Partie Contractante ne peut désigner pour le traitement de données de sa partie nationale du Système d'Information Schengen que des personnes spécialement qualifiées et soumises à un contrôle de sécurité.

4. La Partie Contractante responsable de la fonction de support technique du Système d'Information Schengen prend pour ce dernier les mesures prévues aux paragraphes 1 à 3.

Par courrier du 24 août 1998, le ministre de la Justice faisait part de ses réserves concernant l'opportunité de publier le rapport d'enquête commune dans les rapports annuels 1998 des Comités permanents P et R.

Pour expliquer sa position, le ministre de la Justice faisait état de la réforme des polices en cours et, dans ce contexte, du projet d'intégrer le SGAP dans la direction générale chargée du soutien opérationnel au sein de la future police fédérale. Il faisait mention d'autre part des modifications qui venaient d'intervenir(1) dans la structure et le fonctionnement des organes de gestion du SGAP pour remédier

(1) Voir à ce sujet les considérants de l'arrêté royal du 11 juin 1998, modifiant l'arrêté royal du 11 juillet 1994 concernant le SGAP (*Moniteur belge* du 2 juillet 1998 prévoyant l'élargissement du conseil d'administration à deux nouveaux membres, à savoir un représentant des autorités administratives et un représentant des autorités judiciaires, le remplacement de la règle du consensus pour les décisions par celle de la majorité et enfin le remplacement du comité de direction tricéphale par un directeur.

een einde te maken aan de problemen die er in het verleden op het vlak van het beslissingsproces waren en die de goede werking van de dienst in de weg stonden. Hij wees er eveneens op dat reeds met andere relevante opmerkingen van het onderzoeksverslag rekening werd gehouden. Tot slot vestigde hij er de aandacht op dat de publicatie van het verslag het goede verloop van het lopende gerechtelijke onderzoek, dat niet enkel de aangeklaagde persoon aanbelangt, maar eveneens de werking van de APSD, de afdeling IPS en de dienst SIRENE in het bijzonder, zou kunnen schaden.

In zijn brief van 7 september 1998 nam de minister van Binnenlandse zaken een gelijkaardig standpunt in(1).

Het deel van het onderzoek dat enkel betrekking heeft op « de voorwaarden voor de toekenning van een veiligheidscertificaat aan een persoon beschuldigd van diefstal van documenten» werd echter wel opgenomen in het activiteitenjaarverslag 1998 van het Vast Comité I (pagina's 235 tot 243) in toepassing van artikel 37 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten.

2. Vervolg van het onderzoek

2.1. Op 1 februari 1999 werd een tweede luik van het gezamenlijk onderzoek geopend. Doelstelling hiervan was de controle op de veiligheidsonderzoeken betreffende het personeel na te streven alsook de controle van de veiligheid in het algemeen (de lokalen, de functie van de veiligheidsofficier, informatica, fotokopieermachines, de terbeschikkingstelling van afluisterapparatuur).

Wij wensen er meteen op te wijzen dat dit tweede deel van het onderzoek heel wat vertraging heeft opgelopen als gevolg van interne werkingsmoeilijkheden van het vroegere Comité P en van het ontslag van verscheidene van zijn leden.

Het eindverslag van dit aanvullend onderzoek werd op 15 oktober 1999 aan beide Comités bezorgd.

De nieuwe leden van het Vast Comité P werden op 18 november 1999 aangesteld en traden op 26 november 1999 in dienst. Van die datum af konden deze laatsten, bovendien geconfronteerd met velerlei prioritaire zaken, zich eveneens aan het heronderzoek van het volledige dossier wijden.

2.2. Ondanks deze elementen en hoofdzakelijk het feit dat, in het kader van de organisatie van de nieuwe federale politie, de divisie «Internationale Politiesa-

(1) Voor het tussentijds verslag, zie de parlementaire interpellaties in de Kamer van Volksvertegenwoordigers van België, 49e Zittingsperiode — GZ 1998-1999 — *Beknopt verslag* — COM 14 december 1998.

aux problèmes survenus dans le passé au niveau du processus décisionnel qui avaient empêché le bon fonctionnement du service. Il signalait également que d'autres remarques pertinentes du rapport d'enquête commune avaient déjà été prises en compte. Il attirait enfin l'attention sur le fait que la publication du rapport pouvait porter préjudice au bon déroulement de la procédure judiciaire en cours qui, au travers du cas de la personne incriminée, concernait également le fonctionnement du SGAP, de la section CPI et celui du service Sirène en particulier.

Par courrier du 7 septembre 1998, le ministre de l'Intérieur adoptait une approche similaire à celle de son collègue de la Justice(1).

La partie de l'enquête relative uniquement «aux conditions d'octroi du certificat de sécurité à la personne inculpée de vol de documents» a toutefois été publiée dans le rapport annuel d'activités 1998 du Comité R (pages 217 à 226) en application de l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

2. Les suites de l'enquête

2.1. Une seconde partie de l'enquête commune a été initiée le 1er février 1999. Elle avait pour but de poursuivre le contrôle relatif aux enquêtes de sécurité concernant le personnel ainsi que celui relatif à la sécurité d'une manière plus générale (les locaux, la fonction d'officier de sécurité, l'informatique, les photocopieuses, la mise à disposition de matériel d'écoute).

Il faut souligner d'emblée que cette seconde partie de l'enquête de contrôle a connu de nombreux retards liés aux difficultés internes de fonctionnement de l'ancien Comité P et à la démission successive de plusieurs de ses membres.

Le rapport final de ce complément d'enquête a été transmis aux deux Comités le 15 octobre 1999.

Les nouveaux membres du Comité permanent P ont été nommés le 18 novembre 1999 et sont entrés en fonction le 26 novembre 1999. Ce n'est qu'à partir de cette date que ces derniers, confrontés par ailleurs à de multiples priorités, ont pu également s'atteler au réexamen de l'ensemble du dossier.

2.2. Nonobstant ces éléments et principalement le fait qu'aujourd'hui, dans le cadre de l'organisation de la nouvelle police fédérale, la division «Coopération

(1) Voir au sujet du rapport intermédiaire les interpellations parlementaires dans Chambre des représentants de Belgique, 49e Législature — SO 1998-1999 — *Compte rendu analytique* —COM 14 décembre 1998.

menwerking» — waartoe «Sirene» behoort — vandaag is opgenomen in de algemene directie III, belast met operationele steun(1), achten de Vaste Comités P en I het noodzakelijk, in toepassing van artikel 53 van voornoemde wet van 18 juli, dit gezamenlijk onderzoek af te sluiten en verslag uit te brengen aan het Parlement en aan de minister van Justitie om hen de kern van de besluiten van het aanvullende onderzoek mee te delen.

Deze besluiten zijn een vervolg op de vaststellingen van het tussentijds verslag en geven vooral een evolutie weer op het vlak van veiligheid, die uit dit eerste verslag voortvloeit. Ze onderstrepen anderzijds de noodzaak van de ontwikkeling, het behoud en de toepassing van de gepaste veiligheidsregels, met name op het vlak van informatica, alsook de noodzaak om de middelen te leveren die onontbeerlijk zijn om het resultaat te waarborgen dat wordt vereist door de «Overeenkomst ter uitvoering van het Schengenakkoord» of door de «Europolovereenkomst» die België heeft ondertekend.

Zo heeft de gezamenlijke Dienst Enquêtes vastgesteld dat het veiligheidsprobleem binnen de afdeling Internationale Politiesamenwerking (IPS) in gunstige zin evolueerde.

Het verhaal van de afdeling IPS heeft aangetoond dat, algemeen gezien, het gevaar niet steeds van buitenaf komt, maar ook van binnenuit. Het was nodig om zich hiervan bewust te worden en dit is blijkbaar gebeurd, zoals de enquêteurs tijdens nieuwe bezoeken ter plaatse hebben vastgesteld.

