COMITE PERMANENT DE CONTROLE

DES SERVICES DE RENSEIGNEMENTS

RAPPORT D'ACTIVITES

1998

A Monsieur le Président du Sénat,
A Monsieur le Président de la Chambre des Représentants,
A Monsieur le Ministre de la Justice,
A Monsieur le Ministre de la Défense nationale,

Messieurs les Présidents,
Messieurs les Ministres,

En exécution de l'article 35 de la loi organique du 18 juillet 1991, instituant le contrôle des services de police et de renseignement, le Comité permanent de contrôle des services de renseignement à l'honneur de vous adresser en annexe le cinquième rapport général d'activités.

Ce rapport couvre la période du 1er août 1997 au 31 juillet 1998.

Nous vous prions de croire, Messieurs les Présidents, Messieurs les Ministres, en l'assurance de notre très haute considération.

Véronique Paulus de Châtelet
Présidente

Danielle Cailloux
Conseiller

Guy Collignon
Conseiller

Gérald Vande Walle
Conseiller

Wouter De Ridder
Greffier

TABLE DES MATIERES

TITRE I : CE QUI SE PASSE A L’ETRANGER

ETUDE DE LA LEGISLATION DU ROYAUME-UNI RELATIVE AUX SERVICES DE RENSEIGNEMENTS ET DE SECURITE

1. INTRODUCTION

Dans ses rapports d'activités précédents, le Comité R a publié :

- une étude comparative entre certaines législations étrangères applicables aux services de renseignement et de sécurité[(1)];
- la législation allemande relative aux services de renseignement et aux organes de contrôle [(2)];
- la législation néerlandaise relative aux services de renseignement et au contrôle de ces services [(3)].

Le présent rapport aborde la législation anglaise relative aux services de renseignement et aux organes de contrôle de ces services.

Une différence essentielle doit, en guise de préambule, être mise en exergue : les règles de droit au Royaume-Uni sont différentes de celles de la Belgique. Au Royaume-Uni les juges s'appuient principalement sur la coutume et sur la "règle du précédent" pour trancher (Common Law). En Belgique, nous fonctionnons dans un système de droit écrit; les tribunaux sont tenus d'appliquer la loi que le Parlement vote.

En conséquence, de nombreuses matières sont partiellement ou ne sont pas réglées par la loi au Royaume-Uni. La législation britannique applicable aux service de sécurité et de renseignement illustre bien cette différence, à l'exception des dispositions légales relatives à la violation des propriétés et des interceptions de communications.

La comparaison des deux systèmes britannique et belge, et l'approche critique du système britannique nécessite de tenir compte de ces différences.

---

(1) Voir rapport d'activités 1995

(2) Voir rapport d'activités 1996

(3) Voir rapport d'activités 1997

En vue de ne pas se limiter à une étude des textes et donc d'essayer d'appréhender le côté pragmatique du système britannique, le Comité R a rencontré le président et le greffier du "Intelligence and Security Committee", l'organe parlementaire chargé de la surveillance des divers services de renseignement et de sécurité.

Le Comité R a également pu avoir un entretien avec le "Co-ordinator", personne chargée de la coordination entre les trois services de renseignement et de sécurité, le gouvernement et les services de police.

Il va de soi que, durant ces visites, seules des questions concernant le fonctionnement des services ont été posées à l'exclusion des opérations proprement dites des services de renseignement.

Le Comité R a reçu à cette occasion plusieurs rapports établis tant par les commissaires du gouvernement que par "The Intelligence and Security Committee".

Le 26 mai 1998, le Comité R a rencontré M. David Bickford, ancien conseiller juridique du "Security Service" et de l' "Intelligence Service".

Dans le cadre de cette étude, le Comité R développera les points suivants :

- les services et leur base légale;
- les missions des services;
- les compétences des services et la responsabilité de leurs responsables;
- les méthodes spéciales des services;
- les organes de contrôle;
- la politique en matière de services de renseignement et de sécurité;
- le contrôle parlementaire;
- une approche critique.

2. LES SERVICES ET LEUR BASE LEGALE

2.1. Historique

Le Royaume-Uni compte trois services de renseignements et de sécurité :

- the Security Service (le service de sécurité);
- the Secret Intelligence Service (le service secret de renseignement);
- the Government Communication Headquarters (GCHQ).

A l'origine, ces trois services faisaient partie de l'armée. Aucun texte légal ne réglait leurs compétences et leur contrôle. Une directive datant de 1952 décrit le travail du "Security Service" et la responsabilité du Directeur général.

A cette époque, le "Secret Intelligence Service" et le "GCHQ" travaillaient dans le secret le plus absolu.

A côté de ces trois services existe le "Defense Intelligence Staff" (DIS) relevant du ministère de la Défense nationale et représentant un élément essentiel dans l'appareil de renseignement.

Il fut constitué en 1964 par la fusion des trois organes de renseignement des différentes forces armées et du "Joint Intelligence Bureau", en vue de créer une organisation intégrée pouvant servir les intérêts du ministère de la Défense nationale, de l'armée et d'autres ministères.

Toutefois, le "DIS" n'est pas un véritable service de renseignement. En effet, ce service ne collecte aucun renseignement à l'inverse des services de renseignement et de sécurité. La mission du DIS consiste à analyser les informations issues d'un large éventail de sources, publiques ou secrètes.

Le chef du DIS est responsable du travail fourni par son service. Il cumule cette fonction avec la direction générale de la mission de renseignement de la Défense nationale

Il n'existe pas au Royaume-Uni un véritable service de renseignement militaire, même si un "intelligence corps" recueille des informations de nature tactique (par opposition aux informations de nature politique ou économique) et ce uniquement au sujet des pays où le Royaume-Uni envoie des troupes.

2.2. La base légale

En 1989 les Anglais se sont dotés d'une législation instaurant légalement le "Security Service" dénommé "Security Service Act 1989".

Cette loi a été complétée par la loi de 1994 et par le "Security Act 1996".

"The Intelligence Service Act 1994" a donné une base légale au "Secret Intelligence Service" et au "Government Communications Headquarters".

Cette loi a aussi instauré le "Intelligence and Security Committee" chargé du contrôle parlementaire des services de renseignement et de sécurité.

"The Interception of Communications Act 1985" permet aux services de renseignement de solliciter l'autorisation de procéder à l'interception de la correspondance et des communications téléphoniques.

2.3. Description sommaire des trois services

2.3.1.The Security Service (le Service de Sécurité)

Ce service, connu sous le nom de MI5, est chargé d'une mission assez large, à savoir garantir la sécurité de l'Etat.

Ce service est placé sous l'autorité du ministre de l'Intérieur; son personnel compte environ 2.000 personnes.

Depuis l'approbation de la seconde loi sur le Service de sécurité de 1996, la mission du service a été élargie et inclut le soutien aux services de police et autres services d'ordre en matière de lutte contre le crime organisé.

Leurs locaux se situent dans la Thames House à Londres.
Ce service peut être comparé à celui de la Sûreté de l'Etat belge.

2.3.2.The Secret Intelligence Service (le Service de renseignement)

Ce service, communément appelé MI6, a notamment pour mission de mener des opérations à l'étranger. Il est de nature offensive par rapport au Service de sécurité dont l'objectif est défensif. Il est placé sous l'autorité du ministre des Affaires étrangères; son personnel compte environ 2.000 personnes.

La mission principale de ce service consiste à recueillir des informations secrètes destinées à la sécurité, à la défense, aux lignes directrices de politique extérieure et économique du gouvernement, et ceci dans le cadre des besoins en informations définis par le "Joint Intelligence Committee" (JIC) et approuvés par les ministres.

Les locaux de "l'Intelligence Service" se situent à Vauxhall Cross, Londres.

La Belgique ne dispose pas d'un tel service "offensif" même si le projet de loi organique des services de renseignement et de sécurité précise les circonstances dans lesquelles les services de renseignement belges sont compétents pour exécuter des actions à l'étranger.

2.3.3.The Government Communications Headquarters (GCHQ)

Le "Government Communications Headquarters" fournit aux ministères et aux militaires des "signals intelligence" (des renseignements issus d'interceptions de télécommunications, également appelés "Sigint") afin de garantir la sécurité, la défense, les lignes de politiques économique et étrangère du gouvernement.

Le siège du GCHQ se situe à Cheltenham.

Le GCHQ rassemble des informations via un large éventail de systèmes de communication et d'autres systèmes, tel le radar. C'est dans cet objectif que le GCHQ contrôle et équipe la "Composite Signals Organisation" opérant depuis plusieurs postes au Royaume-Uni et à l'étranger.

Le GCGQ travaille en étroite collaboration avec plusieurs services de renseignement et de sécurité étrangers. Outre la transmission de renseignement sous forme de signaux, le GCHQ conseille également les ministères et les forces armées en matière de sécurité de leur communication et de leurs systèmes technologiques d'information.

Cette tâche est assurée par le "Communications Electronics Security Group" (le Groupe de sécurité en matière de communication électronique) du GCHQ qui travaille également en étroite collaboration avec les administrations, l'industrie et le Service de sécurité afin de s'assurer que l'information officielle est parfaitement protégée dans de tels systèmes.

Le GCGQ est placé sous l'autorité du ministre des Affaires étrangères; son personnel compte environ 5.500 membres. Au cours des années le nombre des agents travaillant pour ce service a diminué.

Le Premier ministre assume la responsabilité politique en matière de renseignement et de sécurité. Il est secondé dans cette tâche par le "Secretary of Cabinet" (le Secrétaire du Cabinet).

3. MISSIONS DES SERVICES

3.1. Security Service Act 1989 (la loi de 1989 relative au service de sécurité)

Le "Security Service" a pour mission :

- la protection de la sécurité nationale et, plus particulièrement, la protection de l'Etat contre les menaces suivantes :
  - l'espionnage;
  - le terrorisme;
  - le sabotage;
  - les activités d'agents à la solde de puissances étrangères;
  - les actions ayant pour objectif de déstabiliser la démocratie parlementaire ou de lui porter préjudice par des actes violents, politiques ou industriels.

- la protection du bien-être économique (The economic well-being) du Royaume-Uni contre les menaces résultant d'actions ou d'intentions de personnes se situant en dehors des îles britanniques.

Le service peut également intervenir pour soutenir les activités des services de police et d'autres services d'ordre dans le cadre de la prévention et de la lutte contre la grande criminalité.

La protection du bien-être économique du Royaume-Uni comprend la lutte contre les actes illicites de pays ou d'organisations étrangers.
Il s'agit non seulement d'espionnage mais aussi et surtout d'alliances économiques et de cartels (mafieux).

La mission de protection de la sécurité nationale est décrite de manière large et comprend toutes les formes de subversion. Le service peut déterminer ce que l'intérêt national comprend, sans que la définition de ce concept ne soit défini par la loi. Le législateur a ainsi voulu laisser place à une approche évolutive de cette notion.

La définition de la subversion donnée par The Security Service est contrôlée par le Commissaire du gouvernement et la Commission(4). Ces instances reçoivent les plaintes des personnes ou des groupements qui estiment avoir été lésées par les activités des services de renseignement. Ces instances disposent de la plus haute autorité.

Le Security Service établit une liste de règles qui permet de déterminer la subversivité d'une personne. Cette liste est remise chaque année au Commissaire du gouvernement qui l'accepte ou la refuse.

Sous sa responsabilité le ministre peut exiger qu'un individu ou un groupement soit repris dans ladite liste. Le Security Service peut refuser cet ajout. Cette divergence de position est tranchée par le Commissaire du gouvernement et la commission. Un débat peut également avoir lieu à ce sujet au Parlement.

Bien que cela ne soit pas prévu par la loi, le "Security Service" effectue aussi les enquêtes de sécurité. Chaque département délivre ensuite ses propres certificats de sécurité à son personnel car il n'existe pas d'autorité nationale de sécurité en Grande Bretagne.

Alors que des enquêtes de sécurité ("vetting") étaient déjà effectuées depuis une quarantaine d'années, le gouvernement a décidé en 1990 que la procédure de ces enquêtes devait être revue et exécutée sur base de critères bien définis et publics.

Le Premier ministre a donc fait en 1990 une déclaration devant le Parlement relative au "Statement of Vetting Policy". Cette déclaration concernant la politique des enquêtes de sécurité est entrée en vigueur le 1er octobre 1990.

(4) Cfr. 6.2. de la présente étude
Cfr 6.3. de la présente étude

Depuis cette date, toute personne devant être soumise à une enquête de sécurité doit remplir un questionnaire portant sur des données personnelles à vérifier dans leur chef. Ce questionnaire explique aussi la procédure suivie pour effectuer l'enquête.

La note gouvernementale part du principe que personne ne peut être désigné dans une fonction vitale pour la sécurité nationale s'il n'a pas fait au préalable l'objet d'une enquête de sécurité. Cette note mentionne les critères à prendre en considération ainsi que les divers niveaux d'enquêtes qui doivent être effectuées en fonction du degré du certificat à accorder.

Pour un certificat de sécurité du niveau "SECRET", les fichiers du "Security Service" et des services de police sont entre autres consultés. Dans certains cas, une enquête complémentaire est prescrite et le candidat est soumis à un interview.

Pour un certificat de sécurité du niveau "TOP SECRET", la solvabilité du candidat est vérifiée et une enquête complémentaire est effectuée sur sa personnalité auprès des membres de son entourage professionnel et familial.

La note gouvernementale prévoit également une enquête de fiabilité, par exemple pour les personnes qui ont une possibilité d'accès sans accompagnement à des bâtiments où sont conservés des documents classifiés de haut degré. Le but d'une telle enquête est de vérifier si la personnalité de l'intéressé est fiable dans le cas où il aurait accès à des informations vitales pour la sécurité nationale. Une enquête de même nature est également effectuée pour des personnes qui entrent en contact avec des personnalités importantes ou qui ont accès à des lieux susceptibles d'être la cible de terroristes.

Bien avant la note gouvernementale, il existait une procédure d'appel pour les personnes dont la fiabilité est mise en doute pour des raisons de sécurité. Cet appel est introduit auprès de trois conseillers nommés par le Premier ministre et qui ont pour mission de conseiller les ministres concernés sur des questions de sécurité. Dans le cas où seul le comportement ou le caractère d'un candidat est mis en cause, une possibilité de recours lui est ouverte auprès du haut fonctionnaire dirigeant le ministère concerné.

Cette procédure d'appel est restée en vigueur après le 1er octobre 1990 mais elle doit être distinguée de la plainte que la personne en question peut aussi adresser au "Tribunal" (la commission dont il est question au point 6 plus loin : les organes de contrôle). En effet, si une personne estime avoir été injustement traitée en la matière, elle peut aussi s'adresser au "Tribunal", lequel pourra, s'il estime que tel est le cas, octroyer une indemnité à l'intéressé. Le "Tribunal" peut par ailleurs conseiller d'octroyer le certificat de sécurité demandé, mais il ne peut pas réformer la décision de le refuser ou de le retirer.

Selon les explications fournies au Comité R par D. BICKFORD, le fait que cette matière ne soit pas réglementée par une loi ne pose aucun problème sur le plan du respect de la Convention européenne des droits de l'homme puisque l'enquête de sécurité ("vetting") est effectuée avec le consentement de la personne concernée.

3.2. The Secret Intelligence Service (Act 1994)

Cette loi définit les missions du "Secret Intelligence Service" et du "Government Communications Headquarters".

Ces services sont des services de renseignement contrairement au “Security Service “ qui est un service de sécurité.

3.2.1. Le “Secret Intelligence Service”

Le “Secret Intelligence Service” a pour mission :

a) collecter et fournir les renseignements relatifs aux actes ou intentions de personnes habitant en dehors des îles britanniques;

b) exécuter d’autres tâches relatives aux actes et intentions de ces personnes.

Les missions de l’Intelligence service peuvent uniquement être effectuées :

a) dans l’intérêt de la sécurité nationale, et plus particulièrement dans l’intérêt de la défense nationale et de la politique étrangère menée par le gouvernement;

b) dans l’intérêt du bien-être économique du Royaume-Uni;

c) dans le cadre de la prévention et de la lutte contre la grande criminalité.

Cette mission est définie de manière large et ceci afin de mettre l’accent sur le fait que MI6 n’a de compétence qu’à l’extérieur des îles britanniques.

3.2.2.The Government Communications Headquarters

Ses missions sont les suivantes :

a) contrôler les signaux électromagnétiques, acoustiques et autres émissions, ainsi que toutes les installations produisant ces signaux; collecter et fournir les informations résultant de ces signaux et des données encodées;

b) conseiller et assister les forces armées, le gouvernement et le ministère de l’Irlande du Nord ou toute autre organisation définie par le Premier ministre et ce, en matière de langues, de cryptographie et de protection de l’information et autres données.

Les fonctions visées au point a. peuvent uniquement être exécutées :

a) dans l’intérêt de la sécurité nationale, et plus particulièrement dans l’intérêt de la défense nationale et de la politique étrangère;

b) dans l’intérêt du bien-être économique du Royaume-Uni pouvant être mis en péril par des actes ou des intentions de personnes habitant en dehors des îles britanniques;

c) dans le cadre de la prévention et de la lutte contre la grande criminalité.

Dans le cadre de cette loi, l'abréviation GCHQ est utilisée tant pour désigner le "Government Communications Headquarters" que pour indiquer tout autre unité ou partie d'unité des forces armées qui, sur ordonnance du ministre, assiste temporairement le "Government Communications Headquarters" dans l'exercice de ses fonctions.

A la différence du "Security Service" qui détermine ses propres priorités conformément à la loi de 1989, le "Secret Intelligence Service" et le GCHQ ne peuvent faire que ce qui leur est demandé ou imposé par le "Joint Intelligence Committee" et approuvé par le "Ministerial Committee on the intelligence Services" (IS).

4. LES COMPETENCES DES SERVICES ET LA RESPONSABILITE DE LEURS DIRIGEANTS

Les différents services exercent leurs compétences sous la responsabilité de chefs de services. La responsabilité du Directeur général du "Security Service" est définie dans la loi de 1989. La loi de 1994 définit les compétences du chef de "l'Intelligence Service" et du Directeur du "GCHQ".

Les chefs de service sont nommés par les ministres compétents en la matière. La durée de leurs mandats n'est pas prévue dans la loi. Les ministres compétents décident, en concertation avec le Premier ministre, de la durée du mandat renouvelable (sous réserve de l'accord de l'intéressé). Ces mandats révocables sont réglés par une procédure administrative.

Le chef de service est responsable de l'efficacité du service et est personnellement tenu de veiller :

a) - à l'élaboration des réglementations qui stipulent que seules les informations nécessaires à l'exécution correcte des missions du service sont collectées;

- à ce qu'aucun renseignement ne soit rendu public sauf :

  (1) en ce qui concerne le "Security Service"

  - si cela s'avère nécessaire pour l'exécution de ses missions;
  - pour prévenir ou lutter contre la grande criminalité;
  - dans le cadre de procédures criminelles.

  (2) en ce qui concerne "The Intelligence Service"

  - pour autant que cela s'avère nécessaire pour l'exécution de ses missions;
  - dans l'intérêt de la sécurité nationale;
  - pour prévenir ou lutter contre la grande criminalité;
  - dans le cadre de procédures criminelles.

(3) en ce qui concerne le GCHQ

- si cela s'avère nécessaire pour l'exécution de ses missions;
- dans le cadre de procédures criminelles.

b) - à ce que les services ne posent aucun acte pouvant servir les intérêts d'un parti politique du Royaume-Uni.

Le Directeur général du "Security Service" veille à l'application de réglementations relatives à la coordination de ses activités avec celles des services de police ou d'autres services d'ordre.

La loi de 1989 stipule, en outre, que les renseignements en possession du "Security Service" ne peuvent être divulgués pour déterminer si une personne peut être employée dans une fonction. Cette disposition concerne principalement le secteur privé.

Les chefs de services établissent un rapport annuel sur le fonctionnement des services qu'ils transmettent au Premier ministre et au ministre compétent.
Ils peuvent, à tout moment, rapporter à chacun de ces derniers tout faits relatifs aux activités du service.

5. METHODES SPECIALES DES SERVICES

La loi permet aux services d'utiliser certaines méthodes, autres que les classiques, pour collecter les informations.

5.1. Les ordonnances (warrants) relatives à la propriété et à la radiotélégraphie

La loi de 1994 autorise le ministre compétent à délivrer une ordonnance relative à l'intrusion de propriétés ou à l'interception de radiotélégraphie. Chacun des trois services peut solliciter une telle ordonnance sous certaines conditions.

Une ordonnance est un mandat donné par le ministre compétent à un service de renseignement ou de sécurité autorisant l'intrusion de propriétés et l'interception de radiotélégraphie.

Par "propriété du plaignant", il faut entendre :

- toute communication sans fil ou radiotélégraphies reçue ou délivrée par celui-ci;
- son domicile, sa résidence ou son lieu de travail.

5.1.1.Procédure de délivrance des ordonnances

Champ d'application

Une intrusion dans une propriété ou une interférence dans une radiotélégraphie n'est pas illégale si elle est autorisée par une ordonnance du ministre compétent.

A la demande du "Security Service", de "l'Intelligence Service" ou du "GCHQ", le ministre compétent peut délivrer une ordonnance qui permet l'intrusion dans une propriété ou d'interférer dans des radiotélégraphies, uniquement :

a) s'il estime que l'action est d'un intérêt primordial pour l'exécution des missions d'un des trois services :

b) s'il est convaincu que l'objectif visé ne peut être raisonnablement atteint par d'autres moyens;

c) s'il est convaincu que l'utilisation des informations recueillies à l'aide de ces méthodes respecteront les règles relatives à la confidentialité prévues par les lois de 1989 et de 1994.

Une ordonnance délivrée à la demande de "l'Intelligence Service" ou du "GCHQ" dans le cadre de leur mission de prévention et de lutte contre la grande criminalité, ne peut porter sur une propriété située dans les îles britanniques.

La même règle vaut pour le "Security Service" à quelques exceptions près.

Conditions de forme

L'ordonnance pourra uniquement être délivrée aux conditions suivantes :

a) elle doit être signée par le ministre compétent;

b) en cas d'urgence, elle doit être signée par un fonctionnaire de grade 3 ou supérieur, si le ministre compétent a expressément autorisé la délivrance d'une telle ordonnance.

Durée de validité

Sauf si elle est renouvelée, l'ordonnance cesse de produire ses effets :

a) au bout de six mois à compter de la date de sa délivrance si elle a été signée par le ministre compétent;

b) dans tout autre cas, à compter du second jour ouvrable suivant le jour de la délivrance.

Renouvellement

Si le ministre compétent l'estime, il peut la renouveler pour une période de six mois, qui commencera à compter de la date de son renouvellement.

Suppression de l'ordonnance

Le ministre compétent annule l'ordonnance s'il est convaincu que l'action autorisée n'est plus nécessaire.

5.2. Autorisations ("authorisations") pour opérer en dehors des îles britanniques

La loi de 1994 dispose que, dans certaines circonstances, le ministre compétent peut mandater l' "Intelligence Service" à poser des actes à l'étranger qui seraient condamnables au Royaume-Uni si cette autorisation n'était pas délivrée.

Le ministre compétent délivre l'autorisation sous les conditions suivantes :

a) chaque opération découlant de cette autorisation doit être nécessaire à l'exécution correcte d'une mission de "l'Intelligence Service";

b) seules des actions nécessaires à l'exécution de ces missions peuvent être menées à l'exclusion de toutes autres, et celles-ci doivent avoir un rapport raisonnable avec l'objectif visé;

c) les informations recueillies à l'aide de ces méthodes doivent respecter les règles relatives à la confidentialité prévues par les lois de 1989 et 1994.

Une telle autorisation peut :

a) être délivrée pour une ou plusieurs actions précises;

b) être limitée à une ou plusieurs personnes déterminées;

c) être soumise à des conditions précises.

L'autorisation est soumise aux mêmes règles de procédures que celles applicables aux ordonnances (voir point 5.1.1.) :

- son mode de délivrance;
- sa durée de validité;
- son renouvellement;
- son annulation.

Cette loi ne peut être assimilée à une "Licence to kill".

Toutefois elle autorise probablement que certains actes de violence soient commis.
Le seule restriction mises à ces activités est que leur nature et leur conséquences possibles doivent avoir une proportion raisonnable par rapport aux objectifs pousuivis.

En dotant les agents de ses services de renseignement d'une immunité légale pour des activités illégales commises à l'étranger, un gouvernement démocratique pose ainsi comme principe que le renseignement est une part essentielle et inhérente à la souveraineté de l'Etat.

Etant donné que cette souveraineté emporte le droit exclusif de recourir à la force (à des moyens violents), ceci est donc étendu aux services de renseignement .

5.3. L'interception du courrier et des communications

La loi de 1985 (Interception of Communications Act 1985) autorise, sous certaines conditions l'interception du courrier et des communications par les services de renseignement et de sécurité, par les services de police, les douanes et les accises.

Il s'agit de l'interception de différentes formes de télécommunication tel que téléphone, fax, télex et d'autres systèmes de transmissions de données via un système public de télécommunication.

5.3.1.Interdiction d'interception

La loi stipule qu'une personne interceptant volontairement un message durant son expédition par la poste ou via un système public de télécommunication est coupable d'un délit (punissable d'une peine allant d'une simple amende à une peine d'emprisonnement de deux ans).

Néanmoins, plusieurs exceptions aux poursuites pénales sont prévues.

Il n'y a pas de délit si :

- celui qui intercepte le message, agit de la sorte en vertu d'une ordonnance délivrée par le ministre ou;

- a des raisons suffisantes de croire que la personne à qui ou par qui le message est envoyé, a autorisé cette interception.

5.3.2.Ordonnances autorisant cette interception

Le ministre compétent peut délivrer une ordonnance en vue d'intercepter une communication au cours de sa transmission par la poste ou par un système de télécommunication public.

Le ministre compétent délivre une ordonnance s'il estime qu'elle s'avère nécessaire :

- dans l'intérêt de la sécurité nationale;
- dans le cadre de la prévention et de la lutte contre la grande criminalité;
- dans l'intérêt du bien-être économique du Royaume-Uni.

Les aspects à prendre en compte lorsque l'on considère la nécessité d'une ordonnance sont de savoir si ces informations ne peuvent pas être obtenues raisonnablement par d'autres moyens.

Une ordonnance délivrée en vue de sauvegarder les intérêts du bien-être économique du Royaume-Uni est jugée utile si l'information concerne des actes ou des intentions de personnes situées en dehors des îles britanniques.

La procédure de délivrance, d'annulation ou de renouvellement de cette ordonnance est similaire à celle prévue par la loi de 1994 pour les ordonnances concernant l'intrusion dans les propriétés ou la radiotélégraphie.

5.3.3.Mesures de sécurité à prendre par le ministre compétent

Lorsque le ministre compétent délivre une ordonnance, il prend les mesures qu'il estime nécessaires afin de s'assurer que les conditions de sécurité relatives aux données interceptées sont remplies. Ainsi, notamment, toute donnée interceptée doit être détruite dès qu'elle n'est plus utile.

5.4. Procédure pour introduire une demande d'ordonnance

Cette procédure n'est pas réglée par la loi.

Les rapports des commissaires de gouvernement assurant le contrôle sur la délivrance des ordonnances et des autorisations relatives à certaines opérations à l'étranger, décrivent clairement la procédure suivie dans le cadre de la délivrance des ordonnances.

Les ordonnances relatives à la violation d'une propriété sont régies par la loi de 1994 ("Intelligence Services Act") tandis que celles relatives à l'interception de communications sont édictées dans la loi de 1985 (Interception of Communications Act 1985 [5]).

La procédure de demande de délivrance est identique pour toutes les ordonnances. La demande écrite émane d'un des services et est adressée au ministre compétent.

Cette demande est motivée en exposant :

- le motif de la demande;
- l'objectif du service;
- les attentes du service;
- l'évaluation des risques;
- les conséquences si l'action était découverte.

La demande d'ordonnance est adressée à la section "Warrants Units" du ministère compétent où elle est scrupuleusement étudiée afin de vérifier que toutes les dispositions légales sont remplies pour sa délivrance.
Si le moindre doute subsiste, la demande est retournée au service.
La demande est instruite par différents fonctionnaires de grade supérieur avant d'être présentée au ministre avec les recommandations nécessaires.

Le ministre et ses conseillers doivent pouvoir se fier à la précision des informations fournies par le demandeur. Si ces informations ne sont pas correctes, l'élément-clé de la sécurité du système est mis en péril.

Les commissaires du gouvernement (voir point 6.2.) peuvent analyser toutes les ordonnances délivrées et ont également accès aux données interceptées.
Les services de renseignement et de sécurité tout comme les ministères sont tenus de leur communiquer les informations nécessaires à leur mission.

L'analyse minutieuse des demandes d'ordonnances et leur contrôle par les commissaires du gouvernement laissent peu de place aux abus de pouvoir.

(5) Les ordonnances d'interception de communications sont le plus souvent délivrées par les ministres de l'Intérieur, des Affaires étrangères ainsi que par les ministres de l'Ecosse et de l'Irlande du Nord.

6. LES ORGANES DE CONTROLE

Les lois de 1985, 1989 et de 1994 prévoient un contrôle sur la délivrance des ordonnances et des autorisations.
Les commissions intitulées “Tribunal” sont créées afin d’étudier les plaintes introduites par des particuliers contre les services de renseignement et de sécurité.