De veiligheidsinstructies zijn zeer precies en de veiligheidsofficier werkt momenteel voltijds om het veiligheidsniveau te verbeteren.

De divisie IPS kreeg adequate technische controlemiddelen toegewezen. Het administratief beheer en de archiefverwerking van de dossiers voldoen eveneens aan precieze veiligheidscriteria.

Er is een gevoelige verbetering vastgesteld voor de veiligheidsenquêtes die werden uitgevoerd bij de aanwerving van personeelsleden, zowel politiemensen als burgers. Vragen in verband met veiligheidsonderzoeken worden gericht aan de Nationale Veiligheidsoverheid die, nadat zij tot de gebruikelijke onderzoeken is overgegaan, een veiligheidsmachtiging van het niveau «zeer geheim» aflevert.

De Vaste Comités P en I vragen zich af hoe deze procedure zal worden toegepast nu de wet van

(1) Een andere opdracht van deze algemene directie bestaat in het beheer van de nationale gegevensbank bedoeld in artikel 44/4 van de wet van 5 augustus 1992 op het politieambt. (artikel 5 van het koninklijk besluit over de bepaling van de algemene directies van de federale politie en de onderlinge verdeling van de opdrachten van de federale politie).

policière internationale» — comprenant «Sirène» — est intégrée dans la direction générale III, en charge de l'appui opérationnel(1), les deux Comités permanents P et R estiment indispensable, en application de l'article 53 de la loi du 18 juillet précitée, de clôturer cette enquête commune et de faire rapport au Parlement et au ministre de la justice en leur communiquant la substance des conclusions de l'enquête complémentaire.

Celles-ci constituent une suite aux constatations du rapport intermédiaire et montrent surtout à ce sujet l'évolution en matière de sécurité qui a suivi ce premier rapport. Elles mettent d'autre part en évidence la nécessité du développement, du maintien et de l'application de règles de sécurité adéquates, notamment dans le domaine informatique, ainsi que celle de fournir les moyens indispensables pour garantir notamment le résultat exigé par «la Convention d'application de l'Accord de Schengen» ou par «la Convention Europol» auxquelles la Belgique a souscrit.

C'est ainsi que le Service d'enquêtes commun a pu constater que le problème de la sécurité au sein de la division Coopération policière internationale (CPI) était en pleine évolution et ce de manière positive.

L'histoire de la division CPI a démontré que, d'une manière générale, le danger ne vient pas toujours de l'extérieur, mais bien de l'intérieur. Une prise de conscience à ce niveau était nécessaire et semble être devenue réalité, comme cela a été constaté à l'occasion des nouvelles visites sur place des enquêteurs.

Les instructions de sécurité sont très précises et l'officier de sécurité travaille maintenant à plein temps pour obtenir une amélioration du niveau de sécurité.

La division CPI s'est dotée d'autre part des moyens techniques de contrôle adéquats. La gestion administrative et l'archivage des dossiers répondent également à des critères précis de sécurité.

Une amélioration sensible au niveau des enquêtes de sécurité effectuées lors de l'engagement du personnel, tant policier que civil, a été constatée. Des demandes d'enquêtes de sécurité sont adressées à l'Autorité nationale de Sécurité, qui délivre une habilitation de niveau «très secret» après avoir fait procéder aux enquêtes d'usage.

Les Comités permanents P et R se demandent comment cette procédure va continuer à être appli-

(1) Cette direction générale a également pour mission la gestion de la banque de données générale nationale visée à l'article 44/4 de la loi sur la fonction de police du 5 août 1992 (article 5 de l'AR portant détermination des directions générales de la police fédérale et répartition entre elles des missions de la police fédérale).

11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen op 1 juni 2000 van kracht is geworden.

De artikelen 8 en 10 van deze wet staan immers een uitzondering toe op de verplichting om houder te zijn van een veiligheidsmachtiging voor de gerechtelijke overheden wat hun eigen bevoegdheden betreft, en anderzijds bepaalt artikel 24 § 4 van het koninklijk besluit van 24 maart 2000, ter uitvoering van de wet, dat « geen enkele vraag om veiligheidsmachtiging aan de voorzitter van de Nationale veiligheidsoverheid mag worden gericht voor de leden van de rijkswacht of andere politiediensten ».

Op het vlak van informatica bestaan er controle-instrumenten en werden bepaalde technieken voor het beheer van informatie ingevoerd om in de toekomst elk misbruik in het kader van niet toegestane toegang tot informatie te voorkomen (1).

Al deze elementen die als voorbeeld werden aangehaald, waren nog niet gekend toen het tussentijds verslag werd opgesteld. De problemen die werden ondervonden, zijn evenwel van die aard dat zij, op elk niveau, een permanente en uiterst nauwkeurige evaluatie vereisen teneinde de doelmatigheid van de gerechtelijke onderzoeken te waarborgen, zowel op nationaal als op internationaal vlak, en daarbij eveneens de eerbiediging van de persoonlijke levenssfeer en de bescherming van personen garanderen.

De toevoeging van artikel 257*bis* aan de wet van 7 december 1998 betreffende de organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (*Belgisch Staatsblad* van 29 december 2000) laat toe tijdelijk, vanaf 1 januari 2001, de controle en het toezicht op de politiediensten — twee opdrachten van het toekomstige federale parket — te concretiseren.

De Vaste Comités P en I zullen, binnen het kader van hun wettelijke opdrachten, aandachtig blijven volgen hoe de veiligheidsproblemen die het voorwerp zijn van dit onderzoek in de nieuwe politieomgeving evolueren.

Onderhavig verslag werd door de Comités P en I goedgekeurd tijdens hun gezamenlijke vergadering van 9 februari 2001.

Bij brief van 19 maart 2001 heeft de minister van Justitie laten weten dat hij geen bezwaar heeft wat betreft de publicatie van dit verslag.

(1) Artikel 18 van voornoemd koninklijk besluit van 24 maart 2000 bepaalt dat « De technische beschermingsmaatregelen en telecommunicatiesystemen en -netwerken voor geclassificeerde gegevens en van informaticasystemen en -netwerken waarin geclassificeerde gegevens worden opgeslagen, behandeld of doorgestuurd, worden bepaald door het Ministerieel Comité voor inlichting en veiligheid ».

quée suite à l'entrée en vigueur le 1er juin 2000 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

En effet, les articles 8 et 10 de cette loi établissent une exception à l'obligation de détenir une habilitation de sécurité en ce qui concerne les autorités judiciaires dans le cadre de leurs compétences propres et, d'autre part, l'article 24 § 4 de l' arrêté royal du 24 mars 2000 portant exécution de la loi, prévoit qu'« aucune demande d'habilitation de sécurité ne pourra être adressée au président de l'Autorité nationale de sécurité pour les membres de la gendarmerie ou d'autres services de police ».

Au niveau informatique, les outils de contrôle existent et certaines techniques de gestion de l'information ont été mises en place pour prévenir dans l'avenir tout abus dans le cadre de l'accès non autorisé à des informations (1).

Tous ces éléments cités à titre exemplatif n'existaient pas lors des constatations qui donnèrent lieu à la rédaction du rapport intermédiaire. Les problèmes rencontrés restent cependant de ceux pour lesquels, à tout niveau, une évaluation permanente et rigoureuse est indispensable pour garantir l'efficacité des enquêtes judiciaires aussi bien sur le plan national qu'international, tout en garantissant également le respect de la vie privée et la protection des personnes.

L'insertion d'un article 257*bis* dans la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (*Moniteur belge* du 29 décembre 2000) permet de concrétiser temporairement, dès le 1er janvier 2001, le contrôle et la surveillance des services de police qui seront deux des missions du futur parquet fédéral.

Les Comités permanents P et R, dans le cadre de leurs missions légales, resteront attentifs pour leur part à l'évolution dans le nouvel environnement policier, des problèmes de sécurité qui ont été soulevés à l'occasion de la présente enquête.

Le présent rapport a été approuvé par les Comités P et R lors de leur réunion commune du 9 février 2001.

Par courrier du 19 mars 2001, le ministre de la Justice a fait savoir qu'il n'avait pas d'objection à la publication de ce rapport.

(1) L'article 18 de l'arrêté royal précité du 24 mars 2000 prévoit que « Les mesures techniques de protection des systèmes et réseaux de télécommunication de données classifiées et des systèmes et réseaux informatiques dans lesquels des données classifiées sont stockées, traitées ou transmises, sont déterminées par le Comité ministériel du renseignement et de la sécurité ».

TITEL III

CONTACTEN VAN HET COMITÉ I

VERSLAG OVER DE DEELNAME VAN EEN LID VAN HET COMITÉ I AAN HET SEMINARIE «MAÎTRISER LES OUTILS DE LA VEILLE ET DE L'INTELLIGENCE ÉCONOMIQUE», GEORGANISEERD TE PARIJS OP 16 EN 17 MEI 2000 DOOR HET «INSTITUTE FOR INTERNATIONAL RESEARCH»

Aangezien het Vast Comité I op 26 januari 2000 besliste een onderzoek te openen betreffende «de manier waarop de Veiligheid van de Staat haar nieuwe opdracht inzake de bescherming van het wetenschappelijk of economisch potentieel vervult,» had het Comité I belangstelling voor het programma van een aantal seminaries die het «Institute for International Research» (IIR) te Parijs organiseerde. Het IIR stelt zich voor als «de grootste organisator van conferenties ter wereld». De conferenties hebben betrekking op de nieuwste ontwikkelingen op het vlak van management, onder andere inzake de economische inlichtingen, een domein dat het wetenschappelijk en economisch patrimonium van een land kan aanbelangen.

Teneinde beter vertrouwd te raken met de praktijken inzake economische inlichtingen (of «intelligence»), besliste het Comité I dus een van zijn leden naar Parijs te sturen om er het seminarie met de titel *«Maîtriser les outils de la veille et de l'Intelligence économique»* bij te wonen. Dit seminarie vond plaats op 16 en 17 mei 2000. Het werd geleid door François Jakobiak, een voormalig scheikundig ingenieur bij de firma «Société Nationale Elf Aquitaine», en momenteel adviseur inzake strategische informatie bij een onderneming die hij in 1994 zelf oprichtte. De heer Jakobiak is niet alleen specialist in het adviseren van bedrijven, waarbij hij hun instrumenten van technologische of concurrentiële bewaking voorstelt, maar is tevens een veelgevraagd spreker op internationale conferenties en docent aan verschillende universiteiten en hogescholen, waaronder ook de «Université Libre de Bruxelles». Hij publiceerde vijf werken op het gebied van wetenschappelijke, technische en strategische informatie.

Het Vast Comité I geeft hierna een samenvatting van het seminarie dat een van zijn leden heeft bijgewoond.

Van wetenschappelijke en technische informatie tot technologische bewaking

In de jaren zeventig gaf het Franse ministerie van Onderzoek voor het eerst een aanzet tot het Franse beleid inzake wetenschappelijke en technische infor-

TITRE III

CONTACTS DU COMITÉ

RAPPORT DE LA PARTICIPATION D'UN MEMBRE DU COMITÉ R AU SÉMINAIRE INTITULÉ «MAÎTRISEZ LES OUTILS DE LA VEILLE ET DE L'INTELLIGENCE ÉCONOMIQUE» ORGANISÉ À PARIS LES 16 ET 17 MAI 2000 PAR L'«INSTITUTE FOR INTERNATIONAL RESEARCH»

Ayant décidé le 26 janvier 2000 d'ouvrir une enquête sur la manière dont la Sûreté de l'État s'acquittait de sa nouvelle mission de protection du potentiel scientifique ou économique, le Comité permanent R s'est intéressé au programme d'une série de séminaires organisés à Paris par l'«Institute for International Research» IIR se présente comme «le plus important organisateur de conférences dans le monde». Ses conférences concernent les domaines les plus récents du management et notamment le renseignement économique, domaine susceptible de concerner le patrimoine scientifique et économique d'un pays.

Pour se familiariser avec les pratiques du renseignement (ou intelligence) économique, le Comité R a donc décidé d'envoyer un de ses membres à Paris pour assister au séminaire intitulé *«Maîtriser les outils de la veille et de l'Intelligence économique»* et qui a eu lieu les 16 et 17 mai 2000. Ce séminaire était animé par François Jakobiak, ancien ingénieur chimiste au sein de la «Société Nationale Elf Aquitaine», actuellement consultant en information stratégique au sein d'une société qu'il a créé en 1994. Spécialisé dans les actions de conseils aux entreprises pour proposer des outils de veille technologique ou concurentielle, M. Jakobiak est aussi conférencier international et chargé de cours dans plusieurs universités et grandes écoles, parmi lesquelles l'Université Libre de Bruxelles. Il a publié cinq ouvrages d'information scientifique, technique et stratégique.

Le Comité permanent R résume ici le contenu du séminaire auquel un de ses membres a assisté.

De l'information scientifique et technique à la veille technologique

C'est dans les années septante que le ministère français de la Recherche a donné une première impulsion à la politique française d'information scientifique et

matie. Binnen dit ministerie was het « Centre de prospective et d'évaluation » (CPE) belast met de systematische bewaking van de voornaamste technische sectoren.

Professionele informatie kan op drie verschillende manieren worden benaderd :

1) commerciële benadering : de informatie wordt beschouwd als een goed of een dienst dat/die toegevoegde waarde of banen creëert;

2) functionele benadering : informatie is belangrijk, omdat ze een bepaalde invloed uitoefent op de economie, de opleiding en de cultuur; ze is belangrijk voor de vernieuwing, de economische ontwikkeling, de productiviteit van de industriële sectoren en het culturele niveau van een land;

3) strategische benadering : hier wordt de informatie beschouwd als een strategisch goed, en bijgevolg is het noodzakelijk onder alle omstandigheden de toegang van het land tot onmisbare informatiebronnen te beschermen, de bevoorradingsbronnen te diversifiëren, en op het nationale grondgebied « strategische informatievoorraden » aan te leggen.

Frankrijk geeft voorrang aan de strategische benadering van de informatie. Dat verklaart waarom de Franse overheid vanaf 1987 campagnes heeft gevoerd ter promotie van de technologische bewaking, die in 1994 hebben geleid tot het officiële ontstaan van het begrip « economische inlichtingen ».

Wie in de economie wil overleven, moet vernieuwen. Om te vernieuwen moet men niet alleen blijk geven van creativiteit, maar moet men ook weten wat de anderen doen. Vernieuwing en technologische bewaking zijn dus nauw met elkaar verbonden.

In 1988 richtte het Franse ministerie van Onderzoek het « Comité d'orientation stratégique de la veille technologique » op, dat experts uit de industrie en vertegenwoordigers van overheidsorganen groepeert. Dit comité heeft de grote lijnen vastgesteld van een beleid van technologische bewaking door de bedrijven, dat resoluut is gericht op wetenschappelijke en technische bewaking.

Ongeacht de omvang van de onderneming omvat deze bewaking de opeenvolgende activiteiten van opsporen, verzamelen en verspreiden van de informatie. Meestal wordt deze fase van de bewaking uitgevoerd door specialisten op het vlak van documentaire informatie. De informatie wordt geëxploiteerd door personen die gespecialiseerd zijn in de specifieke activiteit van de onderneming, en omvat handelingen zoals het verwerken, analyseren, valideren en synthetiseren. De informatie is van velerlei aard : wetenschappelijk, technisch (er wordt veel belang gehecht aan informatie in octrooien), technologisch en economisch. Dit alles moet leiden tot het creëren van instrumenten die helpen bij het nemen van strategische beslissingen. In deze structuur spelen drie soorten

technique. Au sein de ce ministère, le Centre de prospective et d'évaluation (CPE) opérait la surveillance systématique des secteurs techniques majeurs.