Ce contrôle est exercé sur les méthodes de nature à violer les droits des citoyens par les services de renseignement et de sécurité dans l’exercice de leurs missions, telles que l’intrusion dans une propriété ou l’interception de communications.

6.1. Aperçu général de la fonction de Commissaire du gouvernement (“Commissioners”)

En vertu du “Security Service Act” et du”Intelligence Services Act”, la délivrance d’ordonnances et d’autorisations par les ministres est soumise au contrôle de deux commissaires du gouvernement, à savoir le “Security Service Commissioner” et “l’Intelligence Service Commissioner”.
Le commissaire actuel pour les deux services est Lord Justice Stuart-Smith.

Un troisième commissaire du gouvernement, à savoir “l’Interception commissioner” est chargé des interceptions des communications. Il est institué par le “Interception of Communications Act 1985" et exerce un contrôle sur les ordonnances relatives à l’interception de courrier et de communications demandées par les services de renseignement et de sécurité ou d’autres services d’ordre.
Le commissaire actuellement en fonction est Lord Nolan.

6.2. Les commissaires du gouvernement

6.2.1.Nomination des commissaires du gouvernement

En vertu du “Appellate Jurisdiction Act 1876 (Loi sur la jurisprudence d’appel), le Premier ministre nomme au poste de commissaire du gouvernement une personne remplissant ou ayant rempli une fonction judiciaire importante.

Le ministre désigne le nombre de personnes nécessaire à l’accomplissement des fonctions du commissaire du gouvernement après entretien avec le commissaire du gouvernement et sur approbation du ministère des Finances.

6.2.2.Mission

Les commissaires du gouvernement remplissent la fonction selon les dispositions définies lors de leur nomination.

Les commissaires du gouvernement sont chargés du contrôle de l'exercice des compétences octroyées au ministre compétent pour délivrer des ordonnances en vertu des lois de 1989, 1994 et 1985.

Les commissaires du gouvernement apportent également leur collaboration aux commissions intitulées "tribunals" si des plaintes sont introduites contre les services.

Les commissaires du gouvernement vérifient si une ordonnance ou une autorisation a été délivrée. Si c'est le cas, ils vérifient si le ministre compétent a respecté la procédure.

Les commissaires du gouvernement informent les "tribunals" de leurs conclusions relatives à chaque affaire qui leur a été transmise.

Si , dans le cadre d'une plainte, une commission estime que les droits du plaignant ont été transgressés, elle en fait rapport au ministre compétent et au commissaire du gouvernement.

Dans le cas où la commission décide qu'elle ne peut pas prendre de décision favorable au plaignant, l'affaire est néanmoins transmise au commissaire du gouvernement si la commission estime qu'une enquête doit quand-même être menée pour déterminer si les services ont, d'une manière ou d'une autre, agi de façon déraisonnable envers le plaignant ou sa propriété. Dans ce cas, le commissaire du gouvernement peut en faire rapport au ministre qui prend alors toutes les mesures qui lui semblent appropriées.

6.2.3.Les rapports des commissaires du gouvernement

Chaque commissaire du gouvernement établit un rapport annuel à l'attention du Premier ministre. Ils peuvent, à tout moment, lui faire rapport de tout problème rencontré durant l'exercice de leurs fonctions.

Le Premier ministre transmet aux membres de chacune des chambres du parlement, un exemplaire de chaque rapport établi par un commissaire du gouvernement.

Après concertation avec l'auteur du rapport, le Premier ministre peut en supprimer une ou plusieurs parties s'il estime que cette ou ces parties sont de nature à porter préjudice à l'exécution future des missions des services de renseignement et de sécurité.

6.2.4.Obligations des membres des services et des fonctionnaires du ministère

Chaque membre des services, chaque fonctionnaire des ministères compétents et toute personne employée à la poste ou dans une institution publique de télécommunication est tenu de révéler ou de fournir au commissaire du gouvernement tous les documents ou renseignements que celui-ci estimera nécessaire dans le cadre de l'exécution de sa fonction.

6.2.5.Appel

Enfin, la loi dispose que les décisions des commissaires du gouvernement ne sont pas appelables et ne peuvent être évoquées devant un tribunal.

6.3. Les commissions (Tribunals)

Les lois de 1985, 1989 et 1994 créent chacune une commission ayant pour mission d'étudier les plaintes introduites par des particuliers contre les services de renseignement et de sécurité.

La loi de 1989 traite des plaintes contre le Security Service, celle de 1994, des plaintes contre l'Intelligence Service et le GCHQ.

Toute personne peut introduire une plainte auprès de la commission si elle s'estime lésée par un fait commis contre elle ou sa propriété par un service de renseignement ou de sécurité. La commission étudie la plainte sauf si elle estime que cette dernière est manifestement non fondée et téméraire.

De même toutes les personnes croyant que les messages qui lui sont destinés ou qu'elle a envoyés, par la poste ou via un système public de télécommunication, ont été interceptés, peuvent s'adresser à la commission instituée par la loi de 1985 et demander qu'une enquête soit entamée.

Les règles applicables à la composition, aux procédures d'investigation, aux rémunérations, aux dépenses et au personnel sont similaires pour toutes les commissions.

Les commissions se composent de trois membres au minimum et de cinq membres au maximum à l'exception de la commission chargée des interceptions qui se compose toujours de cinq membres. Tous les membres de la commission sont originaires du barreau et nommés par arrêté royal. Leur mandat est de cinq ans renouvelable. Ils perçoivent des indemnités et primes déterminées par le ministre compétent en accord avec le ministère des Finances.

Un membre de la commission peut, à sa demande, être relevé de sa fonction par la Reine. Il peut être démis de sa fonction par la Reine à la demande des deux Chambres du Parlement.

Un membre de la commission, peut en vertu d'un arrêté royal, être nommé au poste de président ou de vice-président de la commission.
En cas d'empêchement du président, le vice-président assure sa fonction.

La commission exerce sa fonction sur tout le territoire du Royaume-Uni par l'entremise de deux ou de plusieurs de ses membres désignés à cette fin par son président.
Les membres de la commission peuvent examiner simultanément plusieurs plaintes.

Chaque membre des services est tenu de fournir à la commission tous les documents qu'elle estimera nécessaires à l'accomplissement de sa mission.
Les Commissions ont toute autorité et ont le droit de recevoir toute information des services de renseignement. Les restrictions qui valent pour l' "Intelligence and Security Committee" ne sont pas ici applicables.

Les commissions remplissent leurs missions en garantissant qu'aucun document ou renseignement qui leur est transmis n'est rendu public ou n'est cédé exception faite pour le commissaire du gouvernement ou de l'accord de celui dont de document émane.
Les commissions n'adressent pas de rapport motivé au plaignant sauf dans les cas où un rapport motivé est adressé au ministre et au commissaire du gouvernement lorsque les droits du plaignant ont été transgressés.

Les commissions peuvent déterminer leurs propres règlement d'ordre intérieur.

6.4. Etude des plaintes

Les procédures relatives à l'étude des plaintes par les commissions instaurées par les lois de 1985, 1989 et 1994 sont semblables.

Tout particulier, organisation et association de personnes peut introduire une plainte auprès des commissions instituées par ces lois.

La commission compétente vérifie si le plaignant a fait l'objet d'enquêtes par les services de renseignement et de sécurité.

La commission vérifie si les services de renseignement et de sécurité disposaient de motifs suffisants pour mener des enquêtes au sujet du plaignant même si l'enquête a été arrêtée au moment du dépôt de la plainte.

De même, si la commission constate que l'enquête à charge du plaignant, a été ouverte en raison de son adhésion à un groupe de personnes qui, selon le service, devait faire l'objet d'une enquête, la commission examine alors si le service disposait de motifs suffisants pour entamer l'enquête à charge du plaignant.
La commission a également pour mission de vérifier que les renseignements en possession du "Security Service" ne sont pas divulgués pour déterminer si une personne peut être employée dans une fonction.

6.4.1.Décision de la commission

En cas d'enquête faite par la commission

Si la commission conclut que la plainte est fondée parce que les services de renseignement et de sécurité n'avaient pas de motifs suffisants pour entamer une enquête :

- elle en informe le plaignant;

- elle adresse au ministre compétent et au commissaire du gouvernement un rapport de ses constatations.

Dans ce cas, elle peut alors :

- ordonner que l'enquête soit arrêtée et que tous les documents relatifs à cette enquête soient détruits, si le service ne possédait pas de motifs suffisants pour entamer une enquête;

- donner au ministre l'ordre de payer au plaignant une indemnité dont elle fixe le montant.

Si par contre ni la commission ni le commissaire du gouvernement n'estiment que la plainte est fondée, elle en informe le plaignant.

Si, dans un cas examiné par la commission, cette dernière estime que le service considérait injustement tous les membres d'un groupe comme des personnes devant faire l'objet d'une enquête, elle transmet alors le dossier au commissaire du gouvernement.
Il s'agit ici d'un transfert de compétence au commissaire du gouvernement qui est prévu uniquement dans la loi de 1989.

En cas d'enquête faite par le commissaire du gouvernement

La commission informe le plaignant de la décision du commissaire du gouvernement qui estime la plainte fondée.

Dans ce cas, la commission peut :

- annuler toute ordonnance ou toute autorisation que le commissaire du gouvernement estime n'être pas valablement délivrée ou renouvelée; et/ou

- donner l'ordre au ministre compétent de payer au plaignant la somme que le commissaire du gouvernement fixe.

6.4.2.La commission des interceptions (instaurée par la loi de 1985)

Toute personne croyant que les messages qui lui sont destinés ou qu'elle a envoyé ont été interceptés durant leur expédition par la poste ou via un système public de télécommunications, peut s'adresser à la commission et demander l'ouverture d'une enquête.
Dans le cadre de ces enquêtes (autres que celles que la commission considère comme manifestement non fondée et téméraire), la commission examine :

a) l'existence d'une ordonnance ou d'un certificat;

b) la légalité de ladite mesure.

Si la commission décide que la plainte est non fondée, elle en informe le plaignant.

Si la commission estime, après enquête, qu'une infraction a été commise au sujet de l'ordonnance, la commission :

a) informe le requérant de cette décision;

b) rend compte au Premier ministre des résultats de son enquête;

c) donne l'ordre :

- d'annuler l'ordonnance en question;
- de détruire les données recueillies et ses copies;
- au ministre compétent de payer au plaignant une indemnité dont elle fixe le montant.

Les décisions prises par la commission sont irrévocables et ne peuvent être attaquées en justice.

7. LA POLITIQUE RELATIVE AUX SERVICES DE RENSEIGNEMENT ET DE SECURITE

7.1. Aperçu général

Comme déjà indiqué ci-dessus, les services de renseignement et de sécurité sont, en ce qui concerne leur fonctionnement quotidien, placés sous la responsabilité de leurs chefs respectifs, eux-mêmes personnellement responsables vis-à-vis de leur ministre.

L'ensemble des organes visés ci-dessous n'est pas institué par une loi. Ils ont été créés sur décisions administratives prises par des Ministres.

Au Royaume-Uni, la loi règle traditionnellement peu de matières. A l'inverse, de nombreuses décisions administratives sont prises(6).

Le "Ministerial Committee on the Intelligence Services" (IS) détermine les priorités des services de renseignement. Sa tâche peut se définir comme suit : le contrôle de la politique des services de renseignement et de sécurité. Les ministres en assument la responsabilité politique.

Dans l'exercice de leurs fonctions, les ministres sont assistés du "Permanent Secretaries' Committee on the Intelligence Services" (PSIS).

Le PSIS constitue en fait le lien entre le "Joint Intelligence Committee" et le "Ministerial Committee on the Intelligence Services".

Le "Joint Intelligence Committee" délivre des avis sur les priorités en matière de collecte d'informations et sur l'établissement de rapports d'évaluation destinés aux ministres et aux fonctionnaires sur des problèmes importants et d'actualité.

(6) Le comité s'est basé pour faire rapport en cette matière sur un document intitulé "Central Intelligence Machinery " et sur les entretiens qu'il a eu avec le Co-ordinator.

Le poste de “Intelligence Co-ordinator” fut créé en 1968 ,ainsi que l’ “Assessments Staff”, chargé de coordonner les besoins et la collecte d’informations et de préparer les documents et les rapports d’analyse destinés au “Joint Intelligence Committee”.

Le “Cabinet Official Committee on Security” (SO), également connu sous le nom de “Sub Committee on Security Service Priorities and Performance” (SO-SSPP), a pour objectif d’évaluer les prestations du Security Service en matière de plans et d’objectifs, d’étudier les priorités futures du service et de conseiller le “Cabinet Secretary” et le PSIS.

7.2. Besoins d’informations et missions

La collecte de la plupart des informations secrètes est effectuée par le GCHQ et le Secret Intelligence Service. Leurs missions sont décrites dans l’Intelligence Services Act 1994.
Le JIC définit les besoins d’information ainsi que les tâches du Secret Intelligence Service et du GCHQ.

Ces besoins sont évalués annuellement sous la direction du Co-ordinateur. Cette évaluation associe une analyse rigoureuse des besoins d’informations secrètes à une enquête détaillée menée auprès des départements “clients” et à l’établissement d’un budget indispensable à la réalisation des activités.
Le rapport d’évaluation qui en est dressé est ensuite transmis pour approbation aux ministres.

Les besoins d’informations sont répartis en trois catégories prioritaires selon leur importance pour la sécurité nationale et le bien-être économique du Royaume-Uni.

Là où jusqu’aux années 90 des informations ont été collectées pour le gouvernement au sujet de l’espionnage, se sont développées au cours des années de nouvelles priorités comme le terrorisme, la lutte contre la grande criminalité et le trafic de drogue.

Les activités des terroristes de l’Irlande du Nord ne sont pas les seules cibles des services de renseignement. Le GCHQ et le MI6 enquêtent aussi sur les activités des terroristes de l’Inde, de l’Iran et du Sri Lanka qui utilisent le Royaume-Uni comme plaque tournante pour recueillir des fonds. Les services de renseignement britanniques s’occupent aussi de” super-terrorisme” comme ils disent en évoquant le terrorisme commis au moyen d’armes nucléaires, bactériologiques et chimiques. Ces différentes formes de criminalité ont un dénominateur commun : le blanchiment d’argent et les moyens utilisés (armes, explosifs etc...).

En conséquence la collecte d’informations se fait dans un but de poursuites judiciaires. Ainsi les services de renseignement collaborent avec les services de police et les autres services d’ordre mais de manière informelle.

Le Security Service détermine ses priorités en toute autonomie conformément aux tâches qui lui sont imposées par la loi de 1989.

Le Security Service intervient et est concerné dans les matières impliquant différents ministères. Afin d’être opérationnel, ce service ne doit pas tenir compte des seuls besoins et exigences du ministère de l’Intérieur. Un contact étroit a donc été instauré entre le Security Service et les différents autres services et ministères, notamment via le JIC et le Co-ordinator.

8. DESCRIPTION DETAILLEE DES ORGANES POLITIQUES

8.1. The Joint Intelligence Committee (JIC)

Le JIC fut institué en 1936 et placé sous la responsabilité de l'Etat-major de l'armée. En 1957, il fut placé sous l'autorité du "Cabinet office". Il travaille sous la responsabilité du "Secretary of the Cabinet"(7).

Il se compose d'un président, des chefs des trois services, du Co-ordinateur et du chef de "l'Assessments Staff", de hauts fonctionnaires des ministères des Affaires étrangères, de la Défense nationale, des Finances et si nécessaire, d'autres ministères tels que celui des Affaires économiques et celui de l'Intérieur.

Ce sont des fonctionnaires conscients des volontés et des besoins des décideurs politiques. Il ne s'agit pas nécessairement (et ce n'est généralement pas le cas) de spécialistes des renseignements mais de collaborateurs possédant une excellente connaissance des besoins d'informations dans certains domaines et certaines régions .

Ces fonctionnaires tiennent des réunions hebdomadaires; ils exercent leur fonction au sein du JIC à temps partiel.

Le JIC a les responsabilités suivantes :

- diriger et contrôler l'organisation et le fonctionnement de l'ensemble de l'activité de renseignement britannique, tant au Royaume-Uni qu'à l'étranger, afin de garantir l'efficacité, la bonne gestion et une adaptation rapide aux besoins qui évoluent constamment;

- présenter à l'approbation ministérielle les rapports relatifs aux besoins et aux priorités de la collecte d'informations ainsi qu'aux autres missions à remplir par les services de renseignement;

- si nécessaire, coordonner les plans des différents ministères en matière d'activités de renseignements;

- assurer le suivi et prévenir à temps les menaces étrangères directes ou indirectes pouvant porter préjudice aux intérêts britanniques, qui se préciseraient en matière politique, militaire et économique;

---

(7) "Cabinet Office" se compose de fonctionnaires au service du Premier ministre et devant lui faire rapport. Ces fonctionnaires peuvent provenir d'autres départements. Il s'agit d'un petit département ayant un rôle central de coordination. Le "Secretary of Cabinet" assure la direction du "Cabinet Office". Il est le fonctionnaire le plus haut en grade et nomme et contrôle également les autres fonctionnaires.

- sur base de l'information disponible, évaluer les événements et les situations relatifs aux affaires étrangères, à la défense nationale, au terrorisme, aux activités criminelles étrangères importantes, aux affaires scientifiques, techniques et d'économie internationale;

- suivre de près les menaces contre la sécurité intérieure et extérieure et trouver une solution aux problèmes qui en résulteraient;

- entretenir et superviser les relations entre les services de renseignement britanniques et étrangers et vérifier si des informations peuvent être mises à leur disposition.

Le JIC émet également des avis destinés aux ministres sur des actions opérationnelles ou politiques.
Cette coordination globale et ces avis permettent d'éviter des prises de positions divergentes.

En outre, le JIC peut agir de sa propre initiative et informer les ministres d'éléments importants; il travaille aussi à la demande des ministres.

Le JIC contrôle annuellement si les deux services de renseignement (SIS et GCHQ) exécutent correctement leurs missions. Il contrôle la quantité et la qualité des renseignements collectées dans ces deux services. A cet effet, il vérifie auprès des différents ministères si ces services ont répondu correctement à leurs demandes. Le JIC exerce ainsi un contrôle a posteriori.
Il faut encore souligner que le JIC définit uniquement les priorités, les besoins et les missions des services de renseignement que sont le "Secret Intelligence Service" et le "GCHQ".

Le Security Service entretient un lien étroit avec les autres services et ministères travaillant notamment avec le JIC.

A l'instar des services de renseignement et de sécurité, le JIC entretient des contacts avec des services identiques à l'étranger, ce qui permet d'avoir accès à des informations et des analyses difficilement disponibles autrement.
Il s'agit d'informations importantes à partager avec des pays avec qui des alliances militaires sont conclues et où des menaces semblables existent; de manière telle que les décisions soient prises en commun.

Le président du JIC assure la supervision générale du travail de son service. Il vérifie que la fonction d'avertissement et de contrôle est correctement remplie. Il fait rapport directement au Premier ministre.
Depuis 1985, les fonctions du président du JIC et du Co-ordinator, jusqu'alors occupées par une seule et même personne, ont été réparties entre deux hauts fonctionnaires du "Cabinet Office".

8.2. The Assessments Staff (Equipe d'analyse)

Le JIC est soutenu par le "Assessments Staff" qu'on pourrait également appeler "Equipe d'analyse". Il se compose de fonctionnaires détachés de différents ministères et services qui représentent plusieurs disciplines.

A cet égard, il faut d'abord souligner que les services de renseignement fournissent des informations brutes. Ils concentrent leurs activités sur la récolte des informations provenant de sources fermées.
Ils peuvent toutefois donner une évaluation de la fiabilité de la source.

L'Assessments Staff est responsable de l'établissement des évaluations et des rapports relatifs aux problèmes et situations actuels.

Ce Staff recueille toutes les informations, non seulement celles provenant des services mais aussi des diplomates.

Au stade de projet, ces évaluations sont analysées par des sous-comités appelés "Current Intelligence Groups" (Groupes de renseignements actuels) composés d'experts des différents ministères et services. Ces derniers peuvent prendre conseil auprès de tout qui leur semble utile.

Leur texte est soumis à l'approbation du JIC et ensuite transmis aux ministres et aux hauts fonctionnaires. Dans des situations de crise, ce texte peut être directement transmis aux ministres et aux hauts fonctionnaires.

"The Assessments Staff" et les "Current Intelligence Groups" analysent tant les sources "ouvertes" que "fermées" (e.a. sources humaines et interceptions de communications).
Cet Assessments Staff se compose en fait d'analystes occupés à temps plein. Huit rapports environ sont établis de manière hebdomadaire.

D'autres analyses sont réalisées au sein des ministères par les "desk officers". Ce ne sont pas des spécialistes en matière de renseignement mais ils travaillent dans des domaines spécialisés.

8.3. Le Co-ordinator (le Co-ordinateur)

Ce Co-ordinateur conseille le "Secretary of the Cabinet" sur la coordination des services de renseignement ainsi que sur les moyens et les missions de ces services. Il assure la présidence des différents organes de concertation statutaires ad hoc chargés de "l'Intelligence management", de la collecte et du traitement des informations.
Il est chargé de déterminer les besoins de renseignement du Royaume-Uni et de conseiller les autorités compétentes au sujet des moyens nécessaires à mettre à la disposition des services de renseignements

Le Co-ordinateur actuel est Monsieur John Alpass que le Comité R a rencontré à Londres le 14 janvier 1998. Durant cet entretien, le co-ordinateur a expliqué au Comité R le travail effectué par les différents organes politiques en matière de services de renseignement et de sécurité au Royaume-Uni. Il a également décrit sa fonction.

Il a en charge la coordination entre les trois services, le gouvernement et les services de police. Dans la pratique, une collaboration a été instaurée avec le "Defense Intelligence Staff", le "DIS", bien qu'aucun texte ne l'instaure.
A cet égard, il faut une nouvelle fois souligner que le DIS n'est pas un véritable service de renseignement. Il se charge de l'analyse des stratégies et de la technologie militaires.

Le Co-ordinateur remplit la fonction de secrétaire du JIC. Il prépare des propositions concrètes. Comme indiqué précédemment, le JIC définit uniquement les besoins et les missions des services de renseignement (SIS et GCHQ). Toutefois, il existe un lien étroit entre le Security Service, les services de renseignement et les ministères. Ces contacts sont entretenus, notamment via le Co-ordinateur.

Ce dernier conseille le PSIS (voir infra). Il occupe même le poste de président d'un comité de conseil connu sous le nom de "Preliminary Committee" chargé d'effectuer une première analyse des dépenses des services.

Les objectifs du Security Service approuvés par le "Cabinet Official Committee on Security" (SO), également connu sous le nom de "Sub-Committee on Security Service Priorities and Performance" (SO-SSPP), sont transmis aux ministres par l'intermédiaire du Co-ordinateur (voir 8.4 pour ce qui concerne le SO (SSPP)).

Le Co-ordinateur a en outre expliqué au Comité R que le Royaume-Uni mène une politique axée sur la sécurité. Depuis quelques mois, c'est lui qui supervise cette politique en matière de sécurité.

Il a insisté sur le fait que son travail revêt un caractère très informel. Il en va de même pour les contacts entre les différentes commissions (Tribunals), le JIC et "The Intelligence Security Committee" (ce dernier est l'organe parlementaire de contrôle des services de renseignement et de sécurité.

Cet organe parlementaire de contrôle reçoit les résultats du travail des services s'il les demande au JIC. Le ministre doit toutefois donner son accord pour que de telles informations puissent être divulguées. Le JIC ne transmet donc pas d'office des informations à l'organe parlementaire de contrôle.

Enfin, le Co-ordinateur doit également tenter de résoudre les problèmes pouvant surgir entre les services de renseignement et de sécurité et les ministères ou les services de police.
La fonction de Co-ordinateur est attribuée à un fonctionnaire ayant une parfaite connaissance des services de renseignement et de sécurité.
Le Co-ordinateur actuel a exercé des fonctions dans un des services de renseignement et de sécurité.

8.4. Sub-Committee on Security Service Priorities and Performance (SO (SSPP))

Les tâches du "Security Service" (le service de sécurité) sont décrites dans les "Security Service Acts 1989 et 1996". En vertu de ces lois, ce service détermine ses priorités en totale autonomie.

Le "Security Service" communique au "Cabinet Official Committee on Security" (SO), également connu sous le nom de "Sub-Committee on Security Service Priorities and Performance" (SO-(SSPP)) les objectifs du service et les menaces existantes. Il demande à ce sujet des avis au (SO (SSPP)).

Le service présente ces projets en termes très généraux, sans que les activités opérationnelles ne soient abordées.

Les objectifs alors approuvés par le SO (SSPP) sont transmis aux ministres par l'intermédiaire du Co-ordinateur.
Le ministre compétent tranche en cas de désaccord entre le Security Service et le SO (SSPP).

Le SO (SSPP) a la responsabilité d'évaluer les prestations du Security Service en matière de plans et d'objectifs, d'analyser les priorités futures du service et de conseiller le "Cabinet Secretary" et le PSIS.

Il se compose de haut fonctionnaires des ministères des Affaires étrangères, de la Défense nationale, des Finances, de l'Intérieur, des Affaires économiques, de la Sécurité sociale, du Ministère de l'Ecosse et du ministère de l'Irlande du Nord, du GCHQ, du Security Service et de l'Intelligence Service, du ministère de la Fonction publique et du Cabinet Office.

Sa présidence est assurée par un fonctionnaire détaché du ministère de l'Intérieur.

Des membres du JIC peuvent également siéger au sein du SO (SSPP) étant donné qu'il est plus efficace de travailler avec les mêmes personnes.

Le SO (SSPP) ne se réunit que deux fois par an.

8.5. The Permanent Secretaries' Committee on the Intelligence Service (PSIS)

Le "Ministerial Committee on the Intelligence services" (IS) est, dans sa fonction de contrôle des services, assisté par le "Permanent Secretaries' Committee on the Intelligence Services" (PSIS). Le Comité des secrétaires généraux analyse les évaluations budgétaires annuelles, les plans de gestion et les besoins de renseignements des services.

Le PSIS est présidé par le "Secretary of the Cabinet" et se compose des secrétaires généraux des ministères de l'Intérieur et des Affaires étrangères, de la Défense nationale et des Finances.

Le Co-ordinateur conseille le PSIS.

Comme indiqué ci-dessus, le PSIS constitue en fait le lien entre le "Joint Intelligence Committee" et le "Ministerial Committee on the Intelligence Services" (IS).

8.6. Ministerial Committee on the Intelligence Service (IS)

La mission du Ministerial Committee on the Intelligence Services (IS) est de contrôler la politique des services de renseignement et de sécurité.
Il supervise, par exemple, les décisions politiques prises en vertu des missions fixées par le "Intelligence Services Act".

Le Premier ministre le préside. Il est composé du Vice-Premier ministre et des ministres des Affaires étrangères, de l'Intérieur, de la Défense nationale et des Finances.

Les plans de gestion, accompagnés des recommandations du PSIS, sont présentés aux ministres chargés de trouver un consensus sur le budget des services. Le gouvernement définit donc globalement le budget des services.

Le Parlement vote globalement le budget accordé aux différents services selon le principe du "Single Intelligence Vote" (SIV). Le chiffre global est rendu public. La répartition du budget entre les différents services est toutefois secrète.
Pour l'année 1996-1997, ce budget avoisinait les 751 millions de livres sterling.

On constate une tendance générale à la diminution des budgets.

9. LE CONTROLE PARLEMENTAIRE

"The Intelligence and Security Committee" exerce le contrôle parlementaire des services de renseignement. Il est institué par la loi de 1994 ("Intelligence Services Act 1994").

Le 13 janvier 1998, le Comité R a eu un entretien à Londres avec Monsieur Tom King, ancien ministre de la Défense nationale et président de l'Intelligence and Security Committee ainsi qu'avec son greffier. Ces deux derniers ont commenté la loi et ont expliqué la méthode de travail du "committee".

Le "committee" n'a pas été institué à la suite de l'un ou l'autre scandale ou difficulté, mais bien parce qu'un désir de transparence des activités du gouvernement et de chacun de ses services (y compris les services de renseignement) était dans l'air du temps.

Les "Select Committees" (les commissions parlementaires permanentes) des différents ministères contrôlent occasionnellement les services de renseignement et de sécurité, mais de manière très superficielle étant donné que le parlement ne connait pas réellement les activités secrète de ces services. De ce fait la nécessité d'examiner et de coordonner le travail de ces trois services d'une manière plus structurée s'est fait sentir.

9.1. Composition et procédure du "Intelligence and Security Committee"

D'après la loi de 1994, le "Committee" se compose de neuf membres choisis parmi les membres de la Chambre des Communes et de la Chambre des Lords. Aucun de ces membres ne peut occuper de fonction ministérielle durant l'exercice de leur mandat à l'Intelligence and Security "committee".

Le Premier ministre nomme les membres du "committee" après concertation avec le chef de file de l'opposition et dans le respect des directives établies dans "The Ministerial and other Salaries Act 1975" (la loi de 1975 sur les fonctions ministérielles et autres). Un de ces membres est nommé au poste de Président.
Les membres du "committee" disposent d'un mandat de la durée de la législature.

Le mandat d'un membre du "committee" prend fin :

- s'il n'est plus membre de la Chambre des Communes;
- s'il n'est plus membre de la Chambre des Lords;
- s'il est nommé au poste de ministre ou;
- à la demande du Premier ministre en cas d'une nomination d'une autre personne.