L'information professionnelle peut être considérée selon trois approches différentes :

1) Dans une approche marchande, l'information est considérée comme un bien ou un service créateur de valeur ajoutée ou d'emploi.

2) Dans une approche fonctionnelle, l'information est importante parce qu'elle a des effets sur l'économie, la formation et la culture : elle est importante pour l'innovation, le développement économique, la productivité des secteurs industriels et le niveau culturel d'un pays.

3) Enfin, l'approche stratégique fait considérer l'information comme un bien stratégique, d'où la nécessité de préserver en toute circonstance l'accès du pays aux sources d'information indispensables, de diversifier les sources d'approvisionnement, de constituer sur le territoire national des « stocks stratégiques » d'informations.

La France accorde une priorité à l'approche stratégique de l'information. Cette priorité explique les actions de promotion de la veille technologique engagées par les pouvoirs publics français à partir de 1987 et qui ont conduit, en 1994, à l'éclosion officielle de l'intelligence économique.

En économie, il faut en effet innover pour survivre. Pour innover, il est non seulement indispensable d'être créatif, mais aussi de savoir ce que font les autres. Innovation et veille technologique sont donc liées.

En 1988, le ministre français de la Recherche constitue le « Comité d'orientation stratégique de la veille technologique » comprenant des experts industriels et des représentants d'organismes de l'État. Ce comité a défini les grandes lignes d'une politique de veille technologique par les entreprises, résolument tournée vers la surveillance scientifique et technique.

Cette surveillance, quelle que soit la taille de l'entreprise, comprend les opérations successives de recherche, de collecte et de diffusion de l'information. Cette phase de surveillance est réalisée, le plus souvent, par des spécialistes de l'information documentaire. L'exploitation est réalisée par des experts du domaine d'activité de l'entreprise et comporte des opérations de traitement, d'analyse, de validation et de synthèse. Divers types d'informations sont pris en compte : scientifique, technique (avec une importance considérable de l'information contenue dans les brevets), technologique et économique. Il doit en ressortir des outils d'aide à la prise de décisions stratégiques. Trois types d'acteurs interviennent donc dans cette structure : les observateurs et collecteurs

actoren dus een rol: waarnemers en verzamelaars van informatie, analisten (of experts) en beslissingnemers.

Concurrentiële bewaking bestaat dan weer in het observeren en analyseren van de markt en van de economische, commerciële en financiële omgeving, zodat men in staat is bedreigingen op het spoor te komen en kansen op ontwikkeling aan te grijpen.

In het rapport van het Xe plan, dat in februari 1994 werd gepubliceerd onder de titel *«Intelligence Economique et stratégique des entreprises»* (ook bekend als het «rapport-Martre», naar de naam van zijn auteur), kreeg dit begrip officiële bekrachtiging en een volwaardige betekenis: «Economische informatie kan worden gedefinieerd als het geheel van gecoördineerde acties van opsporen, verwerken en verspreiden, met het oog op de exploitatie, van de informatie die nuttig is voor de economische actoren.» Voortaan gaat het dus om een nationaal initiatief, niet langer om een initiatief op het niveau van de onderneming. Het concept «economische informatie» gaat verder dan technologische of concurrentiële bewaking, aangezien er sprake is van strategisch en tactisch opzet met interactie tussen de diverse actoren op alle niveaus (privaat, publiek, ...).

Voorts lezen we in het rapport-Martre: «Het inwinnen, verwerken en verspreiden van de nuttige informatie bepalen voortaan niet alleen het concurrentievermogen van de bedrijven, maar ook de economische macht van Staten. In Frankrijk blijft men de vraag in te grote mate uitsluitend defensief benaderen, met als gevolg dat ons systeem minder efficiënt is dan de systemen die sommige concurrerende Staten ontwikkelen.

Om de aanpak te wijzigen is een duidelijk verlangen van de overheid vereist: alleen zij kan, in nauw overleg met alle betrokken actoren, de vereiste impuls geven voor een collectief informatiebeheer.» Het is dus wel degelijk op het vlak van de offensieve aanwending van de informatie dat er een verschil is tussen economische informatie en strategische bewaking. Tot die offensieve aanwending van de informatie behoren bijvoorbeeld beïnvloeding en lobbying.

Economische informatie betreft vijf niveaus van actoren die met elkaar in interactie treden:

— het basisniveau: de onderneming;

— het tussenniveau: een professionele sector, een tak van activiteiten;

— het nationaal niveau: de ministeries en de administraties waar de strategische beslissingen worden genomen; in Frankrijk zijn de inlichtingendiensten (DST, DGSE, DRM) hierbij betrokken;

— het transnationaal niveau: multinationale groepen;

— het internationaal niveau waar de Staten beïnvloedingsstrategieën ontwikkelen.

d'informations, les analystes (ou experts) et les décideurs.

La veille concurrentielle consiste quant à elle à observer et analyser le marché, l'environnement économique, commercial et financier de manière à détecter les menaces et à saisir les opportunités de développement.

C'est le rapport du Xe plan publié en février 1994 et intitulé «Intelligence économique et stratégique des entreprises» (aussi connu sous le nom de «rapport Martre» du nom de son rapporteur) qui officialise cette dénomination et lui donne tout son sens: «L'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques.» Il s'agit donc à présent d'une initiative au niveau national, et non plus au niveau de l'entreprise. Le concept d'intelligence économique dépasse celui de veille technologique ou concurrentielle car il y a intention stratégique et tactique avec interaction entre les acteurs de tous les niveaux (privés, publics, ...).

On lit aussi dans le rapport précité: «Le recueil, le traitement et la diffusion de l'information utile déterminent désormais la compétitivité des entreprises comme la puissance économique des États. En France, la question reste traitée de façon trop exclusivement défensive, si bien que notre système est moins efficace que ceux développés par certains États concurrents.

Changer d'approche appelle une volonté claire de la puissance publique: elle seule pourra, en concertation étroite avec l'ensemble des acteurs concernés, donner l'impulsion nécessaire à une gestion collective de l'information.» C'est donc bien au niveau de l'usage offensif de l'information que l'intelligence économique diffère de la veille stratégique. Cet usage offensif de l'information comprend par exemple l'influence et le lobbying.

L'intelligence économique concerne cinq niveaux d'acteurs entre lesquels il y a interaction:

— le niveau de base: l'entreprise;

— le niveau intermédiaire: un secteur professionnel, une branche d'activités;

— le niveau national: les ministères et les administrations où se prennent les décisions stratégiques; en France, les services de renseignement (DST, DGSE, DRM) sont concernés;

— le niveau transnational: les groupes multinationaux;

— le niveau international où les États se livrent à des stratégies d'influence.

Momenteel stellen vele grote groepen zich nog tevreden met het beoefenen van technologische en concurrentiële bewaking. Daarnaast doen ze ook aan «*benchmarking*», dat is het onderzoeken, bij de concurrenten, welke de meest performante methodes zijn om een bepaalde activiteit te verrichten, teneinde een bepaald overwicht te verwerven. Economische informatie begint zich echter ook in de bedrijfswereld te ontwikkelen.

Sommige Franse universiteiten en hogescholen organiseren specifieke opleidingen inzake technologische bewaking en economische informatie. Op het einde van de opleiding wordt een *Diplôme d'études approfondies* (DEA) uitgereikt. De personen die een dergelijke opleiding volgen, zijn vooral wetenschappers, houders van een *maîtrise* (licentiaatsdiploma) of van een ingenieursdiploma.

De informatiebronnen

Op het gebied van economische informatie bestaat er een heel ruime waaier van informatiebronnen, gaande van wetenschappelijke informatie tot economische, politieke en financiële informatie. Het raadplegen van externe «open bronnen» is hier van doorslaggevend belang.

Tot die open bronnen behoren:

— computerdatabases die steeds vaker toegankelijk zijn via het internet;

— raadplegen van tijdschriften, kranten, diverse periodieke publicaties onmiddellijk na hun verschijning, teneinde sneller in het bezit te komen van de informatie dan via een database;

— gespecialiseerde tijdschriften, boeken, encyclopedieën, thesissen en proefschriften;

— octrooien waarvan de informatieve inhoud kan worden geëxploiteerd met het oog op het ontdekken van nieuwe technologieën, de algemene bewaking van technische sectoren en van de concurrenten;

— de rapporten van adviseurs op ambassades;

— de websites van ondernemingen; er bestaan ook economische informatiesites;

— de jaarverslagen van ondernemingen;

— bestaande wetsbepalingen en wetsbepalingen in voorbereiding: een actief beleid inzake lobbying is niet volledig indien men niet actief deelneemt aan het opstellen van de normen;

— congressen en colloquia;

— discussieplatforms op het internet;

— tentoonstellingen en beurzen waar het interessant is de prospectussen en monsters van concurrenten te verzamelen;

— «multi-client»-onderzoeken die gespecialiseerde firma's op bestelling voeren.

Actuellement, de nombreux grands groupes économiques se contentent encore de pratiquer la veille technologique et concurrentielle, ainsi que le «*benchmarking*» c'est-à-dire la recherche, chez les concurrents, des méthodes les plus performantes pour une activité donnée, afin de s'assurer une supériorité. Mais l'intelligence économique commence aussi à se développer dans les entreprises.

Certaines universités et grandes écoles françaises dispensent des formations spécifiques à la veille technologique et à l'intelligence économique. Ces formations aboutissent à la délivrance de Diplômes d'études approfondies (DEA). Les étudiants de ce DEA sont en majorité des scientifiques, titulaires d'une maîtrise ou d'un diplôme d'ingénieur.

Les sources d'information

En intelligence économique, la variété des sources d'information est extrême, allant de l'information scientifique à l'information économique, politique et financière. La consultation des «sources ouvertes» externes est ici essentielles.

On peut notamment citer:

— les bases informatiques de données de plus en plus accessibles via l'internet;

— la consultation de revues, journaux, publications périodiques diverses dés la parution de manière à capter l'information plus rapidement que sur les bases de données;

— les revues spécialisées, les ouvrages, les encyclopédies, les thèses universitaires;

— les brevets dont le contenu informatif peut être exploité pour la détection de technologies nouvelles, la surveillance globale de secteurs techniques et de la concurrence;

— les rapports des conseillers d'ambassades;

— les sites internet des entreprises; il existe aussi des sites d'intelligence économique;

— les rapports annuels d'activité des entreprises;

— les normes juridiques présentes et en projet: une politique active de lobbying ne se conçoit pas sans participer activement à l'élaboration des normes;

— les congrès et les colloques;

— les forums de discussion sur l'internet;

— les expositions et les foires où il est intéressant de récolter les prospectus et les échantillons de la concurrence;

— les études multi-clients réalisées sur commande par des firmes spécialisées.

Voor een onderneming is het raadplegen van haar rapporten en interne nota's een heel belangrijke technologische informatiebron die ze niet mag verwaarlozen. Sommige grote groepen hebben interne gegevensbanken aangelegd, waarin men gemakkelijk opzoekingen kan verrichten en waar de *knowhow* van de onderneming is opgeslagen. Het hoeft geen betoog dat deze interne gegevensbanken het bevoorrecht doelwit zijn van economische spionage.

Ook het opsporen en verzamelen van informele inlichtingen zijn heel belangrijke operaties binnen het kader van economische informatie. In dit geval gaat het om niet-gestructureerde of gevoelige informatie of om informatie die heel moeilijk verkrijgbaar is. Ze kan alleen worden ingewonnen via netwerken van «gespecialiseerde correspondenten» bij klanten, onderaannemers, ontwerpers van industriële installaties, handelsafgevaardigden, enz. Deze informatie heeft in hoofdzaak betrekking op de noden van de klanten, de voorzienbare vervanging van een product, zijn ontwikkeling, de projecten van de concurrenten.

Om dit type informatie, dat men niet aantreft in klassieke gegevensbanken, op te sporen is het nodig een inlichtingenplan op te stellen.

Economische informatie of economische spionage?

Volgens François Jakobiak «heeft elke specialist inzake economische informatie er belang bij te bestuderen wat de specialisten van Landsverdediging op dit domein hebben verwezenlijkt of geschreven, teneinde er de nodige lessen uit te trekken». Aan bedrijven geeft hij de raad een inlichtingenplan op te stellen, naar het voorbeeld van de Franse inlichtingendiensten. In de voorbeelden van plannen die werden voorgesteld, vinden we inderdaad de typische operaties terug van de militaire inlichtingencyclus (verwerven, beoordelen, interpreteren, communiceren van de inlichting).

François Jakobiak legt er echter de nadruk op dat men op het gebied van economische informatie ernaar moet streven gebruik te maken van open informatie. Dit komt niet noodzakelijk overeen met de praktijken van de inlichtingendiensten, «die gewoon zijn in opdracht van de regering in de clandestiniteit te werken».

In Frankrijk staan vele bedrijfsleiders overigens vrij wantrouwig tegenover het begrip «economische intelligentie». Ze denken daarbij automatisch aan de spionageactiviteiten van de Britse «Intelligence Service» of van het Amerikaanse «Central Intelligence Agency».

Ervan bewust dat we ons hier bevinden op de grens tussen open en gesloten informatie (dat is informatie die niet goedschiks wordt verstrekt), wijst François Jakobiak er op dat men bedrijfsspionage en economi-

Pour une entreprise, la consultation de ses rapports et notes internes est une source très importante d'information technologique qui ne doit pas être négligée. Un certain nombre de grands groupes ont constitué des banques de données internes aisément interrogeables où se trouve archivé le savoir-faire de la société. Ces banques de données internes constituent naturellement la cible privilégiée de l'espionnage économique.

La recherche et la collecte de renseignements informels, sont aussi des opérations capitales en intelligence économique. Il s'agit d'une information non structurée, délicate ou très difficile à obtenir et qui ne peut être recueillie que par des réseaux de «correspondants spécialisés» auprès des clients, des sous-traitants, des concepteurs d'installations industrielles, des délégués commerciaux, etc. Cette information concerne essentiellement les besoins de la clientèle, le remplacement prévisible d'un produit, son évolution, les projets des concurrents.

La recherche de ce type d'information, qui n'a aucune chance d'être obtenu sur les bases de données traditionnelle, doit faire l'objet d'un plan de renseignement.

Intelligenceéconomiqueouespionnageéconomique?

Selon François Jakobiak, tout spécialiste de l'intelligence économique a intérêt à étudier ce que les spécialistes de la Défense nationale ont réalisé ou écrit dans ce domaine pour en tirer de profitables leçons. Et le conférencier de préconiser aux entreprises l'établissement de plans de renseignement semblables à ceux des services de renseignement français. On retrouve en effet dans les modèles de plans proposés les opérations typiques du cycle du renseignement militaire (acquisition, appréciation, interprétation, communication du renseignement).

François Jakobiak insiste néanmoins sur le fait que l'intelligence économique doit s'attacher à utiliser l'information ouverte, ce qui n'est pas nécessairement le cas des services de renseignement, «habitués, quant à eux, à opérer dans la clandestinité au profit du gouvernement».

En France, beaucoup de chef d'entreprises se méfient d'ailleurs du terme «intelligence économique», car il évoque pour eux les activités d'espionnage de l'«Intelligence Service» britannique ou de la «Central Intelligence Agency» américaine.

Conscient que l'on se trouve ici à la frontière de l'information ouverte et de l'information fermée (celle qui n'est pas donnée de plein gré), François Jakobiak rappelle pourtant qu'il ne faut pas faire

sche intelligentie niet met elkaar mag verwarren. Het is dan ook heel belangrijk de ethiek en de deontologie van de ondernemingen ter zake goed te definiëren. Welke grenzen mag men in geen geval overschrijden?