Un membre du "committee" peut démissionner à tout moment après en avoir averti le Premier ministre.

Le mandat des membres du "committee" peut être renouvelé.

Le "committee" se dote d'un règlement d'ordre intérieur qui définit notamment ses procédures.
Le président dispose d'une voix prépondérante.
Les décisions du "committee" se prennent à la majorité des trois voix.

Le premier "committee" se composait de cinq membres du parti conservateur, de trois membres du parti travailliste et d'un membre du parti démocrate-libéral.

Le gouvernement en place depuis le mois de mai 1997 a modifié la composition du "committee" et applique les règles de composition des Select Committees . Il s'en suit que le "committee" se compose actuellement de six membres du parti travailliste, de deux membres du parti conservateur et d'un membre du parti démocrate-libéral. Son président est Monsieur Tom King, membre du parti conservateur, que le gouvernement travailliste a maintenu dans ses fonctions.
Il consacre deux jours par semaine, en moyenne, à l'exercice de son mandat.
Tous les membres du "committee" prêtent serment de respecter le secret professionnel. Le "Official Secret Act" leur est applicable. Ils font donc partie du "Ring of secrecy".

9.2. Mission de "l'Intelligence and Security Committee"

La loi dispose que l'Intelligence and Security Committee a été crée pour contrôler les budgets, les activités et les options politiques du Security Service, de l'Intelligence Service et du GCHQ.

Le Committee analyse le fonctionnement, l'efficacité et les résultats des services, leurs succès et leurs échecs. Il énonce également les nouveaux défis et possibilités, les nouveaux besoins et fait des suggestions. Il étudie des problèmes spécifiques tels que, récemment, le problème du recrutement, des dommages éventuels causés par la trahison ou le mécontentement des employés, les mesures de sécurité, etc ... .

Le Committee analyse également les priorités définies par le gouvernement, par exemple, sur la mission et la collaboration des services de renseignement et de sécurité avec les services de police, notamment, dans la lutte contre le crime organisé ou les questions relatives au "economic well-being of the UK" (le bien-être économique du Royaume-Uni).

Le Committee ne se prononce pas sur des opérations concrètes mais se penche essentiellement sur les grandes lignes, les priorités, les besoins et les missions des services, leurs critères d'efficacité et l'affectation du budget des services contrôlés.

En matière de budget, il s'intéresse principalement à l'affectation générale, à savoir l'importance du budget nécessaire pour pouvoir mener à bien les missions des services de renseignement. Il étudie également les budgets importants spécifiques à certaines opérations.

Pour ce faire, le Committee prend connaissance d'informations fournies par les services et celles détenues par le ministère des Finances et la commission budgétaire.

Le Committee se penche donc essentiellement sur la responsabilité et la justification des compte des services ("responsibility and accountability").

Le "Committee" ne traite jamais les plaintes et n'agit jamais à la demande du parlement à l'inverse du Comité R.

A l'origine, les trois services ont émis des réserves à l'égard de ce Committee.
Leur relation est aujourd'hui empreinte de confiance. Les services considèrent le Committee comme un soutien essentiel.

9.3. Méthode de travail du Committee

Le fonctionnement du Committee dépend de la personnalité de son président. Tom King, le président actuel a une grande expérience, essentielle au bon fonctionnement de cet organe de contrôle parlementaire.

Le Committee tient au moins une réunion hebdomadaire au Cabinet Office.

Il rend souvent visite aux quartiers généraux des trois services et se déplace également dans les autres services ainsi qu'à l'étranger et procède à l'audition de témoins sans que ceux-ci soient entendus sous serment.
Dans le cadre de ces déplacements, des informations officieuses sont collectées. Toutefois, lors des réunions au "Cabinet Office", tout est officiel.

Le Committee est réparti en trois groupes de travail : un pour chaque service. Le "DIS" n'est pas contrôlé par le Committee mais il doit toutefois l'informer des données importantes qu'il détient.

Le Committee travaille de manière très pragmatique et est assisté d'une équipe administrative de trois personnes (dont le greffier et la secrétaire).

D'après Tom King, les membres du Committee divergent rarement de point de vue. La procédure de vote n'est donc pas souvent appliquée.

9.4. Accès aux informations

Les dispositions légales précisent les informations auxquelles le Committee a accès.

Si le Committee demande au Security Service, à l'Intelligence Service et au GCHQ de lui fournir des informations, ces services veillent à ce que :

- les informations soient transmises au Committee conformément aux réglementations approuvées par le ministre compétent;

- le Committee soit informé que les informations ne peuvent être divulguées car :

  a) il s'agit d'informations sensibles, telles qu'elles sont définies ci-dessous, qui, selon eux ne peuvent être dévoilées;
  b) le ministre a décidé que ces informations ne pouvaient être divulguées.

Le caractère sensible des informations ne fait pas obstacle à ce qu'elles soient communiquées au "committee" si le chef du service concerné estime que leur communication ne nuit pas à la sécurité.

Les informations sensibles qui ne devraient pas être dévoilées au Committee lui sont quand-même communiquées si le ministre compétent estime que cela s'avère nécessaire dans l'intérêt général.

Le critère de la sécurité nationale n'est pas le seul critère que le ministre compétent prend en considération pour refuser de divulguer une information. Le ministre compétent agit vis-à-vis du Committee de la même façon qu'il agit vis-à-vis du "Departmental Select Committee of the House of Commons" lorsque cette dernière commission parlementaire demande la divulgation d'une information.

Les informations suivantes sont considérées comme sensibles :

- les informations pouvant conduire à l'identification ou pouvant entraîner la divulgation de détails sur des sources d'informations, ou des méthodes opérationnelles dont disposent les services;

- les informations relatives à certaines opérations dans l'exercice d'une mission quelconque de ces services;

- les informations communiquées par des autorités étrangères qui n'ont pas donné leur aval pour la divulgation de ces informations.

Durant son entretien avec le Comité R, le président du Committee Monsieur Tom King a exposé que lorsque les services refusent de communiquer des informations, il en demande les motifs.

Le Committee est parfaitement conscient de l'incompatibilité des principes rencontrés dans l'exercice de sa mission - à savoir le "need to know" et le "need to secrecy". Il fait donc la balance des intérêts en cause.

Il est évident que des noms ou des détails sur des opérations individuelles pouvant mettre en péril la vie de personnes ou le succès des actions ne sont jamais demandés.
L'établissement d'un rapport de confiance et une excellente relation entre le "Committee" et les services sont essentiels afin de prévenir ce genre de problème.

9.5. Rapports d'activités de l'Intelligence and Security Committee

En ce qui concerne la rédaction des rapports, la loi dispose que :

- le Committee établit un rapport annuel à l'intention du Premier ministre relatif à l'exécution de ses tâches. Il peut aussi, à tout moment, rapporter au Premier ministre tout fait relatif à ses missions;

- le Premier ministre adresse aux Chambres du Parlement le texte de chaque rapport annuel du Committee;

- si le Premier ministre estime, après concertation avec le Committee, que la publication de l'un ou l'autre sujet de ce rapport peut s'avérer néfaste à l'exécution ultérieure des missions des services, il peut l'effacer du rapport présenté aux Chambres du parlement.

Selon Tom King, le Premier ministre, responsable des trois services de renseignement, est conscient de la valeur et du rôle du Committee qu'il a personnellement composé et institué. La majorité des membres du Committee est d'ailleurs issue de son propre parti. Le Committee bénéficie donc de son entière confiance.

Après la rédaction du rapport annuel, des entretiens constructifs ont lieu avec le Premier ministre et, jusqu'à ce jour, aucune divergence d'opinion ne s'est manifestée que ce soit sur le contenu ou sur le principe de la confidentialité.

Les éléments que le Premier ministre souhaite éliminer du rapport à présenter au parlement, seront discutés entre le Committee et le Cabinet office et, en dernière instance, avec le Premier ministre en personne.

Le rapport est ensuite remis à l'ensemble du parlement - et non à une commission parlementaire particulière.

A la suite de la publication du rapport, le Committee organise une conférence de presse. Jusqu'à présent, la presse a toujours respecté la confidentialité des informations non publiées.

9.6. Collaboration avec les services de police et autres services d'ordre vue par le Committee

Le Comité R a reçu les rapports annuels 1995 et 1996 de l 'Intelligence and Security Committee.

Il a également pu consulter les deux rapports intermédiaires du Committee, à savoir ceux du mois de mai 1995 et du mois de décembre 1995.

Ce dernier rapport intermédiaire est intitulé “Report on Security Service Work Against Organised Crime”. Le Committee a établi ce rapport à la suite des négociations relatives à l’implication du Security Service dans la lutte contre le crime organisé.

Le 18 juillet 1996, le “Security Service Act 1996” est entré en vigueur et a permis au Security Service de fournir son aide aux services de police et autres services d’ordre dans le cadre de la prévention et de la lutte contre la grande criminalité.

Les deux autres services de renseignement disposent déjà de cette compétence (visée dans la loi de 1994).Ils entretiennent sans base formelle d’excellentes relations avec le “National Criminal Intelligence Service” et avec le “National Police Agency”.

Dans son rapport d’activités, le Committee aborde longuement cette compétence du Security Service et le fait que son Directeur général veille à coordonner, en accord avec le Directeur général du “National Criminal Intelligence Service “(NCIS), les activités du service avec celles des fonctionnaires de police et des autres services d’ordre.

Le “National Criminal Intelligence Service” est l’organe qui coordonne les informations des services de police dans le cadre du maintien de l’ordre public.

La réglementation intitulée “Réglementations relatives à la coordination des activités du Security Service avec celles des services de police et des autres services d’ordre” a été annexée a ce rapport du Committee. Cette réglementation concrétise l’accord intervenu entre le Sécurity Service et le NCIS en ce qui concerne l’intervention du Security Service dans la prévention et la lutte contre la grande criminalité.
Elle prévoit que le NCIS remplit le rôle d’instance de coordination et a un rôle prépondérant dans la lutte contre la criminalité organisée.

Cet accord a été conclu entre le Directeur général du Security Service et le Directeur général du National Criminal Intelligence Service .
Il fut signé le 2 octobre 1996. Le Committee suit l’application de cet accord et en fera mention dans ses prochains rapports.

10. APPROCHE CRITIQUE

Deux constatations se dégagent de l’étude sur la législation des services de renseignement britanniques.

Tout d’abord, d’un point de vue historique, les services de renseignement britanniques ont profondément influencé l’organisation et le fonctionnement des autres services de renseignement.

Mais peut-on comparer les services de renseignement belges et britanniques ?

Une réponse négative s'impose : ils diffèrent tant en raison de la dimension des territoires sur lesquels ils opèrent qu'en raison du budget qui leur est octroyé, de l'importance du personnel qu'ils emploient et des méthodes de travail qu'ils utilisent. En outre, les deux services de renseignement britanniques sont des services "offensifs" alors que les services belges sont essentiellement "défensifs". Enfin, le Royaume-Uni est confronté à de graves problèmes internes de sécurité.

10.1. La base légale

A l'instar de tous les services de renseignement du monde, les services de renseignement et de sécurité britanniques ont longtemps agi dans le plus grand secret et sans base légale.

Au cours des années 80, des voix se sont fait entendre au sein des services de renseignement. Elles exigeaient une législation appropriée définissant leurs missions et permettant aux services de contrôler leur propre budget.

A la même époque, le Security Service, dont les activités portent sur des ressortissants britanniques, a été pour la première fois sévèrement critiqué.

Le Security service fut le premier à être doté d'une base légale en 1989 en vertu du "Security Services Act 1989".
"L'Intelligence Services Act 1994" allait quant à lui permettre au "Secret Intelligence Service" et au "GCHQ" d'être consacrés légalement.
Enfin, une loi de 1996 a amélioré les lois de 1989 et de 1994 en attribuant une nouvelle mission au "Security Service", à savoir la lutte contre la grande criminalité.

C'est sur l'insistance des services de renseignement britanniques que ces différentes lois ont vu le jour.
La loi de 1994 allait, de plus, instaurer un contrôle parlementaire. En effet, l'Intelligence and Security Committee a été institué pour contrôler les dépenses, la gestion et la politique des différents services de renseignement et de sécurité.

Le Committee n'a pas été instauré à la suite de l'un ou l'autre scandale ou difficulté mais bien parce qu'un désir de transparence des activités du gouvernement et de chacun de ses services (y compris les services de renseignement), était dans l'air du temps.

Ce sont les méthodes des services de renseignement qui furent l'objet de l'attention particulière du législateur.

La loi de 1985 autorise l'interception du courrier et des communications tandis que les lois de 1989 et de 1994 prévoient des procédures autorisant l'intrusion dans la propriété privée et la radiotélégraphie. En outre, la loi de 1994 offre au ministre la possibilité, dans certaines circonstances, de mandater l'Intelligence Service à poser des actes à l'étranger, considérés comme répréhensibles s'ils sont commis au Royaume-Uni.

Outre le contrôle parlementaire, les lois prévoient un double contrôle, à savoir celui des "Tribunals" (commissions), chargés d'examiner les plaintes introduites contre ces services, et les Commissioners (Commissaires du Gouvernement), assurant le contrôle des mesures spéciales que ces services peuvent utiliser.

Par contre, en Belgique, la nécessité d'une législation relative aux services de renseignement et de sécurité et à son contrôle externe s'est fait ressentir à la suite des événements tragiques des années quatre-vingts.

Alors que le Comité R exerce effectivement ce contrôle externe depuis cinq ans déjà, on peut regretter que le projet de loi organique sur les services de renseignement n'est toujours pas voté et que les méthodes impliquant les mesures de nature à violer la vie privée et les droits que la Constitution et la loi confèrent aux particuliers n'y figurent pas. Néanmoins, un projet de loi concernant les habilitations de sécurité est examiné par le Parlement et un projet de loi relatif aux écoutes administratives est actuellement en préparation.

10.2. Les missions

La législation britannique décrit de manière très large les missions de ses services de renseignement.

A l'occasion des travaux préparatoires de la loi, le ministre de l'Intérieur (responsable du Security Service) insista sur le fait que, en la matière, le gouvernement désirait faire face à n'importe quelle nouvelle menace pour la sécurité nationale(8). La définition des missions des services ne devait donc pas être figée. Le législateur a, sans doute pour cette raison, laissé une grande marge de manoeuvre au Security Service puisqu'il lui permet de définir ses priorités en toute autonomie dans le cadre de sa mission très générale de protection de la sécurité de l'Etat.

La situation est quelque peu différente pour le Secret Intelligence Service et le GCHQ. Bien que leurs missions soient formulées de manière plus complète, ils sont moins autonomes puisqu'ils agissent uniquement à la demande du gouvernement par l'intermédiaire d'un organe intitulé "Ministerial Committee on the Intelligence Services" qui peut être comparé au Comité ministériel de renseignement et de sécurité belge.
Ainsi, ces services sont, dans le cadre de leurs opérations, toujours couverts par une demande gouvernementale.

Le projet de loi belge organique sur les services de renseignement ainsi que les amendements proposés, prêtent une attention toute particulière à la définition de leurs missions. Ce projet décrit en outre les différents concepts que sont la sécurité intérieure de l'Etat, la pérennité de l'ordre démocratique et constitutionnel, la sécurité extérieure de l'Etat, l'espionnage, les sectes nuisibles, le crime organisé, etc ... .
Une telle description des missions favorise non seulement leur efficacité mais garantit également la sauvegarde des libertés démocratiques et constitutionnelles des citoyens.
Ces missions peuvent toutefois être mieux définies par le Comité ministériel de renseignement et de sécurité qui précisera notamment le concept de tout intérêt fondamental du pays.

(8) P. Gill - Security Intelligence and the Liberal Democratic State 1994 - Frank Cass- London - p. 99

10.3. La collecte, l'analyse et la diffusion des informations

La législation britannique met en évidence la responsabilité des chefs des service qui doivent s'assurer que seules les informations nécessaires au service et au bon déroulement des missions soient collectées ou publiées. Ceux-ci veillent également à ce que leur service ne pose pas d'actes favorisant les intérêts particuliers d'un parti politique.

Les différents services puisent principalement leurs informations de "sources humaines", de moyens techniques et d'échange de données entre eux et les services de renseignement étrangers. Le GCHQ collecte uniquement les informations à l'aide de moyens techniques.

Les services britanniques disposent donc de plus de moyens que les services belges de renseignement puisque les services belges n'ont pas la possibilité légale de procéder à des écoutes administratives.

Les informations que les services collectent sont expédiées sous leur forme "brute" (non traitées) aux ministères concernés où ils sont analysés.

Une évaluation est toutefois réalisée surtout par le Security service. Cette évaluation est faite par les agents qui ont collecté l'information et non par des analystes.

Ainsi, pour les matières importantes concernant plusieurs départements, l'information brute est transmise au Joint Intelligence Committee qui procéde à l'analyse en collaboration avec l'Assessments Staff.

Ces deux instances étudient les informations reçues à la lumière des données issues des sources ouvertes, telles par la presse par exemple.

En Belgique, chaque service possède ses propres analystes qui étudient les informations transmises par les services extérieurs ou issues des sources ouvertes (presse) et fermées (sources humaines et celles provenant des services de renseignement étrangers).

L'analyse des données telle que pratiquée au Royaume-Uni peut présenter l'avantage d'éviter, grâce à une coordination et une seule évaluation globale, que les différents ministères adoptent une position différente.

Cette méthode de travail présente plusieurs inconvénients :

- les membres du Joint Intelligence Committee tentent parfois de parvenir à une solution de compromis si les experts ne s'entendent pas sur les résultats d'une analyse.
  Mais une analyse fondée sur le concensus le plus large est préférable à des analyses divergentes . En l'occurrence, cette situation est assez rare ;

- la solution britannique est onéreuse car à côté des analyses effectuées par les ministères un organe centralisateur est mis en place ;

- le procédé est critiqué par certains pour sa lenteur; une semaine est parfois nécessaire pour réaliser l'analyse qui en outre est parfois brève et faite sur base d'enquêtes peu approfondies

Toutefois, disposer d'une analyse globale détaillée facilite la prise de décisions des ministres.

En ce qui concerne la diffusion du renseignement, il n'existe pas de différences fondamentales entre la Belgique et le Royaume-Uni; ils diffusent le renseignement au gouvernement.

Le Comité R constate néanmoins avec plaisir que le projet de loi belge organique sur les services de renseignement et de sécurité dispose que le renseignement n'est pas uniquement transmis aux ministres compétents mais également à d'autres autorités. Cependant, ceci exige que ces autorités prennent des mesures suffisantes de sécurité.

10.4. Collaboration mutuelle entre les services de renseignement et les services de police

La législation britannique ne contient aucune disposition concernant la collaboration et la coordination tant entre les différents services de renseignement et de sécurité qu'avec les services étrangers.
Il n'en demeure pas moins que le Security Service et l'Intelligence Service travaillent en étroite collaboration. Le Security Service dépend en grande partie de l'Intelligence Service pour l'obtention de l'information fournie par l'étranger.

Le Co-ordinateur veille à la coordination entre les trois services et les services de police.
Il tente également de résoudre les problèmes entre les services et/ ou avec les services de police.

Les services collaborent aussi avec leurs homologues étrangers. Cette collaboration est supervisée par le JIC

En revanche, la loi édicte la coopération des services de renseignement avec les services de police. Elle prévoit en effet que les chefs des services transmettent les informations nécessaires à la prévention et à la recherche de la grande criminalité. Dès lors, on peut en déduire qu'une obligation d'information existe envers les services de police.

De plus, le directeur général du Security Service a conclu un accord avec le Directeur général du National Criminal Intelligence Service (NCIS) pour coordonner les activités du service avec celles des services de police, ou d'autres services d'ordre.

Comme au Royaume-Uni, le projet de loi belge réglementant les services de renseignement et de sécurité dispose que ces services transmettent des informations aux services de police conformément aux objectifs de leurs missions. En outre, une collaboration efficace est instaurée avec ces mêmes services de police. Cette collaboration se fait sous l'égide du ministère public.

Au Royaume-Uni, la collaboration des services de renseignements avec les service de police et les autres services d'ordre est bonne même si elle n'est pas formalisée dans un protocole d'accord. Cette collaboration porte sur le terrorisme, la criminalité organisée, etc...

10.5. Méthodes particulières des services

La législation britannique permet aux services de renseignement et de sécurité d'avoir recours sous des conditions très strictes à certaines méthodes de nature à violer la vie privée des particuliers et à commettre des actes répréhensibles à l'étranger. Ces derniers ne sont pas à

l'ordre du jour en Belgique. Ces méthodes particulières sont soumises à une autorisation préalable du ministre compétent.

La procédure autorisant l'interception du courrier et des communications est prévue par la loi de 1985 et celle permettant l'intrusion dans la propriété privée et la radiotélégraphie prévue par la loi de 1994.

Le Comité R propose de se baser sur ces législations pour l'élaboration des dispositions législatives permettant aux services belges d'utiliser ces méthodes. Elle lui semble présenter toutes les garanties indispensables à la protection de la vie privée des particuliers et une réponse efficace aux menaces existantes à l'encontre de la sécurité nationale belge.

Le Comité R relève que la législation britannique reprend les principes de subsidiarité et de proportionnalité : il s'agit de s'assurer que ces méthodes sont uniquement utilisées si les informations souhaitées ne peuvent être obtenues autrement, de vérifier si l'action est absolument nécessaire à la bonne exécution des missions du service enfin, et surtout de s'assurer que la loi a été correctement appliquée par celui qui délivre les autorisations à se livrer à de telles méthodes.

Le Comité R recommande également que l'utilisation de ces méthodes soit soumise à un contrôle strict afin de garantir la protection des droits des citoyens.

10.6. Organes de contrôle

Est-il encore nécessaire de répéter que le contrôle des services de renseignement s'impose dans un Etat de droit démocratique. L'analyse de la législation britannique permet de constater que l'appareil de contrôle des activités des services de renseignement appliqué au Royaume-Uni est complexe et peut perdre ainsi de son efficacité. En effet des commissions, des commissaires du gouvernement ainsi que des parlementaires exercent un contrôle sur les services. La multiplicité de ces organes de contrôle ne permet pas au citoyen de situer l'organe auquel il peut s'adresser.

Il est absolument nécessaire que chaque citoyen s'estimant lésé ou directement concerné dans une opération des services de renseignement ait la possibilité de déposer une plainte.

Le Comité R estime toutefois qu'un seul organe peut exercer en Belgique, qui n'est pas un grand pays comme le Royaume-Uni, les différentes formes de contrôle. Ce système permet un contrôle global et une diminution des frais du fonctionnement de l'Etat. Ce seul organe pourrait aussi assurer le contrôle des futures méthodes utilisées par les services.

Au Royaume-Uni, le commissaire du gouvernement a la possibilité de contrôler les ordonnances délivrées par le ministre à la demande des services lorsqu'ils souhaitent s'introduire dans la propriété privée ou procéder à l'interception de communications ou de courriers. Ce commissaire du gouvernement vérifie en effet si le ministre a exercé correctement les compétences qui lui sont octroyées (principe de l'égalité). Il peut intervenir automatiquement ou après introduction d'une plainte.

Le Comité "R" recommande que non seulement les services soient tenus de fournir toutes les informations nécessaires comme en dispose la loi du 18 juillet 1991 relative au contrôle sur ces services mais également d'élargir cette obligation aux fonctionnaires des ministères compétents.

Le Comité R devrait également pouvoir consulter les dossiers constitués par les ministères lors de demandes d'utilisation d'une mesure telle que l'interception des communications ou de la correspondance.

Comme au Royaume-Uni, le contrôle des services de renseignement doit pouvoir continuer à être exercé par un organe au sein duquel l'opposition parlementaire démocratique est représentée .

10.7. Autoriser une Commission parlementaire à exercer un contrôle ?

Au Royaume-Uni, le Premier ministre nomme des parlementaires pour exercer le contrôle sur les services de renseignement et de sécurité. Ceux-ci relèvent directement du Premier ministre. Cette façon de nommer les membres du Committee donne lieu actuellement à un débat.

Ce système ne peut être comparé au contrôle exercé par le Comité R qui rapporte directement au Parlement.
La méthode de travail britannique se caractérise par une grande interaction entre le pouvoir législatif et exécutif.

Le Comité R a posé la question de savoir si on peut donner directement à une commission parlementaire les missions de l'actuel Committee. Tom King a expliqué que l'expérience révèle que chaque document qui entre au Parlement est divulgué. Il n'est donc pas inimaginable de prédire que les services de renseignement se conformeraient à une application très stricte de la loi et refuseraient de fournir des informations qui pourraient mettre en péril leurs activités et leurs relations avec leurs homologues étrangers.

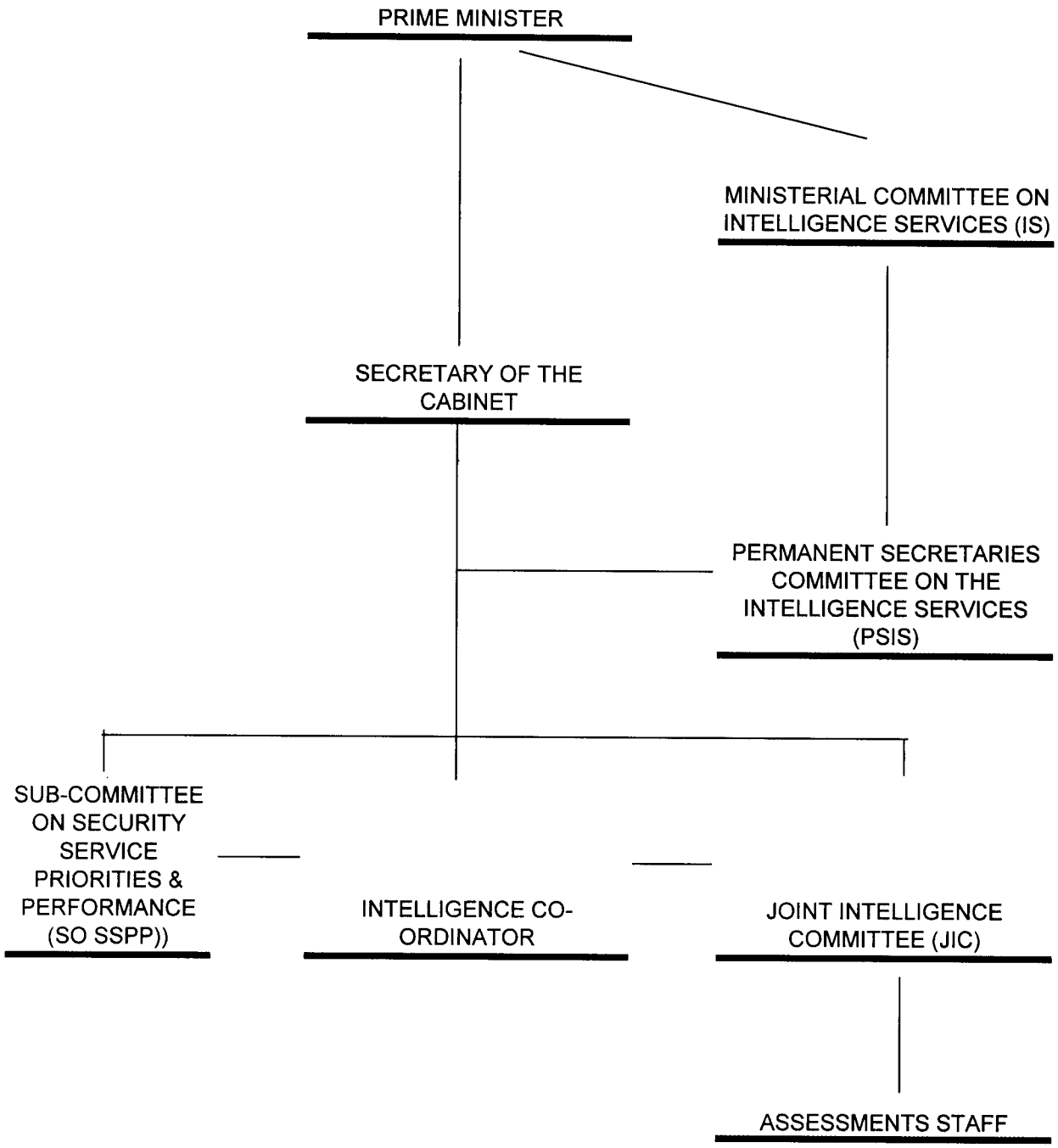
Une telle modification ne contribuerait donc apparemment pas à augmenter le pouvoir de la commission parlementaire chargée directement du contrôle des services en raison du climat de méfiance qui règne à l'égard du parlement.
Pour Tom King, la forme actuelle de contrôle parlementaire peut être considérée par tous comme la plus appropriée si le nouveau Committee poursuit ses activités de manière efficace et professionnelle.

Créer en Belgique une commission parlementaire de contrôle des services de renseignement permettrait une surveillance plus directe des services par des parlementaires. Mais le problème majeur de la diffusion des informations secrètes reste posé.

10.8. L’établissement d’un rapport annuel

Au Royaume-Uni, les chefs des services établissent un rapport annuel sur le fonctionnement des services et le transmettent au Premier ministre et au ministre compétent. Ce rapport n’est pas public.

Comme dans l’étude de la législation néerlandaise relative aux services de renseignement et de sécurité, le Comité R recommande que les services établissent un rapport annuel public. Le Comité R réitère cette recommandation . Il estime que la publication d’un rapport annuel d’activités des services de renseignement est de nature à restaurer et à améliorer la confiance du public dans les services de renseignement.


PRIME MINISTER
MINISTERIAL COMMITTEE ON INTELLIGENCE SERVICES (IS)
SECRETARY OF THE CABINET
PERMANENT SECRETARIES COMMITTEE ON THE INTELLIGENCE SERVICES (PSIS)
SUB-COMMITTEE ON SECURITY SERVICE PRIORITIES & PERFORMANCE (SO SSPP))
INTELLIGENCE CO-ORDINATOR
JOINT INTELLIGENCE COMMITTEE (JIC)
ASSESSMENTS STAFF

TITRE II : NOS SERVICES DE RENSEIGNEMENT

PREMIERE PARTIE : LES ETUDES

CHAPITRE 1 : ETUDE DES PROJETS DE LOI RELATIFS AUX HABILITATIONS DE SÉCURITÉ

1. INTRODUCTION

Les 23 septembre et 6 octobre 1997, le Comité R a été entendu par les Commissions chargées du suivi parlementaire des Comités permanents de contrôle des services de police et de renseignements. A ces occasions et à la demande du Comité R, les commissions n'ont émis aucune objection quant à la proposition du Comité R de procéder à l' étude de l'avant projet de loi relative aux habilitations de sécurité.

Le Comité R a été entendu le 17 février 1998 par la Commission de la Défense nationale à ce sujet.

Dans son rapport général d'activités 1995, le Comité R avait procédé à une enquête sur les certificats de sécurité.

Le but de cette enquête tendait à examiner :

- la manière dont les enquêtes de sécurité étaient menées;
- la manière dont les renseignements obtenus étaient exploités et évalués;
- à qui et par quel moyen le résultat de l'enquête était communiqué;
- les bases et les implications juridiques.

Dans ses recommandations, le Comité R estime que, pour rencontrer les exigences de l'article 8 de la Convention de sauvegarde des droits de l'homme et de ses libertés fondamentales et de l'article 22 de la Constitution, il paraissait urgent de régler la problématique par une loi précise.

En 1996, le Comité R a rapporté au Parlement l'échange de vues qu'il avait eu avec les représentants des ministres de la Justice et de la Défense nationale.

Les points de vue suivants ont été exposés au cours de l'entretien :

- l'enquête s'étend parfois aux membres de la famille de la personne qui a besoin d'un certificat de sécurité. Il s'agit d'un problème très complexe eu égard surtout à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. L'enquête sur l'entourage du candidat sera indispensable dans des cas déterminés notamment en raison de certaines stipulations contenues dans des directives de l'OTAN concernant les certificats de sécurité.

Tous les participants à la réunion étaient d'accord aussi bien sur la complexité de la matière que sur la nécessité de la régler par une loi. Il a été fait référence à la manière dont certains pays ont tenté de remédier à ce problème (par exemple : dans certains pays où l'épouse du candidat remplit un formulaire séparé);

- aucune enquête de sécurité ne peut être effectuée sans l'accord préalable et écrit du candidat. Le problème se posait de savoir si cet accord donné est valable lors du renouvellement du certificat de sécurité (tous les cinq ans). Un risque est réel de voir l'intéressé essayer d'échapper à certaines missions en refusant son consentement à l'exécution d'une enquête de sécurité, principalement pour les militaires dans le cadre d'une mission à l'étranger, si ce consentement est requis à chaque renouvellement;

- la manière dont est menée l'enquête de sécurité et les critères à prendre en ligne de compte devront correspondre au degré du certificat de sécurité. Un équilibre raisonnable doit être trouvé dans l'ampleur de l'enquête de sécurité compte tenu des deux principes applicables en la matière, c'est à dire le "need to know" d'une part et "la possibilité d'accès aux données classifiées" d'autre part. Une certaine souplesse est nécessaire dans la fixation des critères puisque ceux-ci évolueront avec le temps;

- la problématique de la quantité des certificats de sécurité à délivrer a été envisagée. Le projet de loi organique des services de renseignement et de sécurité prévoit que "le collège du renseignement et de la sécurité" sera compétent pour la délivrance des certificats de sécurité mais ne prévoit pas de délégation aux services de renseignement;

- la question de l'accès aux données administratives et de la consultation des dossiers judiciaires détenus par les officiers du ministère public et des dossiers détenus par les employés des administrations publiques, indispensables pour l'exécution des enquêtes de sécurité, a été abordée;

- enfin la procédure d'appel en cas de refus ou de retrait d'un certificat de sécurité a été examinée avec beaucoup d'attention.

Les projets de loi n°1193/1 et 1194/1 ont un double objet : les enquêtes de sécurité d'une part et l'institution du Comité R comme organe de recours en cas de refus de délivrance ou du retrait du certificat de sécurité, d'autre part (projet de loi II (n°1194/1).

2. PROJET DE LOI y (N°1193/1)

Ce projet de loi officialise des procédures actuellement utilisées pour l'octroi des certificats de sécurité. Son grand mérite est de leur donner un fondement légal. Cette loi est nécessaire au regard des articles 8 § 2 et 60 de la Convention européenne de sauvegarde des droits de l'homme, de l'article 22 de la Constitution et de la législation du 8 décembre 1992 relative à la protection de la vie privée.

2.1. Chapitre 1er : Dispositions générales

Article 3

A cet article le Comité R propose d'insérer un point 5° qui serait libellé comme suit :

"Dans la présente loi on entend par :

5° *"document, renseignement ou matériel classifié", tout document ou matériel dont le caractère confidentiel ou secret a été établi par la loi ou par l'autorité habilitée à le faire en vertu de la loi."*

Ce qui suppose qu'une autre loi sur les documents, renseignements et matériels classifiés complète la loi sur les habilitations de sécurité. Cette loi devra indiquer :

- les principes généraux qui peuvent mener à la classification d'un document ou d'un matériel, c'est-à-dire les intérêts à protéger par la classification;

- les documents, renseignements et matériels qui sont classifiés par nature, c'est-à-dire sans le recours à une procédure pour le faire (par exemple : l'identité des sources humaines qui ont demandé l'anonymat, les renseignements classifiés communiqués par une autorité étrangère avec laquelle la Belgique est liée par un accord de sécurité ou de défense, certaines matières et informations dans le domaine de l'énergie et des armes nucléaires, etc...);

- quelle(s) autorité(s) est (sont) habilitée(s) à désigner les autorités, fonctionnaires ou militaires compétents pour classifier/déclassifier un document ou un matériel; (par exemple : le comité ministériel du renseignement, le collège du renseignement, le ministre compétent peuvent désigner des fonctionnaires d'un certain niveau pour classifier certains documents ; cela peut varier en fonction du degré de classification);

- la procédure par laquelle une autorité décide de classifier/déclassifier un document ou un matériel ; éventuellement les délégations possibles ;

- les degrés et les effets de la classification, sa durée ;

- le principe des mesures de sécurité à prendre en vue de protéger les matériels, renseignements et documents classifiés ;

- les modalités particulières relatives à la saisie judiciaire et à la production de documents, de renseignements et de matériels classifiés en justice ou devant des Commissions parlementaires ;

- un système de contrôle extérieur sur la classification, de manière à éviter qu'une telle procédure soit détournée de ses objectifs légaux ;

- les sanctions pénales en cas de divulgation non autorisée d'informations classifiées ou de négligences dans l'observance des mesures de sécurité.

Les degrés de classifications, par exemple, seraient fixées par la loi. Par contre la désignation de certaines autorités ou fonctionnaires compétents pour classifier un document matériel, les mesures de sécurité à prendre, etc... seraient fixées par le Roi.

Article 5

L'article 5 du projet de loi relatif aux habilitations de sécurité établit des systèmes d'exception:

L'administrateur général de la Sûreté de l'Etat et le chef du Service général de renseignement et de la Sécurité des Forces armées sont compétents - actuellement sur délégation de l'ANS pour attribuer (ou retirer) les certificats vis-à-vis de leur personnel.

Le projet de loi restreint les compétences de l'autorité de sécurité dans la mesure où une délégation aux chefs des services de renseignement est prévue. Cette restriction ne concerne pas les départements ministériels concernés.

A l'estime du Comité R et de son Service d'enquêtes, ces compétences éclatées constituent un obstacle à une bonne coordination, elle-même source de sécurité.

Le Comité R recommande dès lors de prévoir que l'autorité de sécurité aura une mission centralisatrice et une compétence de coordination opérationnelle de tout le processus de la délivrance des habilitations de sécurité pour toute personne qui doit obtenir une habilitation de sécurité. Le Comité R recommande donc de ne pas prévoir de délégation aux chefs des services de renseignement mais d'attribuer à l'autorité de sécurité, les prérogatives conférées par l'article 5 à l'administrateur général de la Sûreté de l'Etat et au chef du Service général du renseignement.

Le Roi fixe la composition de l'autorité de sécurité et les procédures d'application en la matière, en ce compris la traduction des exigences légales dans le questionnaire de base.

Tout d'abord, le législateur évitera ainsi des différences de traitement quant aux méthodes utilisées, à l'appréciation des critères de sécurité et aux évaluations des informations recueillies.

Ensuite, outre l'insécurité que de telles disparités génèrent, le Comité R se pose la question de savoir si le projet de loi n'instaure pas de cette manière un régime d'inégalité des citoyens devant la loi.

Enfin, il semble nécessaire que l'autorité de sécurité assure un minimum d'unité de "jurisprudence". Peut-on admettre que des candidats soient traités différemment suivant qu'ils postulent une place dans tel ou tel service ?

2.2. Chapitre II : De l'avertissement et de l'accord

Article 6

"§1er. La personne qui doit obtenir une habilitation de sécurité est avertie du niveau et de l'objet de l'habilitation, ainsi que des types de données qui pourront être examinées ou vérifiées lors de l'enquête de sécurité, des modalités de celle-ci et de la durée de validité de l'habilitation de sécurité.
Son accord est requis pour pouvoir procéder à l'enquête de sécurité nécessaire à la délivrance de l'habilitation. Cet accord vaut également pour toute enquête de sécurité ultérieure visant à vérifier que les conditions requises pour le niveau initial de l'habilitation sont toujours réunies. L'intéressé est néanmoins toujours préalablement averti de chaque enquête de sécurité, conformément au § 1er, alinéa 1er.
Cet accord peut à tout moment être retiré par la personne concernée qui ne consent plus à faire l'objet d'une enquête de sécurité ou à posséder une habilitation de sécurité.
Si l'habilitation est requise pour l'accès à un emploi, une fonction ou un grade, le refus explicite du candidat ou, le cas échéant, l'absence d'accord dans un délai de quinze jours suivant le jour de la réception du document l'avertissant de l'enquête, met automatiquement fin à la procédure de recrutement, d'engagement, de nomination ou de promotion.

§ 2. L'accord prévu au § 1er n'est pas exigé lorsque l'habilitation de sécurité est requise pour l'exercice d'une fonction pour laquelle l'intéressé peut - en raison de son statut - être désigné sans son consentement. L'intéressé est néanmoins toujours préalablement averti de l'enquête de sécurité, conformément au § 1er, alinéa 1er.
Avant son recrutement ou son engagement dans un emploi soumis à un tel statut, le candidat doit consentir à ce que, pour le temps qu'il reste soumis à ce statut et s'il devait être désigné à une fonction requérant une habilitation de sécurité, des enquêtes de sécurité soient effectuées conformément à l'alinéa précédent.

§ 3. Les personnes, âgées de dix-huit ans accomplis, cohabitant avec la personne pour laquelle l'habilitation est requise, sont également averties, lorsqu'en fonction du niveau de l'habilitation, elles doivent faire l'objet d'une enquête de sécurité individuelle."

Commentaires

Alinéa premier :

A l'instar du Conseil d'Etat, le Comité R estime que les restrictions au droit à la vie privée doivent procéder de la loi et non des normes élaborées par des instances de droit international comme la directive CM55/15 de l'OTAN ou des directives de l'UEO dont la Belgique est membre.

Le Comité R recommande en conséquence que la Belgique légifère conformément à la jurisprudence de la Cour européenne de sauvegarde des Droits de l'Homme (arrêts Leander et Malone). La loi doit donc déterminer l'ampleur de l'enquête par rapport aux différents degrés du certificat de sécurité "confidentiel", "secret" et "très secret". De cette manière la loi sera précise (arrêts Leander du 26 mars 1987 et Malone du 2 août 1984).

A défaut de tracer les contours des investigations par rapport à leur finalité spécifique ne sommes nous pas dans le champ d'application d'une loi ... imprécise ? En effet, le citoyen qui en fait l'objet n'est pas à même d'en prévoir les conséquences et se trouve dépourvu de contrôle. Ne serait-ce pas un motif de recours en cas de décision de refus ou de retrait du certificat de sécurité ? A défaut de pouvoir critiquer le fond, l'attaque se focalisera sur la forme.

Alinéa 3 :

Le Comité R estime quant à lui, à l'instar du gouvernement, et contrairement à la Commission de la protection de la vie privée que l'accord de la personne majeure et cohabitant avec la personne qui doit obtenir une habilitation de sécurité n'est pas nécessaire au regard du principe de l'égalité des belges devant la loi.

En effet, le projet de loi cadre bien avec la définition jurisprudentielle de la Cour d'arbitrage de la violation des articles 10 et 11 de la Constitution : "les règles constitutionnelles de l'égalité et de la non discrimination n'excluent pas qu'une différence de traitement soit établie entre des catégories de personnes, pour autant qu'elle repose sur un critère objectif et qu'elle soit raisonnablement justifiée.
L'existence d'une telle justification doit s'apprécier en tenant compte du but et des effets de la mesure critiquée ainsi que de la nature des principes en cause.
Le principe d'égalité est violé lorsqu'il est établi qu'il n'existe pas de rapport raisonnable de proportionnalité entre les moyens employés et le but visé."[(1)]

---

(1) Principe énoncé dans tous les arrêts de la Cour d'arbitrage publiés au Moniteur belge.

Deux personnes font l'objet d'une enquête de sécurité. L'une a besoin d'une habilitation de sécurité pour accéder à une fonction, le cohabitant pas. Elles ne font donc pas partie de la même catégorie de personnes, même si elles font toutes deux l'objet d'une enquête de sécurité.

Le Comité R estime que le gouvernement a justifié raisonnablement et en proportionnalité la différence de traitement de ces personnes en visant d'une part, "l'intérêt professionnel majeur de la personne pour laquelle l'habilitation de sécurité est requise", et d'autre part, "le droit du cohabitant au respect de sa vie privée, qui devra en toute hypothèse être averti de l'enquête de sécurité effectuée à son sujet, ce qui constitue une mesure suffisante au regard de la jurisprudence actuelle de la Cour européenne des droits de l'homme".

Le Comité R est d'avis que le principe d'égalité n'est donc pas violé puisqu'il est établi qu'il existe un rapport raisonnable de proportionnalité entre les moyens employés et le but visé.

Article 7

"*L'avertissement prévu à l'article 6 se fait par la remise à l'intéressé, par l'officier de sécurité et contre accusé de réception, d'un document dont le modèle est fixé par le Roi et d'un questionnaire de base. Le document est conservé par l'intéressé et le questionnaire de base dûment complété est remis à l'officier de sécurité contre accusé de réception.*
L'accord ou le retrait de l'accord prévus à l'article 6 se fait par la remise à l'officier de sécurité, par l'intéressé et contre accusé de réception, d'un document dont le modèle est fixé par le Roi.
L'accusé de réception visé à l'alinéa 1er, le document visé à l'alinéa 2 et le questionnaire de base sont transmis par l'officier de sécurité à l'autorité de sécurité".

Dans la mesure où le projet de loi est revu en son article 6 dans le but d'établir la corrélation entre la catégorie d'habilitation de sécurité et l'ampleur de l'enquête de sécurité, il ne semble plus utile de rencontrer la préoccupation du Conseil d'Etat qui visait "*à faire apparaître les données essentielles qui pourront être recueillies au travers dudit questionnaire".*[(2)]

D'autre part, le gouvernement a parfaitement motivé sa décision en ce qui concerne l'avertissement donné aux personnes cohabitant avec la personne qui doit obtenir une habilitation de sécurité et les personnes mentionnées à l'occasion de l'enquête de sécurité, en justifiant la loi par des critères objectifs et raisonnables (critères de la Cour d'arbitrage).

2.3. Chapitre III : De l'enquête de sécurité

Article 8

"L'enquête de sécurité est effectuée par un service de renseignement et de sécurité.
Lorsque la personne pour laquelle l'habilitation de sécurité est requise réside, transite ou séjourne à l'étranger ou y a transité, séjourné ou résidé, ce service peut solliciter la collaboration des services compétents du pays hôte.

---

(2) Page 38 du document parlementaire étudié

Les agents des services extérieurs de la Sûreté de l'Etat et les membres du Service général du renseignement et de la sécurité chargés d'effectuer les enquêtes de sécurité sont désignés respectivement par le ministre de la Justice, sur la proposition de l'administrateur général de la Sûreté de l'Etat, et par le ministre de la Défense nationale, sur la proposition du chef du Service général du renseignement et de la sécurité des Forces armées.
Ils reçoivent, lors de leur désignation, une carte de légitimation, dont le modèle est fixé par le ministre compétent. Cette carte ne peut être utilisée que dans le cadre des enquêtes de sécurité et doit être immédiatement restituée à l'autorité qui l'a délivrée lorsque la désignation visée à l'alinéa 3 a pris fin".

Article 9

"Dans le cadre des enquêtes de sécurité et uniquement à cette fin, les agents et les membres visés à l'article 8 peuvent, outre les compétences qu'ils tiennent de l'article 10, § 2, de la loi du 18 juillet 1991 organique des services de renseignement et de sécurité, et dans le respect de l'article 10, § 1er, de cette même loi, procéder à toute investigation et recueillir tous les renseignements nécessaires à l'enquête.

A cette fin, ils peuvent, sur présentation de leur carte de légitimation :

1° accéder sans frais, et quel que soit leur niveau, au casier judiciaire central tenu au ministère de la Justice, aux casiers judiciaires et registres de la population et des étrangers tenus par les communes, au registre national, au registre d'attente des étrangers, ainsi qu'aux données policières qui sont accessibles aux fonctionnaires de police lors de l'exécution de contrôles d'identité;

2° sur présentation du document visé à l'article 7 attestant l'accord ou, le cas échéant, l'avertissement de la personne concernée, demander toute information utile en possession des services de police générale;

3° sur présentation du document visé au point 2°, requérir des services publics, dont la liste est arrêtée par le Roi, la communication de tous renseignements utiles relatifs à l'identité ou à la solvabilité financière de la personne concernée, dont ces services disposent. Ces services mettent à leur disposition, sans frais, des photocopies, extraits, ou copies conformes de documents, pièces, registres, livres, bandes magnétiques ou disques informatiques demandés.

Ils sont tenus d'exhiber leur carte de légitimation à toute autre personne dont ils sollicitent le concours dans le cadre des enquêtes de sécurité. Si elle en fait la demande, ils sont également tenus d'exhiber le document visé à l'article 7, attestant l'accord de la personne qui fait l'objet de l'enquête, ou, lorsque cet accord n'est par requis, l'avertissement.

Lorsque l'enquête de sécurité a pour finalité l'octroi d'une habilitation de sécurité à un ressortissant d'un Etat étranger par les autorités compétentes de cet Etat dans le cadre d'accords d'assistance mutuelle liant la Belgique, ces agents et membres sont tenus d'exhiber

un document émanant de l'autorité de sécurité attestant la demande de collaboration de l'Etat étranger."

Article 10

"Les agents et membres visés à l'article 8 doivent prendre les mesures internes nécessaires afin de garantir le caractère confidentiel des faits, actes ou renseignements dont ils ont pris connaissance dans le cadre des enquêtes de sécurité".

Le Comité R recommande que la loi précise que la carte de légitimation prévue par l'article 9 du projet de loi, fasse apparaître les références légales instaurant les pouvoirs de titulaires, ainsi qu'il le préconise dans son enquête sur les cartes de service des services de renseignement. La clarté n'a jamais nuit à une bonne application de la loi.

2.4. Chapitre IV : De l'habilitation de sécurité

Outre ce qui a été écrit au commentaire du chapitre 1er du projet de loi (article 5), le Comité R estime que la loi devrait préciser la durée du certificat de sécurité qui pourrait être d'une période de 5 ans comme c'est le cas à l'heure actuelle.

2.5. Chapitre V : Du secret

Le Comité R regrette, comme il l'a fait dans l'étude auquel il a procédé sur le projet de loi sur les services de renseignement, que ni le projet de loi sur les habilitations de sécurité, ni son exposé des motifs, ne définissent le secret protégé par la loi. Le Comité R renvoie le lecteur à ce propos à sa proposition d'insérer un point 5 à l'article 3 du présent projet de loi et à l'étude qu'il a menée et publiée sur "le secret" dans ce rapport.

Le Comité R estime dès lors, à l'instar du Conseil d'Etat, que puisque cet article ne définit pas le secret, il est préférable de l'insérer dans le chapitre "Dispositions finales" et non pas de créer un chapitre intitulé "Du secret".

2.6. Chapitre VI : Dispositions diverses et finales

Le Comité R a relevé qu'aucune mention n'est faite concernant la durée de conservation des données à caractère personnel recueillies à l'occasion de l'enquête de sécurité. Il estime en outre qu'il convient de détruire ce type de données en raison du caractère ponctuel de la nécessité de l'habilitation de sécurité.

Il propose dès lors d'insérer un article 15 § 1er relatif à la destruction des données recueillies à l'occasion des enquêtes de sécurité et que cet article soit rédigé comme suit :

"Hormis lorsque les raisons pour lesquelles elles ont été recueillies sont toujours présentes et que leur conservation reste dès lors impérative, les données à caractère personnel collectées ou reçues dans le cadre de la présente loi sont détruites dès que la personne concernée ne sera plus susceptible de faire l'objet d'une enquête de sécurité (ou : seront automatiquement détruites dès que la personne concernée n'exercera plus la fonction dans un des secteurs énumérés à l'article 2 al. 1)".

Les données recueillies à l'occasion des enquêtes de sécurité visées à l'alinéa 2 de l'article 2, seront détruites à l'expiration d'un délai de 2 ans, à compter de la date de l'expiration de la validité du certificat de sécurité".

3. PROJET DE LOI II (N° 1194/1)

Ce projet de loi porte création d'un organe de recours en matière d'habilitation de sécurité. Il confie au Comité R une compétence juridictionnelle.

Un triple avantage existe :

- tout d'abord ce projet de loi a le mérite d'exister en même temps qu'il assure la pérennité du Comité R en lui attribuant cette mission spécifique;

- ensuite, le Comité R connaît la matière et est habilité à prendre connaissance des documents sur lesquels la décision de refus de retrait s'appuie;

- enfin, le Comité R peut statuer dans des délais relativement brefs ce qui n'est pas le cas par exemple du Conseil d'Etat ou d'autres juridictions confrontées à un arriéré important.

Les choses ne sont pas aussi simples toutefois. Si l'idée paraît séduisante, il convient de prendre ses distances.

La décision de refus ou de retrait de l'habilitation de sécurité est une décision de type administratif. Dans ces conditions, ne suffisait-il pas de prévoir un recours devant le Conseil d'Etat ?

La décision du Comité R, saisi sur la base d'un recours, est une décision de type "juridictionnel" et, à ce titre, ne peut qu'émaner d'un organe offrant toutes les garanties d'indépendance et d'impartialité.

La loi consacre ainsi l'indépendance du Comité R par rapport au Parlement, même s'il fait rapport à ce dernier (doc. parl. Chambre des Représentants - 1305/1 - 90/91 p. 5).
Le Comité R s'en réjouit donc.

Toutefois, le Comité R peut-il être à la fois juge et partie ?

Dans sa mission de contrôle, saisi sur base d'une plainte, il avalise ou critique la manière dont l'enquête de sécurité a été menée.

La lecture de la loi apprend que, dans le cadre de sa compétence de recours, le Comité R est incompétent pour contrôler les conditions dans lesquelles l'enquête de sécurité a été effectuée. La loi ne mentionne pas explicitement cette compétence même si elle permet certains actes d'enquête (article 5) : *"S'il l'estime utile à l'examen du recours, l'organe de recours requiert du service de renseignement et de sécurité qui a procédé ou procède à l'enquête de lui communiquer une copie du dossier d'enquête dans son intégralité. Il peut également requérir de ce service la communication de toute information complémentaire qu'il juge utile à l'examen du recours dont il est saisi."*

A l'inverse de la loi du 18 juillet 1991, le Comité R ne peut donc pas entendre toute personne qu'il juge utile d'entendre et doit ainsi se limiter aux documents que les services de renseignement accepteront de lui transmettre.

Le Comité R estime dès lors qu'il devra statuer en ayant les yeux partiellement bandés.

Bien que la loi (article 3) précise que les dispositions des articles 32 à 56 de la loi du 18 juillet 1991, instaurant notamment le Comité R ne sont plus d'application, peut-on accepter sans sourciller que les décisions prises dans le cadre d'une plainte soient éventuellement en contradiction avec la décision issue d'un recours introduit à la suite d'un refus de délivrance du certificat ?

Ces deux fonctions sont incompatibles. Préciser que les dispositions légales des articles 32 à 56 de la loi organique du 18 juillet 1991 ne sont plus d'application dans le cadre d'un recours exercé devant le Comité R, est en réalité faire l'aveu de la faiblesse du système par la dénonciation du risque de confusion des rôles. Ce système sèmera le trouble dans l'esprit des requérants.

Ce défaut apparent d'impartialité ne servira-t-il pas de fondement à l'exercice de recours devant la Cour européenne des droits de l'homme ?

Dans ces conditions, ne convenait-il pas de maintenir les pouvoirs d'investigation au Comité R en sa qualité d'organe de recours ? Les membres du Service d'enquêtes ont la qualité d'officier de police judiciaire (article 45 de la loi du 18 juillet 1991). Ils peuvent mettre leurs compétences au service du Comité R notamment quant au point de savoir si les informations recueillies dans le cadre de l'enquête sur l'habilitation de sécurité correspondent à la réalité.

En outre, le projet de loi permet d'opposer le "danger source" au Comité R à l'occasion de son rôle de juridiction de recours, ce que la loi du 18 juillet 1991 n'a pas voulu afin d'établir un véritable contrôle (article 48 de la loi du 18 juillet 1991).

Pour en revenir à la compétence du Conseil d'Etat en qualité d'organe de recours, rappelons que l'arrêté du Régent déterminant la procédure devant la section d'administration du Conseil d'Etat (Moniteur belge 23-24 août 1948; Er. moniteurs belges 8 octobre 1948 et 21 novembre 1948) permet en son article 16 : *"Le conseiller et le membre de l'auditorat désignés peuvent correspondre directement avec toutes les autorités et leur demander tous renseignements utiles.*

Ils ont le droit de se faire communiquer tous documents par les autorités administratives. Ils peuvent réclamer aux parties, à leurs avocats ou au commissaire du gouvernement toutes explications complémentaires."

D'autres solutions peuvent être envisagées. Le gouvernement et le Conseil d'Etat avaient envisagé, dans un premier temps, de créer une commission qui aurait cette compétence spécifique de recours. Le Comité R propose une formule qui pallierait les inconvénients décrits ci-dessus.
Il suggère que le Parlement confie la compétence de recours à une commission qui serait composée de trois magistrats retraités disposant d'un certificat de sécurité, désignés par le premier président de la Cour d'appel de Bruxelles pour une durée de cinq ans, par exemple. Cette proposition s'inspire de la loi sur la libération conditionnelle qui vient d'être votée au Parlement. Ces magistrats disposeraient des mesures d'instruction comparables à celle du Comité R dans le cadre de sa compétence de contrôle ou pourraient saisir le Service d'enquêtes du Comité R pour vérifier les données fournies par l'autorité de sécurité et les services de renseignement. La loi devrait donner au président de cette commission les pouvoirs prévus par l'article 48 de la loi du 18 juillet 1991.

4. RECOMMANDATIONS

4.1. L'autorité de sécurité

Le Comité R recommande de prévoir que l'autorité de sécurité aura une mission centralisatrice et une compétence de coordination opérationnelle de tout le processus de la délivrance des habilitations de sécurité pour toute personne qui doit obtenir une habilitation de sécurité. Le Comité R recommande donc de ne pas prévoir de délégation aux chefs des services de renseignement mais d'attribuer les prérogatives conférées par l'article 5 à l'administrateur général de la Sûreté de l'Etat et au chef du Service général du renseignement, à l'autorité de sécurité.

Le Roi fixe la composition de l'autorité de sécurité et les procédures d'application en la matière, en ce compris la traduction des exigences légales dans le questionnaire de base.

4.2. De l'avertissement et de l'accord

Le Comité R recommande que la Belgique légifère conformément à la jurisprudence de la Cour européenne de sauvegarde des droits de l'homme (arrêts Leander et Malone). La loi doit donc déterminer, avant d'aborder l'avertissement et l'accord, l'ampleur de l'enquête par rapport aux différents degrés du certificat de sécurité : "confidentiel", "secret" et "très secret". De cette manière la loi sera précise (arrêts Leander du 26 mars 1987 et Malone du 2 août 1984).