François Jakobiak stelt voor de volgende regels in acht te nemen:

— alleen open informatie komt in aanmerking;

— discretie is geboden, maar men moet beseffen dat men vaak inlichtingen krijgt wanneer men er zelf in ruil geeft;

— elke correspondent beslist zelf welke informatie hij al dan niet vrijgeeft;

— er wordt op gehamerd om blijk te geven van fair play.

De beoefenaars van economische intelligentie

De beoefenaars van de economische intelligentie zijn afkomstig van vier «verschillende scholen»:

— de specialisten inzake technologische bewaking vormen de eerste school en zijn meestal ingenieurs die heel goed de noodzaak hebben ingezien te evolueren naar economische informatie;

— de tweede school is meer commercieel geïnspireerd; het is de school van de specialisten inzake marketing of concurrentieanalyse;

— tot de derde school behoren specialisten inzake militaire inlichtingen, die zich hebben omgeschoold tot het domein van de economische informatie;

— de aanhangers van de vierde school zijn politieambtenaren die hun kennis van onderzoekstechnieken en van het verzamelen van inlichtingen meebrengen.

Beïnvloeding en lobbying

Het rapport-Martre zegt niets over beïnvloeding en lobbying in zijn voorstellen over het ontwikkelen van de economische informatie in de Franse bedrijven. Beïnvloeding zou dus veeleer behoren tot de economische informatie die door de Staat wordt beoefend. Aangezien de mogelijkheden inzake beïnvloeding en lobbying van de bedrijven beperkter zijn dan die van de Staat, doen ze soms een beroep op officiële instanties, op ministeries of op internationale organen om hun belangen te beschermen, vooral met betrekking tot het opstellen van normen. Japan heeft zich daarin gespecialiseerd.

In de Verenigde Staten zien we een nieuw type *knowhow* ontstaan, dat «InfoWar» wordt genoemd. Dit betekent dat een land zijn industrieën gaat beschermen door zijn informatierijkdommen (onder meer elektronische structuren zoals het internet) te mobiliseren en op die manier een beleid van

d'amalgame entre l'espionnage industriel et l'intelligence économique. Il est donc impératif de bien définir l'éthique et la déontologie de l'entreprise en cette matière. Quelles sont les limites à ne pas franchir?

Et François Jakobiak de proposer la mise en œuvre des quelques préceptes suivants:

— seule l'information ouverte est prise en compte;

— la discrétion est de mise mais il faut savoir que l'on obtient souvent des renseignements en en fournissant soi-même en échange;

— il appartient à chaque correspondant de juger de ce qu'il peut dire ou ne pas dire;

— il est vivement recommandé de faire preuve de fair-play.

Les praticiens de l'intelligence économique

Les praticiens de l'intelligence économique proviennent de quatre «écoles» différentes:

— les spécialistes de la veille technologique constituent la première école et sont le plus souvent des ingénieurs qui ont fort bien compris la nécessité d'évoluer vers l'intelligence économique;

— la seconde école, d'inspiration plus commerciale, est celle des spécialistes du marketing ou de l'analyse concurrentielle;

— la troisième école est constituée par des spécialistes du renseignement militaire reconvertis dans l'intelligence économique;

— une quatrième école provient de fonctionnaires de police qui apportent leur connaissance des techniques d'enquêtes et de collecte de renseignements.

Influence et lobbying

Le rapport Martre ne mentionne pas l'influence et le lobbying dans ses propositions relatives au développement de l'intelligence économique dans les entreprises françaises. L'influence serait donc plutôt une des composantes de l'intelligence économique d'État. Les possibilités d'influence et de lobbying des entreprises étant plus limitées que celles de l'État, il arrive donc que celles-ci s'adressent à des organismes officiels, à des ministères ou à des organismes internationaux pour défendre leurs intérêts, notamment au niveau de l'élaboration des normes. Le Japon s'en est d'ailleurs fait une spécialité.

Aux États-Unis, on voit émerger un savoir-faire de type nouveau, celui de l'«InfoWar». Il s'agit pour une nation, de défendre ses industries en mobilisant ses ressources informationnelles (dont les structures électroniques comme l'internet) pour mettre en œuvre des politiques d'influence fondées sur des guerres de

beïnvloeding te ontwikkelen dat steunt op informatieoorlogen, dit wil zeggen het bezorgen van destabiliserende informatie aan belangrijke actoren.

De informatieoorlog is dus het offensieve gebruik van de informatie teneinde een tegenstander te verzwakken, te destabiliseren of te vernietigen. Tot de aangewende technieken behoren de desinformatie, het manipuleren van informatie, het verspreiden van geruchten of het voeren van propaganda. Men kan dergelijke methodes alleen voorkomen en bestrijden indien men zelf ook de aanvalstechnieken van de informatieoorlog beheerst.

Conclusies van het Comité I

Economische intelligentie, dat is de systematische exploitatie van de informatie om strategische beslissingen te nemen op economisch gebied, is het gevolg van de globalisering van het handelsverkeer en van de sterke concurrentie in deze sector. Net als op militair vlak komt het er in de eerste plaats op aan zelf goed geïnformeerd te zijn, de informatie goed te interpreteren, dienovereenkomstig te handelen en, zo nodig, de informatie offensief aan te wenden. Deze praktijk krijgt steeds vaker een plaats in het management en de strategie van grote ondernemingen. Ook de Staat zelf moet een belangrijke rol gaan spelen op het vlak van economische intelligentie.

In België is er onlangs een eerste stap in die richting gezet. De Veiligheid van de Staat werd immers belast met de opdracht bij te dragen tot de bescherming van het wetenschappelijk en economisch potentieel van het land. Voorlopig gaat het om een louter defensieve maatregel.

De Veiligheid van de Staat zal haar nieuwe opdracht echter alleen naar behoren kunnen uitvoeren indien:

— ze de nodige personele en materiële middelen krijgt;

— ze zelf doordrongen raakt van deze nieuwe cultuur die economische intelligentie inhoudt.

Daartoe moet de Veiligheid van de Staat nauwe relaties aanknopen met de economische actoren van ons land.

DEELNAME VAN HET COMITE I AAN WERKVERGADERINGEN,SEMINARIES,CONFERENTIES EN COLLOQUIA GEDURENDE HET DIENSTJAAR 2000

— Conferentie georganiseerd door het «Koninklijk Hoger Instituut voor Defensie (KHID)» over het thema «Waar gaat Rusland naartoe?» — 1 maart 2000.

— Conferentie van de heer R. Steele, georganiseerd door de Comités P en I — thema: «The recent

l'information, c'est-à-dire la diffusion aux acteurs décisifs d'informations déstabilisatrices.

La guerre de l'information est donc l'utilisation offensive de l'information afin d'affaiblir, de déstabiliser, ou de détruire un adversaire. Les techniques utilisées peuvent être la désinformation, la manipulation d'information, les rumeurs ou la propagande. On ne peut prévenir et lutter contre ces méthodes qu'en maîtrisant soi-même les techniques offensives de la guerre de l'information.

Conclusions du Comité R

L'intelligence économique, exploitation systématique de l'information pour des décisions stratégiques dans le domaine économique, résulte de la mondialisation des échanges et la vigueur de la compétition qui règne dans ce secteur. Comme dans le domaine militaire, il s'agit d'abord d'être bien informé, de bien interpréter, d'agir en conséquence et de faire, si nécessaire, un usage offensif de l'information. Cette pratique s'intègre de plus en plus au management et à la stratégie des grandes entreprises. L'État est lui-même appelé à jouer un rôle important dans l'intelligence économique.

En Belgique, un premier pas vient d'être franchi dans ce sens puisque la Sûreté de l'État a reçu la mission de participer à la protection du potentiel scientifique et économique du pays. Il ne s'agit encore que d'une démarche de nature défensive.