Le Comité R est d'avis que le principe d'égalité n'est donc pas violé puisqu'il est établi qu'il existe un rapport raisonnable de proportionnalité entre les moyens employés et le but visé.

4.3. De l'enquête de sécurité

Le Comité R recommande que la loi précise que la carte de légitimation prévue par l'article 9 du projet de loi, fera apparaître les références légales instaurant les pouvoirs des titulaires des cartes de légitimation, ainsi qu'il le préconise dans son enquête sur les cartes de service des services de renseignement. La clarté n'a jamais nuit à une bonne application de la loi.

4.4. De l'habilitation de sécurité

Le Comité R recommande qu'à l'article 3 de la loi soit inséré un point 5° qui serait libellé comme suit :

"Dans la présente loi on entend par :

5° "document, renseignement ou matériel classifié", tout document ou matériel dont le caractère confidentiel ou secret a été établi par la loi ou par l'autorité habilitée à le faire en vertu de la loi."

Ce qui suppose qu'une autre loi sur les documents, renseignement et matériel classifiés complète la loi sur les habilitations de sécurité.
Outre ce qui a été écrit aux recommandations concernant l'autorité de sécurité, article 5 du projet de loi, le Comité R estime que la loi devrait préciser la durée du certificat de sécurité qui pourrait être d'une période de 5 ans comme c'est la cas à l'heure actuelle.

4.5. Du secret

Le Comité R estime, à l'instar du Conseil d'Etat, que puisque cet article ne définit pas la notion du secret, il est préférable de l'insérer dans le chapitre "Dispositions finales" et non pas de créer un chapitre intitulé "Du secret".

4.6. Dispositions finales et transitoires

Le Comité R recommande qu'un article 15 § 1er relatif à la destruction des données recueillies à l'occasion des enquêtes de sécurité soit rédigé comme suit :

"Hormis lorsque les raisons pour lesquelles elles ont été recueillies sont toujours présentes et que leur conservation reste dès lors impérative, les données à caractère personnel collectées ou reçues dans le cadre de la présente loi sont détruites dès que la personne concernée ne sera plus susceptible de faire l'objet d'une enquête de sécurité (ou : seront automatiquement détruites dès que la personne concernée n'exercera plus la fonction dans un des secteurs énumérés à l'article 2 al. 1)

Les données recueillies à l'occasion des enquêtes de sécurité visées à l'alinéa 2 de l'article 2, *seront détruites à l'expiration d'un délai de 2 ans, à compter de la date de l'expiration de la validité du certificat de sécurité*."

4.7. Recours devant le Comité "R"

Le Comité R, eu égard aux considérations émises ci-dessus, propose au Parlement trois solutions qui peuvent être résumées comme suit :

- le Parlement décide de donner au Comité R la compétence de recours telle que le gouvernement l'a prévu dans le projet de loi, mais en lui conférant les pouvoirs d'enquête tels que définis dans la loi du 18 juillet 1991 aux articles 45 et 48. Dans le cadre de sa compétence de recours, la loi instaure le Comité R en tant que contrôleur de l'autorité de sécurité.
  Ainsi, le Comité R pourra statuer en toute connaissance de cause dans cette matière touchant les droits les plus sensibles des particuliers comme celui relatif à la protection de la vie privée. Le Comité R, à l'instar du Conseil d'Etat, ne peut accepter de statuer à l'aveuglette.

- Le Parlement considère que le Conseil d'Etat est seul compétent pour connaître un recours introduit dans le cadre d'une décision administrative. La loi devrait régler la procédure d'accès de l'organe de recours aux renseignements classifiés ayant servi de base à la décision querellée de l'autorité de sécurité.

- Le Parlement confie la compétence de recours à une commission qui serait composée de trois magistrats retraités disposant d'un certificat de sécurité, désignés par le premier président de la Cour d'appel de Bruxelles pour une durée de cinq ans, par exemple. Cette proposition s'inspire de la loi sur la libération conditionnelle qui vient d'être votée au Parlement. Ces magistrats disposeraient des mesures d'instruction comparables à celle du Comité R dans le cadre de sa compétence de contrôle ou pourraient saisir le Service d'enquêtes du Comité R pour vérifier les données fournies par l'autorité de sécurité et les services de renseignement. La loi devrait donner au président de cette commission les pouvoirs prévus par l'article 48 de la loi du 18 juillet 1991.

CHAPITRE 2 : LES DEVOIRS DE SECRET AUXQUELS SONT TENUS LES MEMBRES DES SERVICES DE RENSEIGNEMENT

Les 23 septembre et 6 octobre 1997, les Commissions chargées du suivi parlementaire des comités P et R ont permis au Comité R de procéder à l'étude de l'avant-projet de loi relative aux habilitations de sécurité (1193 / 1 - 96 / 97).

Le 20 avril 1998, le Comité R a exprimé une série de recommandations concernant l'obligation du secret devant la commission de la Défense nationale de la Chambre des représentants chargée de l'examen du projet de loi sur les habilitations de sécurité. A cette occasion, le Comité R a recommandé l'adoption d'une législation globale relative aux *"documents, renseignements et matériels classifiés",* c'est-à-dire ceux que l'autorité peut ou doit garder secrets pour des raisons de sécurité et/ou de protection de la vie privée.

Le 29 mai 1998, le rapport fait sur ce projet de loi au nom de la commission de la Défense nationale contient en annexe une étude effectuée par le Comité R sur "*les devoirs de secret auxquels sont tenus les membres des services de renseignement*" (1193/9 - 96/97).

Des amendements déposés suite à cette étude ont eu pour effet de modifier l'intitulé et le contenu du projet de loi. Le texte adopté par la Chambre des représentants le 3 juin 1998 est devenu "*projet de loi relatif à la classification et aux habilitations de sécurité"*; il contient désormais un chapitre II intitulé "*de la classification"* (1193/11 - 96/97).

Par la suite, le Comité R a poursuivi et a adapté son étude en fonction du nouveau projet de loi transmis au Sénat (1 - 1011/1). Cette étude complétée par de nouvelles données et de nouvelles recommandations sera publiée très prochainement, à la suite du présent rapport d'activités.

TITRE II : NOS SERVICES DE RENSEIGNEMENT

DEUXIEME PARTIE : LES ENQUETES

A. A LA REQUETE DU PARLEMENT OU DES MINISTRES

RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LES SERVICES DE RENSEIGNEMENT FONT LA DISTINCTION ENTRE LES ACTIVITÉS DE PARLEMENTAIRES EN TANT QUE PACIFISTES ÉCOLOGISTES ET EN TANT QUE PARLEMENTAIRES

1. PROCEDURE

En date du 9 mai 1997, le président de la Chambre des représentants a transmis à la présidente du Comité R la demande d'enquête de Monsieur O. Deleuze, qui souhaite savoir de quelle manière les services de renseignement militaires font pratiquement la distinction entre les activités de parlementaires en tant que pacifistes écologistes et en tant que parlementaires.

Le 15 mai 1997, le Comité R a ouvert cette enquête à la demande du parlement et a décidé d'élargir, d'initiative, l'enquête aux activités de la Sûreté de l'Etat à ce sujet.

Conformément à l'article 46 § 3 du Règlement d'ordre intérieur du Comité R, Messieurs les Présidents de la Chambre des représentants et du Sénat ont été informés de l'ouverture de l'enquête par lettre du 21 mai 1997.

Le 29 mai 1997, le chef du Service d'enquêtes a informé les ministres de la Justice et de la Défense nationale de l'ouverture de l'enquête en application de l'article 43 § 1 de la loi du 18 juillet 1997.

Le 22 mai 1997, le Comité a transmis la question à l'administrateur général de la Sûreté de l'Etat et au général dirigeant le SGR. Le Comité a adressé au Service d'enquêtes deux apostilles, l'une le 13 juin 1997 et l'autre le 7 octobre 1997.

Le 19 mars 1998, le rapport d'enquête a été approuvé par le Comité R.

Au terme du rapport d'enquêtes, un échange de vue a eu lieu à la demande du ministre de la Défense nationale.

Le Comité R a tenu compte des remarques des ministres de la Défense nationale et de la Justice pour la publication du rapport.

2. QUESTIONS ET RÉPONSES PARLEMENTAIRES

Le Comité R a procédé au recensement des questions parlementaires posées sur le sujet depuis 1985 et a examiné les réponses ministérielles qui y ont été apportées.

2.1. Sénat

- Le 12 octobre 1995 - Interpellation du ministre de la Défense nationale par Monsieur Coveliers (VLD) sur les pratiques de la “Sûreté militaire”.

  Réponse : le service de sécurité militaire s’intéresse aux mouvements pour la paix mais aussi aux mouvements écologistes dans la mesure où ceux-ci peuvent entreprendre des actions contre des installations militaires, par exemple : les actions de l’organisation Greenpaece contre des installations militaires à Zeebrugge.

- Question n° 18 de Monsieur Boutmans du 11 janvier 1996 au ministre de la Défense nationale - Communication de renseignements par la gendarmerie à la Sécurité militaire Greenpeace.

- Question n° 19 de Monsieur Boutmans du 11 janvier 1996 au ministre de la Défense nationale - Sécurité militaire - Greenpeace.

  Réponse valable aussi pour la question précédente : lorsque les campagnes de ce mouvement contiennent des éléments concrets en rapport avec de futures actions, elles sont analysées pour évaluer les risques de sécurité pour les installations militaires.

- Question n° 88 de Monsieur Boutmans du 11 janvier 1996 au ministre de la Justice - Sûreté de l’Etat - liste des sujets.

2.2. Chambre

- Question orale de Monsieur Deleuze (ECOLO) au Vice-Premier ministre et ministre de la Justice en date du 19 décembre 1985 (Annales parlementaires séance plénière du jeudi 19 décembre 1985).

  Réponse : ”... aucun membre des deux assemblées ne fait l’objet d’une surveillance de la part de la Sûreté de l’Etat”.
  Cependant, lorsque des manifestations publiques ou des associations font l’objet d’informations de la part de la Sûreté de l’Etat et que s’y rencontrent des parlementaires, il est évident que les rapports d’information le mentionnent, sans plus.”

- Questions n° 44 et 45 de Monsieur Van Dienderen (AGALEV) du 18 mars 1988 au ministre de la Défense nationale - Service de sécurité militaire informations sur le mouvement pacifiste.

  Réponse : le mouvement de la paix n'est pas considéré comme une menace contre l'Etat par le service de sécurité militaire qui ne s'informe que sur les organisations et les personnes qui peuvent nuire à la sécurité militaire ; il existe des dossiers traitant du maintien de l'ordre public qui ne contiennent pas de données sur les personnes ou groupements. Les militants pacifistes ne sont considérés comme une menace que s'ils sont en infraction avec la loi en matière de protection des installations et du personnel.

- Question de Monsieur De Meyer M. (SP) du 18 avril 1988 au ministre de la Justice - Sûreté de l'Etat - Renseignements sur le mouvement pacifiste, demeurée sans réponse à la connaissance du Comité R.

- Question n° 35 de Monsieur Van Dienderen (AGALEV) du 16 août 1988 au ministre de la Défense nationale - Service de sécurité militaire informations sur le mouvement pacifiste. Même réponse que pour les questions 44 et 45 mentionnées ci-dessus.

- Question n° 457 de Monsieur Vanden Eynde (Vl. Bl.) au ministre de la Justice.

  Réponse : Ce service n'établit pas de dossiers personnels en raison d'activités parlementaires et n'effectue pas d'enquêtes concernant des actes commis dans l'exercice d'un mandat parlementaire.

- Question n° 365 de Monsieur Van Dienderen (AGALEV) du 27 septembre 1996 au ministre de la Justice - Service de renseignements militaire SGR - Collecte d'informations sur les militants pacifistes.
  Le ministre a répondu que "la Sûreté de l'Etat ne s'intéresse pas aux organisations pacifistes."

  Réponse : La Sûreté de l'Etat ne s'intéresse pas aux organisations pacifistes ; elle ne constitue pas de dossiers relatifs à des objecteurs de conscience ; seuls des groupements extrémistes retiennent son attention sur le plan idéologique, par exemple : les publications de l'association "Forum voor vredesactie" et les actions qu'elle a entreprises à Kleine Brogel en décembre 1995.

- Question n° 214 de Monsieur Van Dienderen (AGALEV) au ministre de la Défense nationale du 28 novembre 1996 identique à celle du 27 septembre 1996.

Réponse : "Selon aucune des acceptations du mot, le SGR ne "contrôle" le 'Forum voor vredesactie",

Le "Forume voor vredesactie" s'intéresse de manière évidente à la Défense nationale, Il en résulte que le SGR analyse les publications de cette organisation qui, régulièrement, consacrent leurs pages à l'armée et à la défense.

Par voie des sources ouvertes disponibles, le SGR récolte des informations sur les actions éventuelles que pourraient préparer cette organisation contre des installations militaires, Dans certains cas, ces actions sont suivies par le SGR, comme à Kleine Brogel en décembre 1995. Ces activités relèvent de façon évidente de la compétence du SGR.

Pour l'armée, les activités préoccupantes sont celles qui peuvent présenter une certaine menace pour le personnel, le matériel ou l'infrastructure de Forces armées.
Le SGR a des dossiers sur des personnes, membres ou non de mouvements pacifistes, qui se sont fait remarquer par leurs actions contre l'infrastructure militaire.
Le plan de défense du territoire (DMT) ne prévoit aucune mesure spécifique à l'égard de mouvements pacifistes particuliers.
Le SGR n'ouvre pas de dossiers sur des personnes qui possèdent le statut d'objecteur de conscience en raison uniquement de la possession de ce statut,
Toutes les organisations pacifistes qui s'intéressent à l'armée ainsi que leurs publications retiennent l'attention du SGR."

Le Comité R n'a pas connaissance de questions parlementaires relatives à la surveillance éventuelle de parlementaires par le SGR.

3. SYNTHÈSE DE L'ENQUÊTE

Le Comité R a transmis la question posée par Monsieur Deleuze aux responsables des deux services de renseignement le 22 mai 1997 en les priant de bien vouloir transmettre leurs réponses.

3.1. Réponse des responsables des deux services de renseignement

Le SGR

Le 23 juin 1997, le chef du SGR a transmis une lettre au Comité R dont la teneur est la suivante: *"In antwoord op Uw in referte vermeld schrijven kan ik, na raadpleging van de betrokken sectie (i.c. SGR/CI), mededelen dat SGR geen inlichtingen verzamelt met betrekking tot de parlementaire activiteiten van leden van ecologische en pacifistische organisaties.*

Genoemde sectie verzamelt, door middel van open bronnen, enerzijds inlichtingen in het kader van de algemene studie van de ecologische en de pacifistische beweging en anderzijds met betrekking tot acties tegen de Strijdkrachten die eventueel door organisaties in dit kader ondernomen worden."

La Sûreté de l'Etat

Le 5 juin 1997, l'Administrateur de la Sûreté de l'Etat a répondu de la manière suivante :

"En réponse à votre lettre du 22 mai 1997, j'ai l'honneur de vous faire savoir que la Sûreté de l'Etat n'est pas amenée, comme vous l'indiquez, à faire "la distinction entre les activités de parlementaires en tant que pacifistes écologiques et en tant que parlementaires".
La Sûreté de l'Etat ne constitue en effet pas de dossiers sur des membres de groupes pacifistes ou écologistes.

Je me réfère à ce sujet à la réponse à la question parlementaire n° 365 du Député H. Van Dienderen du 27/09/1996, parue dans le Bulletin des Questions et Réponses n° 64 du 06/01/1997."

3.2. Les listes, notes et directives des services de renseignement

Le SGR et la Sûreté de l'Etat établissent périodiquement la liste des mouvements et organisations qu'ils surveillent; ces listes sont appelées "listes des sujets". Le Comité R a procédé l'examen des documents suivants dont il est en possession en application de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Au SGR

La "liste des mouvements suivis" d'octobre 1996 ne mentionne pas les activités des "pacifistes écologistes".

Il n'existe pas de directives relatives à la problématique telle qu'évoquée par Monsieur Deleuze.

Toutefois la liste des mouvements suivis (octobre 1996) fait apparaître le pacifisme et le fondamentalisme écologique.

Interrogé par le Comité R le 21 novembre 1997, sur la définition de ces appelations, le général dirigeant le SGR a répondu le 19 décembre 1997. Ce document peut être résumé de la façon suivante.

Les concepts de pacificisme et de fondamentalisme écologique ne sont pris en considération par le bureau Subversion de la section SGR/CI que lorsqu'ils représentent une menace pour l'armée en général, pour son personnel et ses installations en particulier.

Abstraction faite d'incidents qui se situent dans ce cadre, la collecte d'informations au sujet de ces mouvements se fait uniquement à l'aide de sources ouvertes.

A la Sûreté de l'Etat

La "liste des sujets et des mots clefs" de la Sûreté de l'Etat du 14 octobre 1996 ne reprend ni les "pacifistes écologistes", ni les partis ECOLO et AGALEV. Aucune note de service n'est donc relative à cette problématique.

3.3. Etude des dossiers des parlementaires écologistes détenus par les services de renseignement

Le 13 juin 1997, le Comité R a prié le Service d'enquêtes d'examiner auprès des services de renseignement si des dossiers existaient au nom des parlementaires actuels des partis ECOLO et AGALEV et, dans l'affirmative, d'en faire un résumé.

Le 18 juillet 1997, le Service d'enquêtes a transmis le dossier d'enquête à la présidente du Comité R, conformément à la procédure en cours au Comité R.

Au SGR

Il ressort de cette étude que :

Sur les quinze parlementaires actuels affiliés aux partis ECOLO et AGALEV, dix sont titulaires d'un dossier individuel auprès de ce service de renseignement.

Parmi ces dix dossiers :

- sept ont été ouverts avant l'élection de leurs titulaires à un mandat parlementaire; ils contiennent des pièces provenant de sources ouvertes à une exception près;

- trois ont été ouverts après l'élection de leurs titulaires à un mandat parlementaire; ils ne contiennent que des pièces tirées de sources ouvertes (articles de presse, extraits du Moniteur belge) relatives à des prises de position antimilitaristes et antinucléaires des intéressés.

Aucun dossier ne porte sur l'activité parlementaire proprement dite des intéressés (questions parlementaires, interpellations, dépôt de propositions de loi).

Les dossiers consultés ne contiennent pas d'inventaire de leur contenu; les pièces sont classées par ordre chronologique mais elles ne sont pas cotées.

A la Sûreté de l'Etat

Sur les quinze parlementaires écologistes, huit d'entre eux ont un dossier à la Sûreté de l'Etat. Chacun des huit dossiers a été examiné par le Service d'enquêtes.

Il ressort de cette étude que :

Sept de ces dossiers ont été ouverts avant l'élection de leurs titulaires à un mandat parlementaire; ils relatent diverses activités publiques de ces personnes au sein de certains mouvements (autres qu'ECOLO et AGALEV) connus de la Sûreté de l'Etat.

Un dossier a été ouvert en concomitance avec l'élection de son titulaire mais son contenu a trait à des faits et prises de position de l'intéressé en dehors de l'enceinte parlementaire.

Aucune pièce de ces dossiers n'est postérieure à 1991 et sauf une exception (1) , aucune d'elles ne porte sur l'activité parlementaire proprement dite des intéressés.

Les dossiers ne contiennent pas d'inventaire; les pièces sont classées par ordre chronologique et elles sont cotées.

3.4. Surveillance, interventions et autres suivis des activités des parlementaires écologistes par les services de renseignement

Le Comité R a adressé une nouvelle apostille au Service d'enquêtes le 7 octobre 1997 qui avait pour but de vérifier si les activités des parlementaires font l'objet de surveillances, d'interventions... ou autres suivis de la part des services de renseignement.

Des investigations menées par le Service d'enquêtes du Comité R tant auprès de la Sûreté de l'Etat qu'auprès du SGR, il ressort que les activités des parlementaires écologistes ne font l'objet d'aucune attention particulière de la part des services de renseignement.

(1) Il s'agit d'une question parlementaire que le titulaire du dossier a posé sur la Sûreté de l'Etat et à laquelle ce service a été chargé de proposer un projet de réponse au ministre de la Justice.

En effet, la majorité des dossiers individuels ouverts au nom des actuels parlementaires du parti ECOLO ou AGALEV ont été ouverts par les services de renseignement antérieurement à leur élection à l'une ou l'autre assemblée et pour d'autres raisons que leur adhésion spécifique au parti ECOLO ou AGALEV.

Des vérifications menées au SGR il ressort que :

Aucun dossier spécifique n'est tenu au nom de ECOLO ou AGALEV.

Les dossiers des quinze parlementaires ECOLO/AGALEV, ne contiennent aucune pièce attestant d'un suivi éventuel par le SGR.

A la Sûreté de l'Etat

Il existe bien un dossier au nom d'ECOLO/AGALEV qui se compose essentiellement d'articles de presse relatifs aux activités déployées par ces groupes, mais le dernier rapport date de 1988.

Huit parlementaires des partis ECOLO ou AGALEV sont connus de ce service et ont un dossier individuel mais comme précisé ci-dessus pour des activités publiques non spécifiquement liées à leur activité au sein des groupes ECOLO/AGALEV.

D'autre part le Service d'enquêtes a pu constater qu'aucune pièce relevée dans les divers dossiers individuels n'est postérieure à 1991.

4. CONCLUSIONS

Les quinze parlementaires écologistes ne sont pas tous titulaires de dossiers individuels ouverts auprès des deux services de renseignement.

La Sûreté de l'Etat a constitué huit dossiers sur ces parlementaires écologistes tandis que le SGR en possède dix.

Le Service d'enquêtes a pu constater qu'aucune pièce des dossiers individuels détenus par les deux services de renseignement n'est postérieure à 1991.

Les pièces concernant des informations recueillies depuis le mandat parlementaire exercé par les intéressés, proviennent toutes de sources ouvertes, à une exception près au SGR.

Il existe bien un dossier à la Sûreté de l'Etat ouvert au nom d'ECOLO/AGALEV qui se compose essentiellement d'articles de presse relatifs aux activités déployées par ces groupes, mais le dernier rapport date de 1988.

Au SGR, aucun dossier spécifique n'est tenu au nom des partis ECOLO et AGALEV.

A la Sûreté de l’Etat, toutes les pièces des dossiers sont cotées. Les dossiers ne contiennent pas d’inventaire.

Au SGR, aucune pièce des dossiers n’est cotée. Il n’y a pas d’inventaire de ces pièces, elles sont classées par ordre chronologique.

Depuis 1988, ni la Sûreté de l’Etat, ni le SGR ne surveillent ni ne suivent spécifiquement et particulièrement les activités des parlementaires écologistes.

B. A L'INITIATIVE DU COMITE

CHAPITRE 1 : UNE NOUVELLE MISSION DE LA SÛRETÉ DE L'ETAT : LA PROTECTION DU POTENTIEL SCIENTIFIQUE OU ÉCONOMIQUE

1. PROCÉDURE

Le 11 octobre 1996, le président du Sénat a transmis en sa qualité de président des commissions chargées du suivi parlementaire des Comités P et R, une demande de ladite commission de mener une enquête au sujet de la question orale posée par le sénateur CEDER au ministre des Affaires étrangères le 9 novembre 1995[(1)].

Le 21 octobre 1996, le Comité R a ouvert l'enquête sur base de la demande du sénateur CEDER relative aux activités du service de renseignement militaire dans les universités et l'a élargie à la manière dont les deux services participent éventuellement à la protection des données scientifiques de haute technologie dans ce milieu.

Deux membres du Comité R ont été chargés de suivre cette enquête et de faire régulièrement rapport au Comité R de son déroulement.

Le 24 octobre 1996, le chef du Service d'enquêtes a informé les ministres de la Justice et de la Défense nationale de l'ouverture de l'enquête, conformément à l'article 43 § 1 de la loi du 18 juillet 1991.

Le 28 octobre 1996, le greffier du Comité R a averti les présidents de la Chambre et du Sénat de l'ouverture de cette enquête, en application de l'article 32 de la loi du 18 juillet 1991.

Le 12 novembre 1997, le Comité R a adressé une lettre à toutes les universités du Royaume tendant à leur demander s'ils pouvaient contribuer à donner une définition des données de haute technologie.

Le 21 novembre 1997, le Comité R s'est adressé au ministre de la Politique scientifique pour lui demander sa définition des éléments essentiels du potentiel scientifique.

Le 8 janvier 1998, le Comité R a décidé de classer sans suite l'enquête relative à la question posée par le sénateur CEDER en application de l'article 63 alinéa 1 (point 2) du règlement d'ordre intérieur qui stipule : *"le Comité R peut notamment décider de classer sans suite pour les raisons suivantes : -(...) refuse de prêter son concours ou (...)"*.

(1) Sénat de Belgique - Annales parlementaires - séance du jeudi 9 novembre 1995, p.179

A la même date le Comité R a pris la décision de reformuler le deuxième volet de cette enquête comme suit : une nouvelle mission de la Sûreté de l'Etat : la protection du potentiel scientifique ou économique.

Le 27 janvier 1998 les présidents de la Chambre et du Sénat et le sénateur CEDER ont été avertis de la décision du Comité R du 8 janvier 1998.

Le 28 janvier 1998, les ministres de la Justice et de la Défense nationale ont été informés par la présidente du Comité R de la décision du 8 janvier 1998.

Les 24 et 25 février 1998, un membre du Comité R a assisté à un colloque sur cette problématique à Paris, afin de compléter la documentation du Comité R au sujet de cette enquête. Il est fait rapport de cette visite au titre III du rapport annuel d'activités 1998 du Comité R.

Le rapport d'enquêtes a été approuvé par le Comité R le 9 juillet 1998 et transmis aux ministres compétents.

Ni le ministre de la Justice ni le ministre de la Défense nationale ont fait d'objection quant à la publication de ce rapport.

Le ministre de la Défense nationale a cependant regretté : "*eu égard au point de départ de cette enquête, qu'une attention plus grande n'ait été accordée aux activités du SGR concernant les mesures de protection industrielle, lesquelles ont été consacrées par l'article 11 du projet de loi organique des services de renseignement et de sécurité tel qu'il a été adopté en séance plénière du Sénat le 16 juillet dernier. J'attire en particulier l'attention du Comité sur les activités organisées par le SGR dans le domaine de la sensibilisation des officiers de sécurité des firmes qui bénéficient d'habilitations de sécurité, du contrôle des mesures exigées et du contrôle en cas d'incidents de sécurité."*

2. INTÉRÊT PARLEMENTAIRE POUR LA PROBLÉMATIQUE

Ni le gouvernement dans l'avant projet de loi sur les services de renseignement, ni le Parlement n'ont défini cette nouvelle mission, à l'occasion du dépôt puis des discussions à la Chambre et au Sénat du projet de loi organique des services de renseignement. Le projet actuel laisse la définition de cette nouvelle mission au Comité ministériel du renseignement et de la sécurité.

L'amendement déposé par MM. Van Erps et De Crem proposant de remplacer les mots "*ou le potentiel scientifique ou économique* " par les mots *"le potentiel scientifique ou économique ou tout autre intérêt fondamental"* a été adopté par les commissions de la chambre chargées d'étudier le projet de loi.

Par contre, l'amendement proposé par MM. Delathouwer et Cuyt visant à compléter le §4 deuxième alinéa de l'article 9 du projet de loi n'a pas été adopté. Cet amendement tendait à compléter ce texte par ce qui suit : *"les mesures de protection industrielle ne seront prévues qu'à la demande des maîtres de l'ouvrage".*

D'autre part, Monsieur Borginon s'est demandé, lors de l'audition des membres du Comité R devant les commissions réunies de la Justice et de la Défense nationale de la Chambre *"si un service aussi particulier que la Sûreté de l'Etat doit se charger de collecter des données d'ordre économique, alors même que les méthodes utilisées en général dans ce secteur ne sont pas punissables. Pourquoi une telle extension des compétences de la Sûreté ?".*[(2)]

Il n'en demeure pas moins que certains parlementaires ont abordé des sujets se référant de près ou de loin au potentiel scientifique ou économique de la Belgique :

- Question n° 47 de Monsieur R. Denison (PS) en date du 31 janvier 1986 au sujet du coût de l'investissement de l'aléseuse-fraiseuse Pégard, matériel de haute technologie utilisée par l'armée.

- Question n° 186 posée par Monsieur C. Eerdekens (PS) le 28 juillet 1987 au ministre de la Défense nationale au sujet de la même aléseuse-fraiseuse Pégard placée à l'arsenal de Rocourt.

- Question n° 266 posée par Monsieur H. De Croo (PVV) en date du 19 mars 1991 concernant la liste Cocom des biens dont l'exportation est interdite parce qu'elle comportait du matériel sensible et de haute technologie et concernant la fourniture par les Etats-Unis du matériel informatique sophistiqué à l'Union soviétique qui fournira à son tour aux Etats-Unis un réacteur nucléaire de haut niveau technologique, connu sous le nom de Topaz-2.

3. LA PROBLÉMATIQUE

Le projet de loi sur les services de renseignement attribue à la Sûreté de l'Etat une nouvelle mission en son article 7§ 1er 3° et § 3. En effet cet article stipule :

La Sûreté de l'Etat a pour missions :

1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, ou le potentiel scientifique ou économique du pays défini par le Comité ministériel.

3° "le potentiel scientifique ou économique du pays" : la sauvegarde des éléments essentiels du potentiel scientifique ou économique déterminés par le Comité ministériel contre toute menace d'atteinte grave par des moyens illicites, trompeurs ou clandestins.