La Sûreté de l'État de l'État ne sera pourtant en mesure de s'acquitter de sa nouvelle mission que si:

— elle reçoit des moyens humains et matériels nécessaires;

— elle s'imprègne de cette nouvelle culture qu'est l'intelligence économique.

Il lui sera nécessaire à cet effet de tisser des liens étroits avec les acteurs économiques du pays.

PARTICIPATION AU COURS DE L'ANNÉE 2000 DU COMITÉ R À DES RÉUNIONS DE TRAVAIL, SÉMINAIRES,CONFÉRENCESETCOLLOQUES

— Conférence organisée le mercredi 1er mars 2000 par «L'Institut supérieur de défense (IRSD)» sur le thème: «Où va la Russie?».

— Conférence de R. Steele organisée par les Comités P et R sur le thème: «The recent developments in

developments in the field of open source intelligence in North-America» -— 14 april 2000.

— Deelname aan het seminarie: «Maîtriser les outils de la veille économique» georganiseerd in Parijs door het «Institute for International Research» — 16 en 17 mei 2000.

— Deelnemen aan de conferentie 18, 18 en 19 mei 2000 door het «Haut Comité français pour la défence civile» te Lyon over het thema «Le risque biologique».

— Op 2 augustus 2000 hebben de Comités P en I het bezoek gekregen van twee leden van de parlementaire begeleidingscommissies.

— Op 18 september 2000 hebben de leden van het Comité I deelgenomen aan een informatievergadering voor de stagiairs van de Veiligheid van de Staat. Er werden verschillende uiteenzettingen voorgesteld betreffende de organieke wetgeving inzake het toezicht en de rol van het Comité I.

— 3 oktober 2000 avondconferentie van het KHID: «Internationale betrekkingen. Rol van de diplomatie en potentiële samenwerking met militairen».

— Op 23 oktober 2000 heeft het Comité I een gedachtenwisseling georganiseerd met de verantwoordelijke van de Anti-terroristische Gemengde Groep (AGG) waarin zowel de Veiligheid van de Staat als de Algemene Dienst Inlichting en Veiligheid vertegenwoordigd is.

— Op 27 oktober 2000 hebben de Comités P en I deelgenomen aan een informatievergadering over het communicatienetwerk ASTRID.

— 7 november 2000: avondconferentie van het KHID: «Internationale oorlogstribunalen»

— Deelname aan het «EuFis»-seminarie met als thema: «Open Source Workshop» georganiseerd te Brussel op 19 en 20 oktober 2000.

— 29 november 2000 KHID, conferentie over het thema: «Vredesondersteunende en humanitaire operaties en civiel-militaire samenwerking».

— Op 1 december 2000 heeft de Senaat een gedachtenwisseling georganiseerd met de heer Duncan Campbell betreffende «Echelon».

— Conferentie georganiseerd te Parijs op 7 en 8 december 2000 door het «Haut Comité français pour la défense civile» met als thema: «La défense civile de la France à l'aube du XXIe siècle: constat et avenir».

the field of open source intelligence in North-America» le 14 avril 2000.

— Participation au séminaire «Maîtriser les outils de la veille économique» organisé à Paris les 16 et 17 mai 2000 par «L'institute for International Research».

— Participation à la Conférence organisée par le «Haut Comité français pour la défense civile» à Lyon les 17, 18 et 19 mai 2000 par sur le thème: «Le risque biologique».

— Le 2 août 2000, les Comités P et R ont reçu la visite de deux membres des commissions parlementaires de suivi.

— Le 18 septembre 2000, les membres du Comité R ont participé à une séance d'information des stagiaires de la Sûreté de l'État. Divers exposés ont été présentés à cette occasion concernant la législation organique du contrôle et le rôle du Comité R.

— Le 3 octobre 2000, conférence du soir de l'IRSD «Les relations internationales. Le rôle de la diplomatie et les possibilités de coopération avec les militaires».

— Le 23 octobre 2000, le Comité R a organisé un échange de vues avec un responsable du Groupe-Interforces anti-terroristes (GIA) au sein duquel la Sûreté de l'État et le SGR sont représentés.

— Le 27 octobre 2000, les Comités P et R ont participé à une séance d'information sur le réseau de communication ASTRID.

— Le 7 novembre 2000, conférence du soir de l'IRSD «Les tribunaux internationaux».

— Participation au séminaire «Eufis» organisé à Bruxelles les 19 et 20 octobre 2000 sur le thème: «Open Source Workshop».

— Le 29 novembre 2000 conférence de l'IRSD organisée sur le thème «Des opérations humanitaires de soutien de la paix et la coopération civilo-militaire».

— Le 1er décembre 2000 échange de vues organisé par le Sénat avec Duncan Campbell concernant le système d'écoutes «Echelon»

— Conférence organisée à Paris les 7 et 8 décembre 2000 par le Haut Comité français pour la défense civile sur le thème «La défense civile de la France à l'aube du XXIe siècle — constat et avenir.»

TITEL IV

SAMENSTELLING EN WERKING VAN HET COMITE I

Samenstelling

Sinds de benoeming op 26 november 1999 van mevrouw Danielle Cailloux, als lid van het Vast Comité van toezicht op de politiediensten (Comité P), die tot op die datum deel uitmaakte van het Comité I, hebben de drie overblijvende leden de uitoefening van hun mandaat verdergezet.

De wet van 1 april 1999 (*Belgisch Staatsblad* van 3 april 1999) tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten had de samenstelling van het Comité I beperkt tot één permanent werkend lid, de voorzitter, en twee niet-permanente werkende leden.

De wet van 20 juli 2000 (*Belgische Staatsblad* van 1 augustus 2000) heeft de samenstelling van het Comité I opnieuw gewijzigd, te weten drie voltijdse leden waaronder één voorzitter. Voor elk van hen wordt een plaatsvervanger benoemd.

Bij de goedkeuring van het huidig activiteitenverslag is de benoeming van de drie nieuwe leden van het Comité I nog niet gebeurd, zodat de huidige momenteel in functie zijnde leden zijn:

de heer Jean-Claude Delepière, voorzitter

de heer Gérald Vande Walle, lid

de heer Jean-Louis Prignon, lid.

Deze personen blijven hun functie uitoefenen zolang hun vervangers niet zijn benoemd.

De griffier

Het Comité I wordt bijgestaan door een griffier die ook door de Senaat wordt benoemd. Hij staat in voor het secretariaat van de vergaderingen van het Comité I, stelt de notulen van deze vergaderingen op en ziet er op toe dat de stukken worden verstuurd en in het archief worden opgeslagen. De griffier is ook verantwoordelijk voor de bescherming van het geheim van de documentatie en het archief. Zijn mandaat is van onbepaalde duur. Net als de leden van het Comité I moet hij houder zijn van een veiligheidsmachtiging van het niveau «zeer geheim».

De huidige griffier van het Comité I is de heer Wouter De Ridder.

De Dienst Enquêtes

Het huidig kader van de Dienst Enquêtes bestaat uit vijf personen.

TITRE IV

COMPOSITION ET FONCTIONNEMENT DU COMITÉ R

Composition

Depuis la nomination, le 26 novembre 1999, comme membre du Comité permanent de contrôle des services de police (Comité P), de Mme Danielle Cailloux qui faisait partie jusqu'à cette date du Comité R, les trois membres restant ont poursuivi l'exercice de leur mandat.

La loi du 1er avril 1999 (*Moniteur belge* du 3 avril 1999) modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements avait réduit la composition du Comité R à un seul membre effectif permanent, le président, et à deux membres effectifs non permanents.

La loi du 20 juillet 2000 (*Moniteur belge* du 1er août 2000) a modifié à nouveau la composition du Comité R. Celui-ci comportera trois membres à temps plein parmi lesquels un président. Un suppléant sera nommé pour chacun d'eux.