(2) Doc. Parl.- Chambre des Représentants - Session ordinaire 1996-1997 - 8 octobre 1997-638/14-95/96, p. 76

§ 3. A la requête de la Sûreté de l'Etat, le Service général du renseignement et de la sécurité prête son concours à celle-ci pour recueillir le renseignement lorsque des militaires sont impliqués dans des activités visées au § 1er , 1°.

Ce texte a été voté à la chambre puis au Sénat, qui a amendé le texte initial.
Ni les travaux préparatoires, ni le projet de loi lui-même ne définissent le concept de potentiel scientifique ou économique.
C'est la raison pour laquelle le Comité R a décidé de se pencher sur cette problématique.

3.1. Que protéger ?

De l'expérience vécue par le Service d'enquêtes du Comité R, il ressort que :

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.

Ce milieu est très difficile à protéger : il s'agit d'un monde de spécialistes qui ne perçoit pas toujours le lien entre les résultats de leur travail et un bénéfice autre que scientifique qu'on peut en tirer.

La matière est vaste et pointue et elle est incompréhensible pour les experts de la sécurité, qui ne sont pas des hommes de science. Paradoxalement, les chercheurs scientifiques, confiants envers leurs collègues, développent une attitude méfiante vis-à-vis de ces profanes du monde scientifique, qui de plus se permettent de les conseiller ou de les inviter à suivre certaines règles de sécurité.

Certaines universités se sont rendues compte qu'il fallait faire un effort pour sauvegarder leur patrimoine intellectuel; elles sont motivées notamment par le fait qu'elles tentent de commercialiser le produit de leurs recherches et qu'elles doivent disposer d'un budget non déficitaire.

Depuis tout un temps déjà, la KUL coopère avec des représentants des services de renseignement, mais il s'agit là d'une coopération occasionnelle ; par exemple, l'université signale aux services les agissements suspects de certains chercheurs ou étudiants - étrangers et les services à leur tour demandent des informations sur les chercheurs ou étudiants qui leurs sont connus pour des activités suspectes ou qui en développent.
Cette coopération n'a toutefois pas encore de base légale ou réglementaire et ne résulte de fait que de bons rapports entretenus par tel ou tel membre des services de renseignement avec tel ou tel responsable universitaire.

Dans le monde économique, les problèmes se situent sur un autre plan.
Le profit étant la motivation première des firmes, certaines d'entre-elles se sont déjà rendues compte que la perte d'un secret de fabrication entraînait inexorablement une perte d'argent.
Dans certains secteurs les dirigeants sont donc sensibles à l'aspect de la sécurité.

Certaines firmes ont pris l'habitude de protéger le fruit de leurs recherches alors que d'autres n'apprennent à le faire qu'après avoir subi les conséquences de leur négligence ou parce qu'elles y sont amenées après avoir conclu un contrat avec l'armée ou avec une firme américaine où la problématique de la sécurité est érigée en vertu cardinale.

Mais, si c'est le profit qui motive les entreprises, c'est précisément cet objectif qui constitue parfois leur talon d'Achille. Certaines firmes ont sciemment vendu leur technologie ou celle de leurs partenaires, lorsqu'elles travaillent sous licence, à des tiers qui n'auraient pas dû être en droit d'en disposer. D'autres firmes se sont fait manipuler par des acheteurs potentiels auxquels elles ont donné leur know how, au lieu de le vendre.

Certains hommes d'affaires habiles, spécialistes dans l'art de la négociation, agissent souvent en tant qu'intermédiaires. Ainsi, ils n'ont pas besoin de recruter d'espions dans les firmes, mais ils s'adressent directement aux dirigeants en leur faisant miroiter la signature de contrats extrêmement rentables. Personne ne résiste à la tentation, surtout si l'entreprise se trouve en difficulté.

Il est toutefois très difficile de protéger ces firmes contre elles-mêmes, sauf en envisageant une politique globale d'enquêtes des relations commerciales.

3.2. Comment le protéger ?

L'espionnage industriel se réalise presque toujours par le biais des relations humaines. Ceux qui désirent collecter des informations recherchent ceux qui peuvent les fournir, volontairement (idéologie, argent, jalousie, etc...) ou involontairement (chantage, naïveté, etc...). Le facteur humain constitue l'essentiel de cette problématique.
Ceux qui fournissent des informations sont rarement des "espions" au sens strict du terme (hommes de science, étudiants) et ceux qui recherchent les informations ne le sont pas toujours (certains gouvernements).

Entre les deux se situent toujours des "intermédiaires", c'est-à-dire un membre d'un service de renseignement étranger (lorsque celui qui recherche est un gouvernement) ou un spécialiste de l'espionnage industriel (lorsque celui qui recherche est un concurrent économique)**.**

La politique de protection du potentiel scientifique ou économique doit tenir compte de trois éléments :

- les demandeurs de renseignement sont dans la plupart des cas hors de portée d'une quelconque poursuite judiciaire (ex : un gouvernement étranger ou une entreprise dont le siège est à l'étranger) ;

- les fournisseurs d'informations qui ne sont pas accessibles à tout un chacun sont difficilement identifiables;

- les intermédiaires sont des professionnels formés dans l'art de la négociation et de la manipulation (hommes d'affaires ou membres d'un service de renseignement étranger).

La protection du patrimoine intellectuel et économique implique la protection des recherches. Un système de sécurité doit être installé, l'accès aux données doit être limité aux personnes ayant le "need to know" et des enquêtes de sécurité doivent être réalisées sur le personnel de la firme. Cette première partie peut être idéalement complétée par la surveillance des "intermédiaires" connus, et l'identification des "intermédiaires" moins visibles.

La mission des services de renseignement se limite actuellement aux enquêtes de sécurité, à la surveillance et à l'identification des "intermédiaires". Il serait opportun qu'ils prennent également en charge la sensibilisation du personnel à la sécurité (des cours, des réunions) et, si nécessaire, participent à l'entraînement du personnel de sécurité des entreprises.

Les décisions concernant l'accès aux données doivent être prises par les responsables des entreprises ou par les centres d'études qui sont le plus à même de déterminer qui a besoin de quels accès.

Les services de renseignement peuvent évidemment émettre des avis dans le domaine de la protection physique (niveaux de classification, système d'accès, clefs, etc...).
De même, en ce qui concerne la décision relative au dispositif de sécurité à installer et l'utilisation de ce matériel, les services de renseignement pourraient donner un avis car ils bénéficient d'une expérience dans ce domaine.

Le monde des universités - centres de recherche a une approche différente du monde des entreprises. Pour le premier, il s'agit plutôt de sensibiliser les chercheurs à la problématique de la sécurité, alors que pour le second il s'agit plutôt de protéger les entreprises contre les risques de la séduction au profit. Dans les deux cas il faut cependant se concentrer sur le facteur humain (enquêtes de sécurité, surveillances) qui est le maillon faible de la chaîne, alors que l'aspect de la protection purement physique est plus aisé à réaliser.

4. APERÇU HISTORIQUE

Dans les années 60, les industriels japonais ont envoyé des espions japonais de renseignement aux Etats-Unis et en Europe avec pour mission d'étudier les résultats des recherches scientifiques les plus rentables. Ce n'est toutefois qu'une vingtaine d'années plus tard que les services de renseignement des pays occidentaux ont commencé à réaliser que la razzia de leur patrimoine scientifique et économique entraînait chaque année une perte considérable évaluée à plusieurs milliards de dollars.

En 1963, le KGB a créé une nouvelle direction[3], intitulée le directorat T, en abrégé de "="J84 4 G,N>484" (Naouki & Techniki) (Sciences et Techniques) dont l'objectif déclaré était de rattraper le retard de l'industrie soviétique par des méthodes "spécialisées". La mission de ce directorat T consistait surtout à recueillir des informations dans les domaines suivants : recherches nucléaires et spatiales, fusées, sciences stratégiques, cybernétique, procédés industriels.

Le directorat T s'occupait de la coordination de l'espionnage scientifique, industriel et technique avec les autres départements du KGB. Il désignait aussi les scientifiques soviétiques autorisés à participer à des conférences internationales et plaçait des espions dans les groupes qui voyageaient à l'étranger. Le directorat T a connu une expansion rapide.

Au début des années septante, son quartier général se composait de quelques centaines d'officiers dont certains étaient présents dans les ambassades soviétiques des pays industrialisés. Quelques années plus tard les soviétiques ont attiré des entrepreneurs occidentaux pour qu'ils construisent des usines en Union soviétique de manière à obtenir leur know how (technologie, organisation), tout en continuant à faire de l'espionnage scientifique et industriel.

Vers le milieu des années 80, la priorité a été donnée au renseignement scientifique et technique avec un intérêt marqué pour les technologies qui ne sont pas spécifiquement militaires. Les autres pays de l'ancien bloc de l'Est devaient y participer. Cet effort visait surtout à recueillir des informations dans le domaine de la haute technologie, l'électronique, de la chimie, de la génétique, etc... en fait tous les domaines rendus plus ou moins inaccessibles suite à la création en 1949, en marge de l'OTAN, du Coordinating Committee for Multilateral Export Controls[4].

Le but de la création de ce dernier comité (COCOM) était d'empêcher, ou tout au moins de retarder, la constitution d'une industrie moderne d'armement en Union soviétique et dans les états de l'Est. Ce COCOM, qui a cessé ses activités en septembre 1994, a travaillé sous l'égide du groupe consultatif de l'alliance atlantique. L'effort de la direction du KGB (Naouki & Techniki) ne s'est cependant plus limité à l'aspect purement militaire des applications des recherches scientifiques, mais a englobé également toutes les applications industrielles.

Les officiers de renseignement qui travaillaient à l'étranger pour le directorat T appartenaient à la ligne dénommée X dans l'organigramme du KGB. Cette ligne X a pris de l'importance et comptait, en Belgique, entre 4 et 6 officiers qui pouvaient se faire aider par des officiers d'autres "lignes". En 1985 et 1986, quelques officiers de la ligne "X" furent interceptés par la Sûreté de l'Etat (Makeev et Dimitriev), déclarés, par après, persona non grata.

En avril 1992, cette ligne X a été démantelée en Belgique, lors de l'opération Glasnost, suite au transfuge de Vladimir Konoplev, chef de cette ligne X. Les déclarations de Konoplev ont donné lieu à des expulsions en France et aux Pays-Bas.

---

(3) J. BARON – "*KGB*" Amsterdam Boek B.V. p. 95

(4) *"Problèmes politiques et sociaux"* n° 64, 9 novembre 1990, "*les transferts de technologie Ouest-Est-Quel avenir pour le COCOM",* par Bertrand Warusfel.

Le responsable du SVR , nouvelle dénomination du KGB de l'époque, déclara aux journalistes que son service n'avait pas l'intention de diminuer ses activités de renseignement en Occident même si le climat politique entre l'Est et l'Ouest avait changé.
Sensibilisés par les Américains, les Européens ont commencé à prendre certaines mesures au début des années 80. C'est ainsi qu'au début de cette décennie, les services de renseignement français ont initié un système pour protéger leur patrimoine scientifique et économique.

Un réseau de quelques centaines de fonctionnaires ont reçu pour mission de veiller à ce que les fruits de la recherche scientifique et technologique française (universités, monde industriel, défense) n'aboutissent pas entre les mains de ceux qui en profiteraient sans en avoir payé le prix. Non seulement les pays du bloc de l'Est, l'Union soviétique en particulier, mais aussi d'autres pays tels que le Japon et les USA étaient visés par ces mesures de protection.

En Belgique, les services de renseignement se sont cantonnés aux implications militaires éventuelles (affaire Pégard) du transfert de haute technologie dans le strict respect des directives prescrites par le comité COCOM.
Les mesures prises par les Français ont cependant eu quelques répercussions sur l'activité des services de renseignement belges. La Direction de la Surveillance du Territoire (DST) et la Sûreté se sont concertées et les responsables français ont expliqué à leur homologues belges leurs méthodes; des possibilités ont été étudiées... .

En 1986, des pourparlers préparatoires ont eu lieu entre des représentants de la Sûreté et le Directeur général du département de la recherche scientifique du ministère des Affaires Economiques et des contacts ont été pris avec la FEB.
Une conférence a même été donnée par des membres de la Sûreté de l'Etat à quelques dizaines d'industriels. Aucune suite n'a cependant été donnée à cet effort de sensibilisation.

La Sûreté de l'Etat a limité ses activités à la problématique de prolifération des armes non conventionnelles (nucléaire, bactériologique, chimique), englobant la lutte contre le terrorisme (et accessoirement le communisme), dont quelques inspecteurs et un ou deux analystes sont toujours chargés. C'est principalement dans ce contexte et dans le cadre de certaines enquêtes concernant les "firmes mixtes" (essentiellement Belgo-Russes) que la Sûreté entretient des contacts avec des entreprises.

Par manque de personnel et de moyens, ces contacts sont toutefois sporadiques et leur objectif tend plutôt à contrôler les activités d'import-export de ces firmes et les activités particulières de certains membres de leur personnel (liens avec les nouveaux milieux maffieux) qu'à les protéger et à les sensibiliser à la problématique de la protection de leur patrimoine scientifique et économique.

Cette politique que l'on peut qualifier de passive peut être mise en parallèle avec la politique développée par le SGR au sujet des certificats de sécurité octroyés aux firmes collaborant avec le ministère de la Défense nationale; le SGR se contente également de délivrer une "clearance" à une entreprise ou à une firme sans aborder l'aspect de la protection de son patrimoine.

Après la chute du mur de Berlin, le monde a eu tendance à croire que l'espionnage industriel était quelque chose de suranné. La réalité allait brutalement démontrer le contraire dans plusieurs pays de l'Europe occidentale.

En Belgique l'affaire "Glasnost" (1992) a démontré que les services de renseignement russes ont maintenu l'existence d'un réseau de renseignement scientifique et technologique composé d'une quinzaine d'agents connus. Le démantèlement de ce réseau a été limité à une action tendant à mettre fin aux activités des espions, action restée d'ailleurs sans suite judiciaire.

5. SITUATION ACTUELLE

Depuis la chute du mur de Berlin, les pays qui faisaient partie de l'ex bloc de l'Est ont progressivement cessé leurs activités de renseignement économique en Belgique, la Russie en raison du démantèlement de son réseau en 1992 et les autres parce qu'ils n'ont nullement besoin d'une publicité négative contrariant leurs efforts à devenir membres de la CEE et de l'OTAN.

Actuellement le danger vient donc d'autres pays (Chine, Inde, Pakistan, pays arabes, etc...) ou d'organisations terroristes qui essayent de s'approprier le know how qu'ils ne savent pas obtenir grâce aux sources ouvertes ou à un prix raisonnable sur les marchés.
La menace provient également des activités de certaines organisations maffieuses qui volent dans le but unique de revendre au plus offrant et de tirer le maximum de profits de leurs opérations illicites.

A présent, l'administrateur général de la Sûreté de l'Etat prépare son service aux nouvelles missions des services de renseignement relatives à la protection du potentiel scientifique ou économique.

Ainsi, le 6 février 1998, l'administrateur général de la Sûreté de l'Etat a transmis au Comité R une note de service, suivant laquelle il décide qu'afin de préparer l'exécution de la nouvelle mission, à savoir la protection du potentiel économique ou scientifique du pays, toutes informations utiles et correspondance lui seront dorénavant transmises.

La veille soit le 5 février 1998, l'administrateur général de la Sûreté de l'Etat avait transmis au ministre des Affaires économiques une note de travail relative à la problématique. L'Administrateur de la Sûreté de l'Etat a envoyé cette note au Comité R le 23 juin 1998.
Cette note a été établie en réponse à la demande du Comité ministériel du renseignement qui avait 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'Etat qui a formulé les propositions d'actions suivantes :

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) *Déterminer et enquêter sur les menaces[5] et leurs origines par des contacts avec les secteurs visés, et organisation d'échanges d'informations.*

3) *Elargir ou adapter les recherches dans les domaines classiques [6]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.[7]*

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) *Etude des législations étrangères et des aspects juridiques liés à la matière.*

La note se poursuit en exprimant le besoin en personnel de la Sûreté de l'Etat pour réaliser cette nouvelle mission.

Une augmentation de 32 personnes pour les services administratifs et 50 personnes pour les services extérieurs est réclamée.

---

(5) 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.
Ne seraient pas inclus dans la mission de la Sûreté de l'Etat, l'espionnage industriel développé par une firme contre une autre au niveau du secteur privé national.

(6) Espionnage (politique), terrorisme, extrémisme idéologique, sectes nuisibles, crime organisé, prolifération de matières NBC, protection de personnes, nombreuses tâches de recherche et d'avis administratifs,...

(7) Une liste - non exhaustive - de départements et services concernés est jointe en annexe.

A la date du 15 juillet 1998, l'administrateur général de la Sûreté de l'Etat attend des nouvelles des ministres concernés afin de pouvoir faire face à cette nouvelle tâche.

Le Comité R a entendu l'administrateur général de la Sûreté de l'Etat le 23 juin 1998. Au cours de cet entretien, le responsable de ce service a précisé que deux problèmes devaient être résolus avant de pouvoir commencer à mener des actions :

1) Il s'agit d'un nouveau concept qui devra en tout premier lieu être défini par le Comité ministériel du renseignement et de la sécurité.

2) Le problème des moyens supplémentaires à octroyer à la Sûreté de l'Etat, sans oublier que les personnes engagées devront suivre une formation d'au moins deux ans avant de pouvoir accomplir une telle tâche.

En réponse à une question du Comité R, l'administrateur général a déclaré que son service n'était pas en relation avec le ministère des Affaires économiques pour l'application de la loi du 10 janvier 1955.

Le Comité R a interrogé les ministres de la Défense nationale et des Affaires économiques le 26 mai 1998 sur le fait de savoir si les services de renseignement les assistaient dans le cadre de leur attribution prévue par la loi du 10 janvier 1955 sur la propriété industrielle pour contrôler les conditions d'exploitation, d'inventions et de mise en oeuvre des secrets de fabrique.

Le ministre de la Défense nationale a répondu le 6 juillet 1998 que : *"... le ministre de la Défense nationale est représenté par le SGR dont la section "Sécurité militaire et industrielle" (SGR/SMI) assure la gestion des brevets* "classifiés" *conjointement avec le ministre des Affaires économiques-OPRI.*

Il s'agit en l'occurrence uniquement de la gestion des brevets et des inventions dits "classifiés" et qui à ce titre ne peuvent être divulgués conformément à la loi en question c'est-à-dire faire savoir de quels brevets il s'agit , le signaler aux Affaires économiques ainsi que le cas échéant signaler la levée du secret pour ces brevets. La section SGR/SMI assure également le contrôle des conditions d'exploitation d'inventions faisant l'objet de tels brevets lorsque cette exploitation se fait par une société industrielle installée 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 Etat étranger, dans le cadre de l'article 12 de la loi en question."

6. MONDIALISATION DE LA PROBLÉMATIQUE

Les colonnes du "Monde du renseignement" font régulièrement état de l'intelligence économique ou de la veille technologique. Celles du 5 mars 1998 (n° 330) consacrent, par

exemple, une page à la veille technologique et une autre page à l'intelligence économique. Il mentionne le rôle discret mais efficace de l'ambassadeur délégué aux investissements internationaux au ministère français de l'Economie, Jean Daniel Torjman qui vient de remettre un rapport tirant les leçons de la 28ème session du Forum économique mondial qui s'est tenu fin janvier-début février à Davos. Il voit notamment le retour en force de l'Europe dans les nouvelles technologies.

Jean Daniel Torjam relève cependant que les Etats-Unis dominent très largement le reste du monde en termes de concentrations géantes de sociétés. *"Les entreprises américaines sont les mieux placées au monde pour se placer en position gagnante dans le futur : sur les 30 entreprises mondiales classées par capitalisation, élément clef de la force de frappe financière, 20 sont américaines, 5 britanniques, 3 japonaises, et 2 suisses. La première allemande est 36ème, la première italienne 48ème, la première suédoise 57ème, la première brésilienne 66ème, la première de Hong Kong 68ème et la première française 79ème."*

Daniel Rouach dans son ouvrage consacré à cette problématique(8), relate que dans les années cinquante s'est mis en évidence la notion de flux et l'augmentation croissante du volume de connaissances au niveau mondial.

Il ajoute : *"les coûts de la recherche et de développement deviennent de plus en plus élevés: dupliquer une recherche, s'orienter vers des voies sans issue, se laisser surprendre par des concurrents n'est plus acceptable. Ceci est vrai à la fois pour les entreprises internationales, les grandes sociétés hexagonales ou même les PME."*

La France a mené son combat sur base d'une réflexion de la situation mondiale. Ainsi Daniel Rouach(9) a mis en exergue l'internationalisation des développements industriels et l'apparition de menaces "géographiquement" délocalisées. *"Par exemple si nous craignons particu-lièrement l'attitude dynamique du Japon, celui-ci craint à son tour le développement des potentiels scientifiques et techniques, technologiques et technico-économiques des little dragoons : Corée, Taiwan, Singapour, Hong-Kong..."*
..."Si, au Japon, la démarche de l'intelligence économique qui s'est imposée progressivement, repose sur une étroite synergie entre les sphères politique, étatique, semi-publique et privée et concerne toutes les fonctions vitales de l'économie, d'autres pays comme l'Allemagne ont pris l'habitude d'utiliser l'information concurrentielle pour systématiquement planifier leurs objectifs stratégiques."

Toutefois, cet auteur spécialisé dans ce domaine, estime que les entreprises françaises restent faibles sur le terrain de la veille technologique et économique, notamment les PME. Le partage de l'information entre sociétés spécialement au niveau international est encore exceptionnel.

---

(8) *"La veille technologique et l'intelligence économique",* Presses universitaires de France - 1996 Collection "*Que sais-je ?*"

(9) Op. Cit. p. 13.

Le Canada, comme nous le verrons plus tard, [10] a également étudié la problématique au niveau mondial.

7. LA NÉCESSAIRE COLLABORATION ENTRE ACTEURS PUBLICS ET PRIVÉS

Le rôle des acteurs publics reste essentiel dans le domaine de la défense du patrimoine scientifique ou économique. Rappelons que deux ministres sont responsables des activités de renseignement : le ministre de la Justice (Sûreté de l'Etat) et celui de la Défense nationale (SGR). Jusqu'à présent les acteurs publics belges ne se sont pas beaucoup préoccupés de cette matière pourtant essentielle pour l'avenir de la Belgique.

D'après une lettre de l'administrateur général de la Sûreté de l'Etat le 11 février 1998, en réponse à la question qui lui était posée par le Comité R, "*A l'initiative des ministres de la Justice et de l'Intérieur, la Sûreté de l'Etat a participé à une concertation entre divers services d'une part et la Fédération belge des Entreprises (FEB) d'autre part.*"

Le secteur privé a récemment réalisé l'importance de la problématique. Fin 1994, la FEB et ses fédérations membres ont décidé de créer une plate-forme de concertation pour la protection des entreprises (PCPE). Ce groupe est composé de spécialistes en matière de "security". Sur base du travail du PCPE, la FEB a adressé en juillet 1995 au Premier ministre un mémorandum plaidant en faveur d'une collaboration constructive entre les pouvoirs publics et les entreprises dans tous les domaines touchant la problématique de la protection des entreprises.

La demande du groupe est la suivante :

"1) que les pouvoirs publics reconnaissent la PCPE comme interlocuteur représentatif en ce qui concerne les activités malveillantes contre les entreprises;

2) que les autorités judiciaires et de police accordent la collaboration constructive nécessaire à la réalisation d'une concertation efficace entre leurs services et la PCPE;

3) que le personnel dirigeant des instances judiciaires et de police puisse disposer d'une formation de criminalité dont les entreprises sont victimes;

4) que le législateur consulte la PCPE lors de la conception des projets de loi ou arrêtés royaux ayant directement ou indirectement un impact sur les questions de protection des entreprises;

---

[10] Cfr. Point 8 de ce rapport : Approche d'une définition

5) *que la politique de poursuite, liée aux aspects de criminalité dans ou contre les entreprises, soit coordonnée au plus haut niveau."*

L'aspect sécurité dans le domaine de la criminalité était donc la principale préoccupation de la PCPE.

"Cet appel (appel de la FEB au Premier ministre dont question ci-dessus) *a favorablement été accueilli puisque les ministres de l'Intérieur et de la Justice, en personne, nous ont conviés à une réunion de concertation le 21 mars 1996 en présence de toutes les parties concernées : Police du Royaume, Gendarmerie, Collège des Procureurs généraux, les Magistrats nationaux, la Sûreté de l'Etat, etc... (selon Stefan De Clerck "in tempore non suspectu" une primeur en Belgique !!).*
Divers groupes de travail ont ensuite été mis en place, plus particulièrement "criminalité avec violence ", "criminalité économique" et "recherche".

En janvier 1997, les rapports de ces groupes ont été présentés aux Ministres lors d'une seconde séance plénière avec les mêmes interlocuteurs qu'en mars 1996.
Il a été convenu de mettre en place une structure de gestion mixte, sous statut ASBL pour gérer les fonds (50% pouvoirs publics, 50% secteur privé) permettant de financer les projets de recherche.
Les statuts ont été préparés mais l'affaire "Dutroux" et la réorganisation des services de police ont constitué un "trouble-fête".
Les Cabinets de l'Intérieur et de la Justice nous annoncent maintenant une relance du projet après Pâques 1998."

La Plate-Forme de Concertation "Protection des Entreprises" (PCPE), interne à la FEB organise des réunions de contacts avec diverses instances, dont les services de renseignement.

Lors de sa visite à la PCPE le 19 juin 1998, le Comité R a rappelé qu'en matière de potentiel scientifique ou économique, dès 1947 un arrêté-loi a fixé le statut de création et de fonctionnement de centres chargés de promouvoir et de coordonner le progrès technique des diverses branches de l'économie nationale par la recherche scientifique (arrêté-loi "De Groote du 30 janvier 1947)[(11)]. Un cadre juridique a donc été créé "dans lequel peuvent s'insérer, en jouissant des avantages de la loi, les institutions ayant pour objet de promouvoir le progrès technique des diverses branches de l'activité économique du pays. Il détermine la procédure, selon laquelle l'initiative privée peut entreprendre la fondation de telles institutions en leur assurant les ressources financières prévues par la loi."

De leur côté la PCPE a exposé au membre du Comité R que les entreprises souhaitent être sensibilisées par la Sûreté de l'Etat sur les risques potentiels qu'elles encourent de manière régulière. L'administrateur de la Sûreté de l'Etat est venu leur parler des sectes mais elles désirent que des rencontres soient organisées au moins tous les six mois sur d'autres sujets plus en rapport avec leurs activités. Ces rencontres devraient notamment permettre aux entreprises et à ce service de renseignement d'échanger des informations en matière économique et scientifique de manière à regrouper ces informations destinées à protéger les entreprises belges.

---

(11) Recueil des lois et arrêtés royaux, p. 848

La France a sensibilisé les entreprises à la nécessité d'une surveillance efficace de leurs produits, surtout après le développement considérable de l'informatique.(12)

Les administrations concernées, dont fait partie le ministère des Affaires économiques détiennent une masse d'information; par exemple : le service des licences et contingents.

Cette autorité est chargée par la Belgique d'appliquer le Règlement européen. Ce service détermine la liste des produits qui peuvent être exportés aux nations considérées comme une menace pour la sécurité de l'Europe. Ce service est en relation avec la Sûreté de l'Etat depuis les années 70.

Le Comité R estime qu'une solution peut être trouvée dans la création d'un organe de concertation entre les ministres concernés et les entreprises détentrices d'un potentiel scientifique ou économique vital pour la Belgique.

Dans ces perspectives, il paraît opportun d'examiner notamment l'expérience des services de renseignement français qui sont déjà actifs dans le domaine depuis plus de dix ans.
Le Comité pour la compétitivité et la sécurité économique a été créé en 1995.
Ce Comité dépend de la Direction des Relations Economiques Extérieures du ministère de l'Economie et des Finances. Il est chargé de donner des avis sur les activités d'intelligence économique.

Son fonctionnement est assuré par trois organes :

- un conseil de haut niveau sous l'égide du Premier ministre réunissant des industriels ;

- le Comité de pilotage économie et défense où le Secrétariat Général de la Défense nationale est présent (boulevard de la Tour Maubourg 75700 Paris 07 SP tél. 33.1.44018080.90 - fax : 44.18.18.80.90) ;

- un groupe de travail interministériel auquel participe le centre de documentation pour l'intelligence économique.

Toutefois, il est d'ores et déjà important de noter que le Comité pour la compétitivité et la sécurité économique belge et la Sûreté de l'Etat seront nécessairement amenés à développer en la matière une politique différente du modèle français :

- ce Comité et la Sûreté seront dans ce domaine confrontés à tout ce qui résulte de la fédéralisation de la Belgique et des compétences économiques des régions ayant des intérêts qui ne sont pas nécessairement convergents;

- la tâche de ce Comité et de la Sûreté sera compliquée par le fait que la politique scientifique du pays n'est plus du ressort unique du gouvernement fédéral.

---

(12) D. ROUACH "La veille technologique et l'intelligence économique" ,
" Presses universitaires de France, 1996 p. 65 - collection "Que sais-je ?

D’autres expériences comme celles des Allemands, des Hollandais et des Britanniques sont tout aussi intéressantes. Elles sont évoquées dans le chapitre qui suit.

8. APPROCHE D’UNE DÉFINITION

8.1. Le Canada

Les questions de sécurité économique ont été définies par le gouvernement canadien comme l’ensemble des “conditions nécessaires pour maintenir la position concurrentielle internationale du Canada, pour fournir des emplois productifs et pour lutter contre l’inflation”(13) .

Le rapport du Comité de Surveillance des Activités de Renseignement de Sécurité (CSARS), relate que le service canadien (SCRS) a adopté en 1991 une approche globale face à deux questions : la sécurité économique et la prolifération des armes de destruction massive. Pour coordonner le travail de ses sections déjà lancées dans des enquêtes en ces domaines, le SCRS a constitué la sous section des exigences -transferts de technologies (ETT).
En 1993, le SCRS a commencé à exécuter sa mission de protection du potentiel économique.

Le programme existe depuis six ans et l’examen du CSARS montre que la principale difficulté que rencontre le Service pour l’exécution de sa mission, gît dans la définition, trop générale, de ce que représente une menace économique.

En effet, il s’agit d’une vision politico-économique très large qui met l’accent sur les intérêts de la nation. En analysant l’information recueillie par le service de renseignement canadien, le CSARS a conclu que le SCRS avait amassé et conservé des renseignements qui n’étaient pas liés directement à des menaces contre la sécurité du Canada.

Le CSARS a également constaté qu’à l’occasion de séances d’information ou d’exposés présentés dans le cadre du programme de sensibilisation et de liaison, le SCRS recueillait parfois des informations, à caractère administratif, qui en bien des cas, n’avaient aucun lien particulier avec des menaces contre la sécurité du Canada.

Cette expérience illustre les risques que peut entraîner une définition trop large du potentiel scientifique ou économique ou même de tout autre intérêt fondamental du pays.

(13) Rapport annuel du CSARS 1996-1997. p. 14

8.2. La France

Un groupe de travail constitué en 1992 par le Commissariat général au plan, en vue d'éclairer les acteurs sociaux sur l'enjeu de "l'intelligence économique", s'est accordé sur la définition suivante[14] :

"L'intelligence économique peut être définie comme l'ensemble des actions de recherche , de traitement, de diffusion et de protection de l'information utile aux différents acteurs économiques.

Ces acteurs sont conçus comme un système global destiné à inspirer la stratégie de la direction générale de l'entreprise, tout comme à informer en continu et à innerver ses différents niveaux d'exécution, afin de créer une gestion offensive et collective de l'information, qui devient une richesse principale."

Pour Henri Martre[15], *"l'intelligence économique, c'est l'information recoupée, traitée, ciblée pour pouvoir éclairer les décisions. Pour prendre des décisions économiques optimales, il faut comprendre la réalité dans laquelle elles s'appliquent. Comme dans l'impressionisme, on se sert des éléments glanés ci et là pour brosser le tableau le plus proche de la réalité".*

Pour François Renier[16] "*le concept d'intelligence économique élargit le champ des éléments de connaissance nécessaires pour des décisions lourdes, par exemple celles qui amènent à engager un nouveau programme de recherche, voire à interrompre un programme déjà en cours. "Knowledge is that you can put into", disait William James[17]*.

Et Henri Martre d'ajouter : *"C'est donc un caractère concret que revêt l'intelligence économique qui va au-delà des données sur les marchés, au-delà de l'information scientifique et technologique, de celle sur les brevets ou sur l'évolution de la réglementation et prend en charge des aspects plus vastes tels que la connaissance de l'évolution de l'état de l'art ou du contexte socio-politique et socio-culturel."*

Le renseignement économique, dénommé en France "intelligence économique", inclut pour tous les auteurs, de quelque nationalité qu'ils soient, la veille technologique.

Pour Daniel Rouach et Patrice Santi [18] l'intelligence économique intègre un ensemble de veille telles que la veille commerciale, concurrentielle, sociétale et technologique.

---

(14) Rapport du groupe présidé par Henri Martre, Documentation française, 1994.

(15) Ancien PDG de l'Aérospatiale et président du groupe de réflexion "Intelligence économique et stratégies industrielles".

(16) François RENIER (synthélabo), IIR, janvier 1995, *De la veille technologique à l'intelligence économique : l'exemple de la R&D dans l'industrie du médicament.*

(17) "Le savoir est ce que vous pouvez mettre en action."

(18) "L'effet booster de la veille sur les transferts d'innovation" Expansion Management Review du mois de juin 1997

Le Comité R a relevé les définitions les plus précises de ce dernier concept :

Pour Daniel Rouach et Patrice Santi[19] , la veille technologique c'est "*l'art de repérer, collecter, traiter, stocker des informations et des signaux pertinents (faibles, forts) qui vont irriguer l'entreprise et permettre d'en orienter le futur. Elle permet de protéger le présent et l'avenir face aux attaques de la concurrence. Elle se pratique dans la légalité et le respect des règles de déontologie."*

Pour R. Beaussier, de la société CEGELEC : la veille technologique est *"l'exploitation systématique et surtout organisée de l'information industrielle. Cette technique de veille technologique consiste à savoir écouter et regarder pour repérer toutes les innovations utiles assurant l'aide aux développements techniques indispensables à l'entreprise face à la concurrence mondiale".*

La revue *"La Recherche"* donne un caractère opérationnel à la veille technologique. La définition retenue est la suivante[20] : "*La veille technologique est le moyen pour l'entreprise de faire émerger les éléments stratégiques de la masse d'information disponible aujourd'hui. Ni espionnage industriel, ni réalisation d'un état de l'art purement spéculatif dans un domaine technique restreint, la veille est avant tout destinée à éclairer les responsables de l'entreprise dans la résolution des problèmes industriels auxquels ils sont confrontés*."

Pour Henri Dou, directeur du CRRM (Université Aix-Marseille III), "*La veille technologique qui prend en compte les aspects scientifiques, techniques, technologiques et parfois même technico-économiques, va s'insérer au niveau de l'entreprise dans un contexte plus large. En effet, les choix technologiques, la détermination des menaces, la notion d'intelligence globale est en train de voir le jour. Le déplacement des conflits sur le plan économique conduira nécessairement à la globalisation du concept de Défense. Ce qui vaut pour une Nation, est aussi nécessaire à ses entreprises. Les enjeux sont si importants que cette préoccupation s'impose déjà comme un passage indispensable à tous les niveaux du développement*."[21]

La France a opté pour une approche souple de définition de son potentiel scientifique en établissant une liste des technologies clés d'un point de vue socio-économique. Cette liste a été établie par le ministère de l'Industrie dans un ouvrage intitulé : "Les 100 technologies clés pour l'industrie française à l'horizon 2000"[22].

Le classement de ces technologies est regroupé sous les titres suivants :

1. Santé et technologie du vivant;
2. Environnement**;**
3. Transports;

---

(19) Op. cit

(20) Eric WENER et Paul DEGPOUL, "La veille technologique, un nouveau métier de l'entreprise" , *la Recherche*, n°269 - octobre 1994, vol.25, pp.1068 à 1077.

(21) CERAM, Master spécialisé en Intelligence économique, groupe CERAM, Chambre de commerce et d'industrie Nice-Côte d'Azur.

(22) Ministère de l'industrie, direction générale des stratégies industrielles, juillet 1995, pp. 193-197.

4. Matériaux;
5. Energie;
6. Bâtiment et infrastructures**;**
7. Technologies organisationnelles et d'accompagnement
8. Production, instrumentation et mesure.

Le Comité R estime qu'il serait intéressant d'établir une telle liste en Belgique, afin qu'elle serve de base de référence pour l'exécution de la mission de la Sûreté de l'Etat. On ne devra pas perdre de vue les secteurs où l'on peut s'attendre au développement de technologies de pointe. Notons qu'une telle liste a aussi été élaborée en Hollande, mais qu'elle n'est pas publiée en raison de son caractère confidentiel, comme indiqué dans le point 8.3. du présent rapport.

L'optique française de la définition de cette problématique est résolument offensive et tournée vers le secteur économique alors qu'en Belgique la mission de la Sûreté de l'Etat ne vise qu'à donner le renseignement aux ministres compétents.

8.3. La Hollande

Généralités

Les missions du BVD (homologue néerlandais de la Sûreté de l'Etat) sont définies par l'article 8 de la loi du 3 décembre 1987, portant sur les règles relatives aux services de renseignement et de sécurité.

Le BVD a pour mission de :

- 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'Etat;

- exécuter des enquêtes de sécurité;

- favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'Etat, 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, dont fait partie la protection de l'économie nationale, permet au BVD d'évoluer continuellement dans le travail qu'il effectue. Il existe peu de sujets définitifs et continus; le service préfère s'adapter à la situation telle qu'elle se présente.

Le BVD procède d'abord à une évaluation de chaque nouvelle mission :

- y a-t-il une menace réelle ?
- quelle en est l'importance ?
- cette menace ne peut-elle être combattue que par les activités du BVD ?

Dans le cadre de la protection du secteur du monde économique, le BVD s'occupe actuellement d'enquêtes sur des activités de services de renseignement étrangers dirigées contre les intérêts économiques des Pays-bas, d'enquêtes de sécurité et également, et ce en permanence, de la sensibilisation des chefs d'entreprises à ce type de menace.

De "economische veiligheidsbelangen":[23]

Dès sa création le BVD a rempli une tâche de sécurité dans le monde des entreprises néerlandaises. Il s'agissait particulièrement d'entreprises travaillant pour l'armée et de celles qui pourraient être victimes de sabotage. En 1994, des pourparlers d'orientation ont eu lieu entre des représentants des entreprises et du ministère des Affaires économiques. Une conclusion s'est dégagée de ces réunions : l'exécution de la mission du BVD relative au domaine économique devait être reconsidérée.

Lors des discussions, il est apparu qu'il y avait une relation entre les intérêts économiques et la sécurité du pays puisque la position d'un pays sur le plan mondial est déterminée pour une grande partie par la stabilité de l'économie, la capacité innovatrice de chacune des entreprises et le fonctionnement optimal du système du marché libre. Le maintien de la force économique d'un pays contribue à la prévention des troubles sociaux et de l'extrémisme politique. Si la force économique est atteinte, la stabilité du pays, qui constitue un des piliers de la sécurité nationale, est menacée.

Le BVD a une mission spécifique dans le cadre des activités d'espionnage économique. Il peut également grâce à son expérience signaler à temps certaines formes de concurrence illicite. Sa mission porte aussi sur la découverte d'organisations criminelles internationales, travaillant de plus en plus sous couverture de firmes légales, et représentant un danger pour la vie économique.

Si dans ces trois domaines il appartient d'abord aux entreprises elles-mêmes de prendre des mesures, elles doivent pouvoir compter sur les autorités compétentes, le BVD devant s'occuper des menaces moins facilement discernables c'est-à-dire :

- lorsque les services de renseignement étrangers récoltent des données économiques essentielles concernant des firmes néerlandaises ;

---

[23] Sources: Rapports annuels 1994 et 1995 du BVD, Séance de la Deuxième Chambre du 27 août 1996 sur le rapport de la Commission de contrôle des services de renseignement et de sécurité pour les activités de 1995.

- lorsque des campagnes de presse calomnieuses sont lancées dans le but de discréditer des entreprises néerlandaises ;

- lorsque la présence de la maffia est suspectée dans la gestion d'une entreprise ayant pignon sur rue.

Si lors du début d'exécution de la mission du BVD, la priorité a été mise sur la protection des secteurs technologiques, au cours des discussions avec les entreprises, il est apparu nécessaire d'élargir cet objectif.

En effet, le BVD a constaté que les services de renseignement étrangers et la maffia s'intéressaient davantage aux données économiques ne relevant pas de la recherche et du développement scientifique. Sur base de cette constatation, un "groupe de projet" a été mis sur pied. Ce groupe a reçu pour mission d'étudier la problématique en coopération avec le ministère des Affaires économiques et des représentants des entreprises (33 entreprises néerlandaises importantes ont participé à cette étude). Ce groupe a été dénommé "Economische Veiligheidsbelangen" (Intérêts de sécurité économique) et s'est donné comme priorité la finalisation de l'analyse des risques avant la fin de l'année 1995 afin de déterminer les aspects de la protection du potentiel économique dont le BVD devait s'occuper.

Les conclusions du groupe "Economische Veiligheidsbelangen" sont les suivantes :

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 telles que des écoutes ou des informateurs pour gagner ces marchés;

3. il est indispensable de mener des enquêtes sur la fiabilité d'entreprises et d'investisseurs qui entretiennent des rapports avec le crime organisé (maffia).

Il a été décidé que les activités du BVD devaient porter sur ces trois menaces spécifiques.

En outre, la mise sur pied d'un "stuurgroep" (commission d'experts) a été prévue pour 1996. Cette commission d'experts, placée sous la direction du Secrétaire-général du ministère des Affaires économiques devait élaborer, via une collaboration interdépartementale, une définition de la problématique et un plan d'action.

Ce "stuurgroep" n'a jamais été mis sur pied. Le ministre de l'Intérieur, Monsieur Dijkstal, a souligné en août 1996 que le gouvernement avait décidé entre-temps que le BVD s'occuperait bien d'enquêtes relatives aux activités des services de renseignement étrangers dirigées contre les intérêts économiques des Pays-Bas. Il ajoutait qu'un "contactgroep" (groupe de contact) avait été créé réunissant des membres du ministère des Affaires

économiques et du BVD. Ce groupe était chargé d'analyser et d'étudier les menaces concrètes qui ne venaient pas de services de renseignement étrangers. L'analyse de ces autres menaces devaient déboucher sur des actions éventuelles du BVD. Le ministre Dijkstal estimait que la législation relative au BVD était suffisante pour que le BVD remplissent les tâches définies par le groupe "Economische Veiligheidsbelangen".

Un parlementaire, Monsieur Van Oven a demandé à l'occasion d'une interpellation(24) au ministre de l'Intérieur si la liste des entreprises présentant un intérêt vital pour les Pays-Bas serait portée à la connaissance de la Chambre. Le ministre a répondu qu'en raison de son caractère confidentiel, cette liste ne serait transmise qu'à la commission de contrôle des services de renseignement et de sécurité. Cette liste constituait le fondement légal de la protection par le BVD des entreprises désignées comme étant vitales pour l'économie néerlandaise par le ministre de l'Intérieur .

La Hollande adopte une optique défensive mais qui prévoit d'associer le monde économique au monde politique. Cette optique a une base légale. En effet, la loi hollandaise sur les services de renseignement autorise le BVD à attirer l'attention des entreprises sur les mesures de protection à prendre.

8.4. L'Allemagne

Grâce à l'obligeance d'un membre des services de renseignement allemand, le Comité R a reçu au sujet de cette problématique les informations suivantes.

En Allemagne fédérale, la protection du potentiel scientifique ou économique n'est pas réglée par la loi, c'est-à-dire dans le cadre de la protection légale des entreprises.

Il y a cependant la loi sur la concurrence déloyale (UWG - Gesetz gegen den aunlauteren Wettbewerb). A titre d'exemple, le § 17 de cette loi traite de la protection du secret industriel. Il appartient néanmoins aux entreprises elles-mêmes d'organiser la protection de leurs données sensibles.

Ainsi, le 9 novembre 1993, les industriels allemands ont chargé un organisme central de la problématique de la protection des entreprises de haute technologie, la "Arbeitsgemeinschaft für Sicherheit der Wirtschaft - ASW" *(Groupe de travail pour la sécurité industrielle)* ainsi que des "Landesverbände für Sicherheit der Wirtschaft" *(Fédérations régionales pour la sécurité industrielle)*.

La "ASW" conseille et soutient ses membres dans la protection de leurs intérêts de sécurité et requiert leur coopération pour résoudre tout problème dans le domaine de la sécurité industrielle.

C'est uniquement pour la protection, dans l'intérêt commun, des secrets d'Etat dans les domaines publics ou pour des entreprises et sociétés privées travaillant pour l'Etat qu'il existe une *"lex specialis".* Cette loi s'intitule la "Gesetz über die Voraussetzungen und das

(24) Séance de la Deuxième Chambre du 27 août 1996

Verfahren von Sicherheitsüberprüfungen des Bundes - Sicherheitsüberprüfungsgesetz - SÜG" (*Loi fédérale sur les conditions et les modalités d'exécution des enquêtes de sécurité*) du 20 avril 1994.

Cette loi, nécessaire eu égard à l'intrusion dans la vie privée inévitable lors d'une enquête de sécurité établit un règlement légal, clair et spécifique relatif aux droits, devoirs et compétences des personnes concernées dans le cadre des enquêtes de sécurité. Le BfV[25] n'est qu'une autorité exécutante. Il n'établit ni critères, ni définitions.

8.5. L'Angleterre

La législation anglaise prévoit 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)[26]. Aucune des deux lois ne définissent ce concept de bien-être économique.

Le Comité R a invité un expert en la matière puisqu'il s'agit de David Bickford, un des pères de cette législation anglaise.

Ce dernier a remis un texte au Comité R qui peut être résumé comme suit :

La signification du bien-être économique revêt une grande importance eu égard à l'article 55 de la Chartre des Nations unies, à l'article 8 de la Convention européenne de sauvegarde et des libertés fondamentales car elle permet de limiter les droits à la vie privée des particuliers mis en balance avec le bien-être économique d'un pays. Enfin les états de la Communauté économique européenne ont établi un marché commun au sein duquel la problématique est expressément prévue (articles 2 et 3 du Traité de Rome).

L'économie politique est définie comme "l'art de la gestion des ressources d'un peuple et de son gouvernement" (Adam Smith).
Cet art comporte deux éléments. Le premier est relatif à l'identification des ressources et le second concerne l'interprétation de la gestion.
Les ressources sont définies, dans le contexte macro-économique, comme les moyens collectifs que possèdent un pays pour sa propre subvention et défense. Le terme "ressources" intègre tant les personnes que les biens.

La gestion inclut tant les personnes (immigration, besoins sociaux tels que la santé, sécurité et bien-être) que les biens (ressources et développement, production, environnement, import-export, achat-vente). Ceci étant la théorie selon Adam Smith, David Bickford examine ensuite ce que font les Etats.

---

(25) BfV : Das Bundesamt für Verfassungsschutz (Office fédéral de la protection de la Constitution)

(26) Cfr; "*Etude de la législation du Royaume-Uni relative aux services de renseignement et de sécurité*", rapport annuel d'activités du Comité R 1998.

Coexistant avec les Nations unies, la Communauté Economique Européenne constitue une institution internationale de référence pour la compréhension de la nature du bien-être économique dans la communauté internationale. La Communauté économique est fondée sur la Communauté européenne du charbon et de l'acier, la Communauté européenne de l'énergie atomique et sur la Communauté économique européenne.

Le Traité de Rome reconnaît les relations étroites entre l'économie, le social et l'environnement dans la société moderne.

D'autres traités, tout aussi importants et plus récents tant européens qu'internationaux, ont érigés en droit le bien-être économique des pays européens .

La protection du bien-être économique

Les préjudices subis par le bien-être économique comme ceux causés à la sécurité sont de nature à entraîner des dommages à l'intégrité du pays.
Il en résulte que des actions doivent être menées par le politique de cet état pour soutenir ses intérêts de sécurité et de bien-être économique.

Dans cette optique, les états sont justifiés à collecter des informations au sujet du bien-être économique et des stratégies d'autres pays qui pourraient menacer son intégrité. Pour les mêmes raisons, la récolte de renseignement à l'intérieur de l'état est légitime afin de protéger les intérêts économiques vitaux du pays ainsi que sa politique.

Il n'est pas nécessaire qu'une menace se soit développée pour attendre de récolter du renseignement au sujet du bien-être économique. Il convient qu'un état s'assure d'un niveau adéquat d'information à propos de matières affectant ses intérêts économiques vitaux afin de déterminer quels intérêts, et par conséquence son intégrité, peuvent être menacés et sont susceptibles d'être préjudiciés.

De façon plus pragmatique, David Bickford a indiqué au Comité R que tant le Mi5 que le Mi6 s'intéressent aux actions venant de l'étranger étant donné que les menaces dans ce domaine viennent toujours de l'étranger; l'économie nationale dépend de son commerce international. Le concept de concurrence internationale est donc pris en compte comme au Canada.
Le spectre des recherches d'informations est donc très large.

L'importance du marché intervient dans la définition de la mission : pour prendre un exemple caricatural, ni le Mi5, ni le Mi6 ne s'intéressent à un magasin chinois car il ne représente pas une menace pour le marché britannique. Ce n'est pas le cas pour le marché du blé pour qui le marché russe peut représenter une menace. Il s'en suit que pour qu'il y ait recherche il faut que la menace ait un impact sur une partie de l'économie britannique. La recherche de renseignements est donc en relation avec les événements d'importance.

Les ministres concernés sont impliqués. Ils doivent être capables de définir 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'Etat 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.

Les services de renseignement mettent sur pied des équipes composées notamment d'avocats avant d'entamer leurs actions de manière à assurer le succès de l'opération tant sur le plan renseignement que sur le plan légal.

Commentaires

Il appert de cette brève étude que cette matière délicate est réglée de manière fondamentalement différente selon les états européens.

Les Pays-Bas, l'Angleterre et le Canada incluent cette mission dans la loi sur les services de renseignement, comme la Belgique.

Aux Pays-Bas comme en Allemagne et en France les entreprises ont pris des initiatives à des degrés divers suivant les pays.
Aux Pays-bas, en Allemagne, comme au Canada il est question de renseignement défensif, c'est-à-dire dans le cadre de la protection tandis qu'en France la problématique est abordée tant sous l'aspect offensif que sous l'aspect défensif.

Le caractère offensif se caractérise notamment par une recherche du renseignement à l'extérieur du pays afin de prendre des marchés, tandis que le caractère défensif se limite à la protection des intérêts nationaux.

En Angleterre, le renseignement est au service de l'Etat de manière offensive dans un but défensif de la sécurité de l'Etat tandis qu'en France, il s'agit d'une véritable coopération des services de renseignement avec les entreprises et dans leur intérêt.

La France a permis à ses services de s'intéresser à cette matière sans base légale.

La position de la Belgique se situe dans le contexte canadien puisque le projet de loi inclut la mission spécifique de la protection du potentiel scientifique et économique dans les compétences de la Sûreté de l'Etat en visant la protection et non la recherche offensive du renseignement.

La question se pose de savoir comment l'Europe dans le cadre de sa construction politique envisagera cette problématique et si les intérêts personnels des états ne vont pas prévaloir sur les intérêts de l'Europe économique.

9. RÉPONSES DES UNIVERSITÉS BELGES

Le Comité R a reçu le 16 février 1995 le professeur Geysen de la KUL qui a fait un exposé sur :

1. la présentation de cette université;

2. le contrôle exercé par les services de la KUL pour la protection des données de haute technologie et les droits intellectuels les accompagnant.

De la comparaison de cet exposé et des briefings donnés par les deux services de renseignement au début du fonctionnement du Comité R il apparaît que :

- les services de renseignement ne s'occupent pas de façon systématique de la protection des données scientifiques de haute technologie. Leur intervention se limite à des enquêtes occasionnelles de la Sûreté de l'Etat effectuées à la suite d'informations ponctuelles données par l'université ou des tiers. Cette carence est due à un manque de personnel et de moyens financiers.

La Belgique ne possède pas ou peu de ressources naturelles. Ses richesses sont principalement d'ordre intellectuel.

Une lettre a été adressée à toutes les universités du pays ainsi qu'au ministre de la Politique scientifique pour leur demander s'ils pouvaient donner une définition des données de haute technologie et des éléments essentiels du potentiel scientifique.

En effet, comme indiqué dans l'approche que font les français de l'intelligence économique, si la loi ne mentionne nulle part les 'données de haute technologie', il s'agit bien d'un aspect essentiel du potentiel scientifique, lequel, à son tour, ne constitue qu'une partie de la notion de "potentiel scientifique et économique".

DÉFINITION DES "DONNÉES DE HAUTE TECHNOLOGIE"

Les réponses fournies par les universités peuvent être résumées comme suit :

1. ULB

On peut qualifier de 'haute technologie' toutes les matières faisant l'objet de recherches actuelles et susceptibles d'usage extra académique.

2. NOTRE DAME DE LA PAIX DE NAMUR

Il appartient au législateur de donner une définition de 'données de haute technologie'.

3. ST. LOUIS

Pas de réponse puisque faculté de sciences humaines et donc pas du tout technologique.

4. GEMBLOUX

Toute donnée susceptible de conduire à un brevet ou de constituer un élément de ce dernier.

5. R.U.G. (Gent)

Résultats de recherches innovatrices (recherches ou procès basés sur l'application de technologies avancées nouvelles, se trouvant bien souvent elles-mêmes dans un stade de développement) qui peuvent faire l'objet de l'octroi d'un brevet.

6. VUB (Bruxelles)

Pas de réponse.

7. KUL (Leuven)

Une définition thématique, éternellement valable n'est pas indiquée en raison de l'évolution constante de ces matières.

Le fait que certains produits soient susceptibles de se voir octroyer un brevet n'est pas suffisant en lui-même pour leur octroyer un caractère de haute technologie.

Les publications, bien que sources d'informations fiables sur le caractère avancé d'une technologie, n'offrent aucune garantie quant à la validité dans le temps.

Une définition doit être basée sur un cadre de référence qui tient compte de publications, de brevets et d'une évaluation de la valeur technologique réelle par un organisme reconnu, comme par exemple "**I**nstituut ter bevordering van het **W**etenschappelijk en **T**echnologisch onderzoek in de industrie -Vlaams Technologisch Observatorium".

Dans le contexte des missions de la Sûreté de l'Etat : les nouvelles connaissances ou technologies qui peuvent en cas d'abus menacer la sécurité du citoyen ou de la communauté.
Une telle définition est plutôt utilisée en fonction d'applications possibles et non pas en fonction de la nature ou du caractère innovateur de la technologie elle-même.

8. UCL

Ces données ne font pas l'objet d'une définition sous forme synthétique mais bien par voie d'énumérations de produits ou de secteurs . La liste COCOM ou la liste UE de biens à double usage publiée au Journal officiel des Communautés européennes le 30 octobre 1996 constituent des bases permettant d'approcher le sujet. Il s'agit du "Règlement (CE) N° 3381/94 du Conseil, du 19 décembre 1994, instituant un régime communautaire de contrôle des exportations de biens à double usage". Ce règlement est d'application à partir du 1er mars 1995.

Considérations se trouvant à la base du Règlement

- Dans la réalisation du marché intérieur, la libre circulation des marchandises, y compris des biens à double usage, doit être assurée conformément aux dispositions pertinentes du traité. Actuellement les échanges intra-communautaires sont soumis à des contrôles par les Etats membres. La suppression de ces contrôles améliorera la compétitivité internationale de l'industrie européenne.

- L'objectif du Règlement est de soumettre les biens à double usage a un contrôle efficace lors de leurs exportations de la Communauté.

- Un tel contrôle est nécessaire en vue de respecter les engagements internationaux des Etats membres et de l'Union européenne, notamment en matière de non-prolifération.

- Des listes communes de biens à double usage sont des éléments essentiels d'un dispositif de contrôle efficace.

- Les décisions portant sur le contenu de ces listes sont de nature stratégique et relèvent de la compétence des Etats membres.

- Les ministres des Affaires étrangères de la Communauté ont adopté, le 20 novembre 1984, la déclaration de politique commune qui porte sur les modalités relatives aux transferts intercommunautaires de plutonium récupéré et d'uranium enrichi au-delà de 20%, ainsi qu'aux installations, aux principaux composants et à la technologie liés au retraitement, à l'enrichissement et à la production de l'eau lourde.

- L'action commune susvisée et le présent Règlement constituent un système intégré.

- Ce système représente un premier pas d'un système commun de contrôle cohérent. Dans ce contexte il est souhaitable que les procédures d'autorisation appliquées par les Etats membres soient harmonisées de façon progressive et rapide.

- Que rien dans le présent Règlement ne limite les pouvoirs conférés par le code des douanes communautaire et ses dispositions d'application. Les Etats membres devraient, lors de l'examen des conditions relatives à la réexportation ou à l'utilisation finale des biens à double usage, prendre en considération les principes pertinents du droit international.

- Il n'y a pas d'obstacle à ce que les Etats membres arrêtent ou maintiennent, dans le plein respect du marché intérieur, des mesures supplémentaires de contrôle des exportations qui soient compatibles avec les objectifs du présent Règlement.

- Pour éliminer le risque de détournement de biens à double usage pendant la phase initiale d'adaptation, il y a lieu de prévoir l'application de contrôles simplifiés aux échanges intercommunautaires de ces biens.

- Les Etats membres garderont la possibilité d'effectuer des contrôles sur des biens à double usage pour assurer l'ordre public ou la sécurité publique.

- Chaque Etat membre doit prendre des mesures pour doter les autorités compétentes des pouvoirs appropriés.

- Chaque Etat membre détermine les sanctions à appliquer en cas d'infraction aux dispositions du présent Règlement.

Le Règlement donne des définitions des termes les plus important utilisés :

'Biens à double usage': biens susceptibles d'avoir une utilisation tant civile que militaire

'*Exportation'*: le régime permettant la sortie temporaire ou définitive de marchandises communautaires (et non communautaires en cas de ré-exportation) du territoire douanier de la Communauté.