À la date d'approbation du présent rapport général d'activités, la nomination des trois nouveaux membres du Comité R n'est pas encore intervenue, de sorte que les trois membres encore en fonction sont:

M. Jean-Claude Delepière, président

M. Gérald Vande Walle, membre

M. Jean-Louis Prignon, membre

Ceux-ci continuent à exercer leurs fonctions jusqu'à la nomination de leurs remplaçants.

Le greffier

Le Comité R est assisté d'un greffier, lui aussi nommé par le Sénat. Il assure le secrétariat des réunions du Comité R, en dresse les procès-verbaux et veille à l'expédition des pièces et à la conservation des archives. Le greffier est également responsable de la protection du secret de la documentation et des archives. Sa fonction est d'une durée indéterminée. Comme les membres du Comité R, il doit être titulaire d'une habilitation de sécurité du niveau «très secret».

Le greffier actuel du Comité R est M. Wouter De Ridder.

Le Service d'enquêtes

Le cadre actuel du Service d'enquêtes est de cinq personnes.

Het hoofd van de Dienst Enquêtes wordt door het Comité I benoemd voor een periode van vijf jaar die eenmaal kan worden verlengd. Het moet een ervaren persoon zijn die wordt gekozen onder de magistraten, de leden of ambtenaren van de inlichtingen- of politiediensten. Hij moet de Nederlandse en Franse taal machtig zijn. Momenteel staat de heer Paul vander Straeten, eerste substituut van de procureur des Konings bij het parket van Brussel, aan het hoofd van de Dienst Enquêtes.

De leden van de Dienst Enquêtes worden door het Comité I benoemd op voorstel van het hoofd van deze Dienst. Om benoemd te kunnen worden moeten het hoofd en de leden van de Dienst Enquêtes eveneens houder zijn van een veiligheidsmachtiging van het niveau « zeer geheim ».

De huidige vier leden van de Dienst Enquêtes zijn benoemd voor een periode van vijf jaar die kan worden verlengd; ze zijn gedetacheerd van een politie- of inlichtingendienst.

Tijdens het afgelopen dienstjaar werd het mandaat van twee leden van de Dienst Enquêtes hernieuwd.

Het administratief personeel

Tijdens het voorbije jaar werd een documentaliste van niveau 1 aangeworven.

Bij de publicatie van het huidig activiteitenverslag bestaat het administratief kader uit de volgende medewerkers :

— één documentaliste in statutaire dienst;
— één boekhouder in statutaire dienst;
— één sécretaresse in statutaire dienst;
— één bediende in statutaire dienst;
— één bode in statutaire dienst;
— één receptionniste in statutaire dienst;
— één chauffeur-technicus ter beschikking gesteld door de Krijgsmacht.

De activiteiten

Tussen 1 januari 2000 en 31 december 2000 heeft het Comité I vijftig keer vergaderd. Op deze plenaire vergaderingen worden beslissingen genomen inzake de onderzoeken, de teksten voor het jaarverslag en de logistiek.

De leden van het Comité I hebben twaalf keer vergaderd met de parlementaire begeleidingscommissies.

Daarenboven heeft het Comité I eveneens een ontwerp van koninklijk besluit opgesteld om aan zijn leden alsook aan de leden van zijn Dienst Enquêtes de

Le chef du Service d'enquêtes est nommé par le Comité R pour un terme de cinq ans renouvelable une fois. Il doit être une personne d'expérience choisie parmi des magistrats, des membres ou des fonctionnaires des services de renseignements ou de police. Il doit connaître les langues française et néerlandaise. Le chef actuel du Service d'enquêtes est M. Paul vander Straeten, premier substitut du procureur du Roi au parquet de Bruxelles.

Les membres du Service d'enquêtes sont nommés par le Comité R sur proposition du chef du Service d'enquêtes. Pour pouvoir être nommés, le chef et les membres du Service d'enquêtes doivent également être titulaires d'une habilitation de sécurité du niveau « très secret ».

Les quatre membres actuels du Service d'enquêtes ont été nommés pour un terme renouvelable de cinq ans par détachement d'un service de police ou de renseignement.

C'est ainsi qu'au cours de l'exercice écoulé, les mandats de deux membres du Service d'enquêtes ont été renouvelés pour un nouveau terme.

Le personnel administratif

Au cours de l'année 2000, le recrutement d'une collaboratrice-documentaliste de niveau 1 a été concrétisé.

À la parution du présent rapport d'activités, le cadre administratif du Comité R se compose donc des collaborateurs suivants :

— une documentaliste;
— un comptable à titre statutaire;
— une secrétaire à titre statutaire;
— une employée à titre statutaire;
— un huissier à titre statutaire;
— une réceptionniste à titre statutaire;
— un chauffeur-technicien mis à disposition par les Forces armées.

Les activités

Le Comité R s'est réuni du 1er janvier 2000 au 31 décembre 2000, cinquante fois. Lors de ces réunions, des décisions ont été prises concernant les enquêtes, les textes du rapport d'activités et la logistique.

Les membres du Comité R se sont réunis 12 fois avec les commissions de suivi parlementaire.

Outre ce qui est repris au chapitre I, le Comité R a également établi un projet d'arrêté royal permettant à ses membres ainsi qu'aux membres de son Service

toegang te verlenen tot het Rijksregister van de natuurlijke personen.

Dit ontwerp werd op 6 december 2000 aan de ministers van Binnenlandse Zaken en van Justitie gestuurd.

d'enquêtes d'accéder au Registre national des personnes physiques.

Ce projet a été transmis aux ministres de l'Intérieur et de la Justice par courrier du 6 décembre 2000.

De financiële middelen

De middelen van het Comité I komen voort uit een dotatie die jaarlijks toegekend wordt door het Parlement.

Sinds de wet van 1 april 1999 is de griffier de rekenplichtige van het Comité I. Het huishoudelijk reglement van het Comité I stelt een interne controle op de uitgaven in. Deze wordt uitgevoerd door een lid van het Comité I.

De uitvoering van de begroting wordt gecontroleerd door het Rekenhof, dat jaarlijks een verslag opstelt in opdracht van de Kamer van volksvertegenwoordigers.

De dotatie van het begrotingsjaar 2000 bedroeg 72 450 000 frank.

Voor het jaar 2001 werd een budget van 73 480 000 frank aangevraagd.

Les moyens financiers

Les moyens du Comité R proviennent d'une dotation qui lui est accordée annuellement par le Parlement.

Depuis la loi du 1er avril 1999, le greffier est responsable des comptes du Comité R. Le règlement interne du Comité R prévoit un contrôle interne des dépenses. Celui-ci est effectué par un des membres du Comité R.

L'exécution du budget est contrôlée par la Cour des comptes, qui établit chaque année un rapport à la demande de la Chambre des représentants.

La dotation de l'année budgétaire 2000 se montait à 72 450 000 francs.

Un budget de 73 480 000 francs a été demandé pour l'année 2001.

Gemeenschappelijke activiteiten met het Comité P

Tijdens de vernoemde referteperiode hebben de twee Comités P en I vier gemeenschappelijke vergaderingen gehouden.

Er werd eveneens een werkgroep opgericht, samengesteld uit leden van de beide Comités, de griffiers, alsook vertegenwoordigers van het administratief personeel; zij kwamen tijdens het dienstjaar 2000, vijftien maal bijeen om een ontwerp van tekst met het nieuwe statuut voor het administratief personeel op te stellen. Het ontwerp werd op 7 juli 2000 aan de voorzitter van de Kamer van volksvertegenwoordigers toegezonden.

Activités conjointes avec le Comité P

Pendant la période de référence, les deux Comités P et R ont tenu 4 réunions conjointes.

De plus un groupe de travail, composé de membres des deux Comités, des greffiers ainsi que des représentants du personnel administratif, s'est réuni 15 fois au courant de l'exercice 2000 pour élaborer un projet de statut commun du personnel administratif. Ce projet a été finalisé. Il a été communiqué le 7 juillet 2000 au président de la Chambre des représentants.

59.106 — E. Guyot, n. v., Brussel