'Exportateur': toute personne physique ou morale pour le compte de laquelle est faite la déclaration d'exportation et qui est le propriétaire des biens à double usage ou qui a un droit similaire de disposition de ceux-ci en question lorsque la déclaration est acceptée.

'Autorités compétentes': les autorités chargées dans les Etats membres d'appliquer le présent règlement.

'Déclaration d'exportation': l'acte par lequel une personne manifeste, dans les formes et les modalités prescrites, sa volonté de placer un bien à double usage sous le régime douanier de l'exportation.

Pour décider de l'octroi éventuel d'une autorisation d'exportation, les autorités compétentes prennent en considération les lignes directrices communes figurant à l'annexe III de cette décision.

Annexe III

Pour décider de l'octroi éventuel d'une autorisation d'exportation, les autorités compétentes prennent en considération les éléments ci-après:

a) leurs engagements au titre d'accords internationaux en matière de non-prolifération et de contrôle de biens sensibles;

b) leurs obligations au titre des sanctions imposées par le Conseil de sécurité de l'ONU ou approuvées dans le cadre de l'Union européenne ou d'autres organisations internationales (notamment les embargos commerciaux, les embargos sur les armes et les équipements militaires ou sur les biens à double usage);

c) des considérations de politique étrangère et de sécurité nationale, y compris, le cas échéant, celles qui s'inscrivent dans le cadre des critères qu'ils ont approuvés lors des Conseils européens de Luxembourg - juin 1991, et de Lisbonne - juin 1992, en ce qui concerne les exportations d'armes conventionnelles;

d) des considérations relatives à l'usage final prévu et au risque de détournement.
Les Etats membres procéderont, le cas échéant, à un échange de vues sur ces lignes directrices, afin de les réexaminer si nécessaire.

Il est difficile de donner une définition unique des données de haute technologie mais il est plus exact de préciser que cette notion varie en fonction de l'évolution de la technologie elle-même et de choix politiques.

Le critère de définition des biens à double usage n'est pas leur appartenance à la haute technologie mais bien leur usage stratégique éventuel.

La liste de l'Union Européenne constitue la concrétisation technique des accords internationaux sur le contrôle des biens à double usage, et notamment l'arrangement de Wassenaar, le régime de contrôle de la technologie relative aux missiles, le groupe des fournisseurs d'articles nucléaires, et le "groupe Australie". Il n'a pas été tenu compte des articles que des Etats membres souhaitent placer sur une liste d'exclusion. Il n'a pas été tenu compte des contrôles nationaux (contrôles qui ne sont pas effectués au titre d'un régime) éventuellement maintenus par des Etats membres.

Le Comité R estime que sur base des “définitions” il semble logique que le concept d’une liste (COCOM -U.E.) offre en fait les meilleurs garanties pour arriver à une délimitation précise qui est de plus adaptable aux changements de la politique internationale ou dans le contexte scientifique ou social.

Il faut cependant souligner que le premier but de listes, comme celle du COCOM (passé) ou de l’U.E., n’est pas la protection du potentiel scientifique ou économique. Elles ont été conçues principalement pour éviter que certaines technologies ou certains produits ne tombent dans les mains de personnes, groupements ou nations qui sont censés pouvoir les utiliser pour menacer la sécurité du monde occidental. C’est aussi la raison pour laquelle différents produits figurant sur ces listes n’ont aucune valeur de haute technologie.

Les produits mentionnés sur la liste actuelle de l’U.E. (produits à double usage) sont soumis à des limitations d’exportation. Nonobstant la sévérité des contrôles exercés, on peut se poser la question s’il appartient à la Sûreté de l’Etat de faire, avec les moyens limités à sa disposition, un effort supplémentaire dans ce domaine en effectuant un double contrôle. La Sûreté de l’Etat s’occupe déjà de cette matière dans le cadre de la prolifération des armes nucléaires, biologiques et chimiques. Elle pourrait néanmoins utiliser cette liste en tant que cadre de référence, à côté d’autres, afin de délimiter le champ d’application de sa mission (QUOI protéger).

A la connaissance du Comité R, seul l’Instituut ter bevordering van het Wetenschappelijk en Technologisch onderzoek in de industrie a élaboré une liste des produits de haute technologie.

10. DIFFICULTÉS DE L’EXÉCUTION DE CETTE NOUVELLE MISSION POUR LA SÛRETÉ DE L’ETAT ET PROPOSITIONS

S’il entre dans les préoccupations des responsables politiques de mettre sur pied un système de protection du patrimoine scientifique ou économique du pays par les services de renseignement, comme le laisse prévoir le projet de loi sur les services de renseignement, il faudra nécessairement tenir compte de quelques paramètres dans différents domaines .

Le projet de loi prévoit que la Sûreté de l’Etat sera chargée de “rechercher, d’analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l’Etat et la pérennité de l’ordre démocratique et constitutionnel, la sûreté extérieure de l’Etat et les relations internationales, ou *le potentiel scientifique ou économique du pays défini par le Comité ministériel.* Il convient d’être conscient de la difficulté de trouver une définition qui permette une application souple de cette nouvelle mission de la Sûreté de l’Etat que le Parlement laisse au Comité ministériel du renseignement et de la sécurité.

L’exemple canadien démontre la nécessité d’un contrôle sur l’exécution de cette mission.

Il faudra prévoir que la Sûreté de l'Etat dispose de normes pour effectuer cette tâche :

- définition exacte de sa sphère de compétence;
- dispositions permettant une coopération avec les universités et les entreprises;
- dispositions légales (en projet de loi) autorisant les services à effectuer des enquêtes de sécurité sur les personnes travaillant dans les secteurs à protéger.

La question se pose de savoir si les moyens adéquats seront mis à la disposition de la Sûreté de l'Etat pour que cette mission, très importante, devienne réalité. L'exercice concret de cette mission est indissociable de la nécessité permanente de sensibiliser les entreprises et les universités à cette problématique. Elles ont leur part de responsabilité à prendre. Dans le cadre de l'exécution de cette mission, la Sûreté devra prévoir :

- la mise sur pied de l'infrastructure (organigramme : tâches - effectifs);
- l'organisation de la coopération avec les organisations ou firmes à protéger, éventuellement via le ministère des Affaires économiques par la création d'un poste spécifique (ex : officier de liaison);
- personnel;
- la formation spécialisée et suivie de son personnel;

Les autres administrations concernées (ministère des Affaires économiques, ministère de la Politique scientifique, les Régions, etc...) doivent de leur côté permettre l'exercice de cette mission.

A cet égard le Comité R suggère :

- la création d'un organe de concertation entre les ministres concernés et les entreprises détentrices d'un potentiel scientifique ou économique ou d'un intérêt vital pour la Belgique. Il faudra déterminer les compétences de cet organe de concertation, ainsi que son rôle de coordinateur entre le monde industriel, le monde scientifique et la Sûreté de l'Etat.
  Sa tâche pourrait consister notamment à favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'Etat, des secteurs, des pouvoirs publics et du monde économique et qui sont de l'avis des ministres compétents, d'un intérêt vital pour le pays.

Enfin il faudra tenir compte de l'approche psychologique particulière des différents acteurs, chercheurs et industriels, avec les spécificités propres au monde scientifique et au monde des entreprises.

11. CONCLUSIONS

Cette enquête a pour but de sensibiliser les autorités politiques à la nouvelle mission qu'ils viennent d'impartir à la Sûreté de l'Etat en la chargeant de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer (....) le potentiel scientifique ou économique du pays ... .

La définition de cette mission est laissée à l'appréciation du Comité ministériel du renseignement et de la sécurité.

Le Comité R estime que cette définition ne doit pas être ni trop large, au risque de voir ce service de renseignement confronté aux mêmes difficultés que son homologue canadien, ni trop figée étant donné que les éléments du potentiel scientifique ou économique sont évolutifs par nature et ce à grande vitesse.

La Belgique qui ne possède pas ou plus de ressources naturelles. La protection du potentiel scientifique ou économique doit se comprendre dans le cadre de la construction de l'Europe.

Le Comité R préconise, pour réaliser cet objectif, la création d'un organe de concertation entre les ministres concernés et les entreprises détentrices d'un potentiel scientifique ou économique ou d'un intérêt vital pour la Belgique .

Cet organe pourrait concevoir la liste des technologies clés d'un point de vue socio-économique en se basant sur le règlement (CE) n° 3381/94 du Conseil de l'Europe qui institue le régime communautaire de contrôle des exportations de biens à double usage, par exemple.

Le Comité R prône que cet organe de concertation serve de lieu de rencontre où la Sûreté de l'Etat sensibiliserait les entreprises et les universités aux menaces en provenance de l'étranger et qu'il serve de lieu d'échange d'informations entre les entreprises, les universités et les services de renseignement. En effet, le SGR est également confronté à cette mission puisqu'il devra au sens du projet de loi sur les services de renseignement et de sécurité prêter son concours à la Sûreté de l'Etat pour recueillir le renseignement lorsque les militaires sont impliqués dans ce type d'activités.

D'autre part, cet organe de concertation devrait pouvoir recueillir la masse d'informations que détiennent les administrations comme par exemple le service des licences et contingents au ministère des Affaires économiques.

Enfin il ne faudra pas négliger de fournir à la Sûreté de l'Etat les moyens qu'elle réclame au risque de voir cette disposition législative rester lettre morte.

CHAPITRE 2 : ENQUÊTE SUR LES COMPÉTENCES ET LE FONCTIONNEMENT DU SERVICE "LÉGISLATION EN MATIÈRE D'ARMES" DE LA SÛRETÉ DE L'ETAT

1. INTRODUCTION

Le Comité permanent R a décidé d'ouvrir une enquête relative à la compétence et au fonctionnement du service "législation en matière d'armes" afin d'apprécier si cette matière doit bien relever de l'Administration de la Sûreté de l'Etat.

2. PROCÉDURE

Le Comité R a décidé d'ouvrir cette enquête d'office le 20 novembre 1996. Deux de ses membres ont été chargés d'en suivre le déroulement et d'en faire rapport.

Le 27 novembre 1996, en application de l'article 46, alinéa 3 du règlement d'ordre intérieur, les présidents de la Chambre des représentants et du Sénat ont été informés qu'une enquête était en cours sur les compétences et sur le fonctionnement de la Sûreté de l'Etat en matière de législation sur les armes.

Le 12 décembre 1996, le Comité R a suivi un briefing concernant la législation sur les armes en Belgique.

A la demande de la présidente du Comité R, l'administrateur général de la Sûreté de l'Etat a fait parvenir le 10 mars 1997 au Comité R une note circonstanciée sur les compétences légales de son "service législation en matière d'armes" et sur les raisons de transférer cette tâche à un service de police administrative.

La présidente du Comité R a adressé une apostille au chef du Service d'enquêtes le 16 avril 1997.

Le 17 avril 1997, le greffier du Comité R a informé le chef du Service d'enquêtes que l'enquête était élargie aux deux services de renseignements et à toute la problématique de la réglementation, de la possession et de l'emploi d'armes par ces services.

Le 30 avril 1997, en application de l'article 43 alinéa 1er de la loi organique du 18 juillet 1991, le ministre de la Justice et le ministre de la Défense nationale ont été informés par le chef du Service d'enquêtes qu'une enquête était ouverte concernant les services de renseignements et la problématique de la réglementation des armes.

Les 11 septembre et 25 novembre 1997, des documents ont été demandés à la Sûreté de l'Etat. Ceux-ci ont été reçus par le Comité R le 2 décembre 1997.

Le 9 décembre 1997, le Comité R a procédé à l'audition du conseiller-adjoint qui a été responsable du service "législation en matière d'armes" de la Sûreté de l'Etat du 1er janvier 1995 au 13 octobre 1997.

Des explications complémentaires ont été demandées à l'administrateur général de la Sûreté de l'Etat par lettre du 30 décembre 1997. Ce dernier a répondu le 10 février 1998.

En exécution d'une apostille du 20 mars 1998, le service d'enquête du Comité R a procédé à une vérification auprès de la Sûreté de l'Etat pour constater la manière dont ce service alimente en informations le registre central des armes. Le rapport de cette vérification à été remis au Comité R le 27 avril 1998.

Le présent rapport a été approuvé par le Comité R le 5 mai 1998.

3. L'INTÉRÊT PARLEMENTAIRE

Le Comité R n'a recensé qu'une seule question parlementaire en rapport avec l'objet de la présente enquête. Il s'agit de la question n° 640 du député Michel Wauthier (PRL) au ministre de la Justice le 18 juillet 1997: le député questionne le ministre sur une éventuelle réforme de la législation sur les armes.

Le ministre répond qu'un projet de loi remplaçant la législation existante sur les armes, trop complexe et améliorable, est en préparation.

Ce projet s'inspire de la directive de l'Union Européenne 91/477/CEE qui fixe un certain nombre de normes minimales et qui vise à une harmonisation européenne (Chambre des représentants - session 96/97 - Questions et réponses - 22 septembre 1997 - N. 98, p. 13.292).

4. GENÈSE DE LA COMPÉTENCE DE LA SÛRETÉ DE L'ETAT EN MATIÈRE D'ARMES À FEU

4.1. Compétences de la Sûreté de l'Etat antérieure à la modification du 30 janvier 1991 de la loi du 3 janvier 1933

La compétence de la Sûreté de l'Etat en matière d'armes n'est pas récente. Déjà en 1994, l'Office des Etrangers (qui dépendait à l'époque de l'administration de la Sûreté Publique) était

compétente pour recevoir et répondre aux demandes de renseignements des commissaires de police et des Commandants de gendarmerie en ce qui concerne les demandes d'acquérir des armes à feu de défense introduites par des étrangers de passage en Belgique.

L'Office des Etrangers devait répondre de toute urgence mais n'avait aucun avis à formuler. Plusieurs instructions ministérielles des années 1976 et 1986 ont donné délégation à la Sûreté de l'Etat, alors branche de l'Administration de la Sûreté Publique avec l'Office des Etrangers :

- pour accorder à des ressortissants belges non domiciliés en Belgique l'autorisation d'importer ou de porter, dans le pays, des armes dans un but sportif ;

- de procéder à des enquêtes approfondies concernant des autorisations de porter une arme octroyée à des étrangers venant en Belgique ;

- de délivrer des permis de port d'arme à des ressortissants belges non domiciliés en Belgique dans le cadre de leurs activités professionnelles dans le Royaume.

La compétence de la Sûreté de l'Etat était cependant tout-à-fait résiduaire et se limitait alors à quelques rares cas, l'Office des Etrangers n'ayant pas pour sa part de compétence à l'égard des Belges.

En 1990 toutefois, une procédure élaborée entre le ministère des Affaires étrangères, le ministère de l'Intérieur et le Ministère de la Justice accorda à la Sûreté de l'Etat la compétence de délivrer des permis temporaires de port d'arme aux membres des services étrangers accompagnant une personnalité officielle en visite en Belgique, pour la durée de leur mission.

4.2. Compétences de la Sûreté de l'Etat après la modification du 30 janvier 1991 de la loi du 3 janvier 1933

Outre la compétence précitée de délivrance de permis temporaire de port d'arme aux membres des services de protection étrangers, la Sûreté de l'Etat a initialement conservé sa compétence à l'égard des belges n'ayant pas de domicile en Belgique.

Elle était donc chargée en qualité de déléguée du Ministre de la Justice, Administration de la Sûreté Publique (à l'époque), de leur délivrer les autorisations de détention d'armes à feu de défense ou de guerre et les permis de port d'armes dans les cas d'achat d'une arme en Belgique, de pratique occasionnelle du tir sportif ou de la chasse, d'activité professionnelle et de transit par la Belgique.

Vu le nombre peu élevé de cas, mais compte-tenue de la complexité de la matière, la gestion de celle-ci avait été centralisée au service juridique de la Sûreté de l'Etat. L'Office des Etrangers, quant à lui, disposait de la même compétence à l'égard des étrangers non domiciliés en Belgique.

La scission de l'Administration de la Sûreté publique

L'arrêté royal du 31 décembre 1993 relatif à l'organisation du Ministère de l'Intérieur et de la fonction publique, entré en vigueur le 1er janvier 1994 a opéré la scission organique des deux

branches de l'Administration de la Sûreté publique par le transfert des services de l'Office des étrangers au ministère de l'Intérieur.

Dans cette perspective, une décision ministérielle est intervenue le 7 janvier 1993 par laquelle *"(...) sont transférées à la Sûreté de l'Etat à partir du 1er mars 1993, les compétences exercées par l'Office des Etrangers en matière de délivrance des autorisations de détention et des permis de port d'armes à feu aux étrangers non domiciliés en Belgique en application des articles 6, §2; 7 alinéa 2, et 11, §1er, alinéa 2, de la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes et au commerce des munitions, modifiées par la loi du 30 janvier 1991".*

5. LES COMPÉTENCES DE LA SÛRETÉ DE L'ETAT DANS LE CADRE DE LA LÉGISLATION BELGE ET EUROPÉENNE SUR LES ARMES

5.1. La loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions, (modifiée notamment par la loi du 30 janvier 1991 et des arrêtés d'exécution)

La vente, la cession ou l'importation d'une arme à feu de défense ou de guerre n'est autorisée qu'aux personnes physiques ou morales titulaires d'un agrément d'armurier, de fabricant, de courtier ou de collectionneur ainsi qu'aux titulaires d'une autorisation de détention de ces armes (articles 5, 8 et 9 de la loi du 3 janvier 1933).

La délivrance d'une autorisation de détention d'une arme à feu de défense ou de guerre est subordonnée à divers contrôles préalables tels la connaissance élémentaire de la législation, l'aptitude à la manipulation de l'arme, la nature de l'arme faisant l'objet de la demande, les motifs de celle-ci (défense personnelle, pratique du tir sportif, pratique de la chasse, activité professionnelle, autres motifs tels que arme faisant partie du patrimoine familial, placement financier,....), la personnalité du demandeur, etc ...

Les demandes relatives à des armes de guerre doivent être examinées avec plus de circonspection.

L'autorisation de détention permet de détenir l'arme au domicile ou à la résidence du titulaire. Par dérogation à l'exigence d'un permis de port d'arme pour porter l'arme en dehors des lieux précités, l'autorisation de détention d'une arme à feu permet également de porter l'arme vers un stand de tir, ou de la transporter, non chargée et hors de portée, soit dans une valise fermée à clef : soit dans un emballage quelconque à la condition que l'arme soit munie d'un dispositif indépendant empêchant temporairement son utilisation, sur le trajet entre son domicile ou sa résidence, ou entre un de ces lieux et un stand de tir ou le lieu d'activité d'une personne agréée.

Dans ces hypothèses, le titulaire est tenu d'être porteur de l'autorisation de détention (article 17 de l'arrêté royal du 20 septembre 1991).

Le port d'une arme de défense n'est autorisé que pour un motif légitime et moyennant possession d'un permis de port d'arme tandis qu'il est interdit de porter une arme de guerre (il n'existe pas de permis de port d'arme de guerre) sans motif légitime.

Les militaires, les gendarmes, les adeptes d'une discipline sportive à l'arme de guerre disposent d'un tel motif. Le permis de port d'arme (article 7 de la loi du 3 janvier 1933) ne peut être délivré que pour une arme que le demandeur détient régulièrement, c'est-à-dire avec une autorisation de détention ou un document assimilé.

La délivrance de ce document est subordonnée à des vérifications strictes tant au plan du motif de la demande qu'au niveau de la sécurité. Le permis doit mentionner clairement les conditions et les circonstances dans lesquelles le port de l'arme est autorisé.

Lorsque le requérant n'est pas domicilié en Belgique, les articles 6,§ 2 (délivrance de l'autorisation de détention d'une arme à feu de défense), 7, al. 2 (délivrance d'un permis de port d'arme de défense) et 11,§ 1er, al. 2 (délivrance d'une autorisation de détention d'une arme à feu de guerre) de la loi de 1933 confèrent la compétence de délivrer les autorisations et permis précités, *au Ministre de la Justice ou à son délégué.*

Les mêmes articles prévoient que le ministre de la Justice ou son délégué peut suspendre, voire même retirer, une autorisation de détention d'une arme de défense ou de guerre "*s'il apparaît que la détention peut porter atteinte à l'ordre public*". Cette décision de suspension ou de retrait doit être motivée.

5.2. L'arrêté royal du 20 septembre 1991 exécutant la loi du 3 janvier 1933 précitée (modifié par les arrêtés royaux des 18 janvier 1993, 30 mars 1995 et 6 février 1996)

L'article 9 §1er, 2° et §2, 2° de cet arrêté prévoit que la demande d'autorisation de détention respectivement d'une arme à feu de défense et d'une arme à feu de guerre est adressée par les personnes non domiciliées en Belgique *au Ministre de la Justice, administration de la Sûreté de l'Etat*.

De même, l'article 15, 2° du même arrêté stipule que la demande de permis de port d'arme de défense est adressée par les personnes non domiciliées en Belgique à l'autorité précitée.

Les articles 14 et 16 prévoient qu'en cas de retrait ou de suspension d'une autorisation de détention d'une arme de défense ou de guerre, le ministre de la Justice ou son délégué, ou le gouverneur de province notifie sa décision au titulaire de l'autorisation par lettre recommandée avec accusé de réception. Cette décision de suspension ou de retrait doit être motivée et communiquée au Registre central des armes.

L’arrêté royal du 20 septembre 1991 institue aussi au sein du Service général d’appui policier un registre central des armes. La Sûreté de l’Etat est tenue d’alimenter ce registre qui n’est accessible qu’à certains ministres et à un nombre strictement limité d’autorités judiciaires, administratives et de police.

L'article 28 al. 3 de l'arrêté royal du 20 septembre 1991 stipule que *"Les informations relatives à l'acquisition ou la cession d'armes à feu en Belgique par des ressortissants étrangers sont communiquées aux autorités judiciaires et services de police du pays dont ces personnes sont ressortissantes à l'intervention du Service général d'appui policier* ".

5.3. Compétences décisionnelles de la Sûreté de l’Etat

En application des textes qui précèdent, la Sûreté de l'Etat délivre donc des autorisations de détention d'une arme à feu de défense (modèle N° 4 prévu à l'annexe de l'arrêté royal du 20 septembre 1991) et des permis de port d'arme de défense (modèle N° 5 prévu à l'annexe de l'arrêté royal du 20 septembre 1991) :

- aux étrangers qui n'ont pas de domicile en Belgique ;
- aux belges qui résident à l’étranger.

5.3.1. Les étrangers qui n'ont pas de domicile en Belgique

Les catégories d’étrangers n’ayant pas de domicile en Belgique pour lesquelles la Sûreté de l’Etat est compétente sont :

- les personnes à statut diplomatique visés par l'article 1er de l'arrêté royal du 30 octobre 1991 lesquels ne font pas l'objet d'une mention dans les registres communaux (pour des motifs de défense personnelle avec autorisations de détention et permis de port d'arme) ;

- les militaires étrangers en poste au SHAPE (pour la pratique du tir sportif avec autorisation de détention) ;

- les agents d'entreprises de gardiennage étrangères reconnues en Belgique et qui y exercent certaines activités professionnelles pour lesquelles des autorisations de détention et permis de port d'arme sont nécessaires.
  Dans cette hypothèse, en application de l'article 31 al. 2 de l'Arrêté royal du 20 septembre 1991 précité, le *“Ministre de la Justice, administration de la Sûreté publique”* prend l'avis du Ministre de l'Intérieur, direction de la Police générale du Royaume ;

- les étrangers qui désirent acquérir en Belgique une arme soumise à autorisation soit en vue de son exportation, soit pour la laisser dans un club de tir sportif en vue de la pratique de cette activité avec autorisations de détention.

En vertu de l'article 7.1. de la Directive 91/477 /CEE du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes, les ressortissants de l'Union Européenne sont soumis à cet égard au régime de la double autorisation en vue de pouvoir acquérir une arme sur le territoire d'un autre Etat membre : ils doivent donc au préalable obtenir l'accord de leur autorité nationale compétente.

- les étrangers non membres de l'Union Européenne qui désirent pratiquer le tir sportif et la chasse avec des armes soumises à autorisation en Belgique (autorisations de détention);

- les membres des services de protection étrangers officiels pour la protection de leurs personnalités nationales en visite en Belgique. L'autorisation temporaire de détention et de port d'une arme à feu de défense est délivrée après avis du Ministre de l'intérieur, Police générale du Royaume conformément à l'article 31 al.2 de l'arrêté royal du 20 septembre 1991 cité supra;

- les tireurs sportifs étrangers (non membres d'un club de tir) et chasseurs étrangers qui participent exceptionnellement à une compétition de tir ou à une chasse ou qui transitent par la Belgique avec des armes qui nécessitent une autorisation (autorisation de détention temporaire d'une arme à feu de défense ou de guerre).

5.3.2. Les Belges qui résident à l'étranger

Les catégories de Belges qui résident à l'étranger pour lesquelles la Sûreté de l'Etat est compétente sont :

- les Belges résidant à l'étranger qui souhaitent acquérir une arme à feu soumise à autorisation et l'emporter dans le pays de résidence et ce, soit pour des motifs de pratique sportive ou de chasse, soit pour des motifs de sécurité.
  Le service des Contingents et Licences du Ministère des Affaires économiques est consulté pour les problèmes d'embargo éventuel.

- les Belges résidant à l'étranger qui souhaitent acquérir une arme à feu pour la pratique du tir sportif lors de leurs séjours en Belgique.

5.4. 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 - l'arrêté royal du 8 août 1994 relatif aux Cartes européennes d'armes à feu

Les normes belges précitées sont conformes à la directive précitée qui prévoit notamment que les Etats membres ne permettent l'acquisition et la détention d'armes à feu soumises à autorisation qu'à des personnes qui ont un motif valable et qui ne sont pas susceptibles de présenter un danger pour eux-mêmes, pour l'ordre public ou pour la sécurité publique.

L'article 12 de la Directive précitée institue aussi la carte européenne d'armes à feu notamment afin de permettre aux chasseurs et tireurs sportifs de l'Union européenne de se déplacer avec plus de facilité sur le territoire des Etats membres pour pratiquer leurs activités.

La carte européenne d'armes à feu est délivrée par l'autorité compétente du pays de résidence du demandeur. En Belgique, cette autorité nationale est le Service général d'appui policier, Registre central des armes.

Cette carte peut être comparée à une sorte de passeport européen pour les armes; elle mentionne les armes que le demandeur souhaite y voir figurer et pour lesquelles il détient les autorisations de détention requises.

Le chasseur ou tireur sportif qui désire pratiquer son activité sur le territoire d'un autre état membre de l'Union Européenne doit y être autorisé par l'autorité compétente de cet Etat.

En vertu de l'article 8 de l'arrêté royal du 8 août 1994 précité, *"Toute personne, détentrice d'une carte européenne délivrée par un Etat membre de l'Union européenne qui souhaite séjourner temporairement en Belgique avec des armes à feu qui, selon la législation belge, sont soumises à autorisation de détention doit préalablement transmettre la carte délivrée par son autorité nationale au Ministre de la Justice, Administration de la Sûreté de l'Etat, en précisant la durée et les motifs de son séjour. Une fois munie du sceau du Ministère de la Justice, la carte vaut autorisation de détention temporaire de ces armes en Belgique. Cette autorisation peut être accordée pour un ou plusieurs séjours et ce, pour une période maximale d'un an, renouvelable.*
(...)

Toute personne, détentrice d'une carte européenne délivrée par un Etat membre de l'Union européenne, qui souhaite séjourner temporairement en Belgique avec des armes à feu qui, selon la législation belge, ne sont pas soumises à autorisation de détention doit seulement être porteur d'une carte en cours de validité et mentionnant ces armes à feu. (exemple : les armes de chasse)
(...)

Les personnes visées aux alinéas précédents doivent être en mesure justifier la raison de la présence temporaire de ces armes sur le territoire belge".

5.5. La compétence d'avis de la Sûreté de l'Etat

Outre ses compétences décisionnelles précitées en matière d'armes, la Sûreté de l'Etat a été investie d'une compétence d'avis à l'égard d'autres instances chargées de l'application de cette législation, à savoir, les gouverneurs de province, les polices communales et l'Office des Etrangers.

5.5.1. La compétence d'avis à l'égard des gouverneurs de province

La consultation préalable de la Sûreté de l'Etat par les gouverneurs de province a été requise ou conseillée par certaines circulaires ministérielles ou par instructions de l'administration. La compétence des gouverneurs s'exerce en effet dans le cadre de la délivrance :

A) Des 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 ;

En ce qui concerne la délivrance des permis de port d'arme pour les membres du personnel des représentations diplomatiques, c'est le point 6.4.4., c) de la circulaire coordonnée du 30 octobre 1995 qui demande aux gouverneurs de consulter la Sûreté de l'Etat avant de statuer.

Après avoir statué, il est demandé aux gouverneurs d'en informer cette même administration, *"de manière à ce qu'elle ait une vue d'ensemble sur le port d'armes de défense par le personnel des missions diplomatiques et assimilés".*

B) Des 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);

La délivrance des agréments d'armuriers est prévue par l'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. L'administrateur général de la Sûreté de l'Etat invoque la circulaire 1260/VII/13 du ministre de la Justice datée du 20 septembre 1993 qui demande en effet aux gouverneurs de province de soumettre ces demandes d'agrément à un examen rigoureux.

Cet examen doit notamment comporter une demande d'avis officieux à la Sûreté de l'Etat *"pour savoir si le demandeur se livre à des activités qui pourraient, conformément à l'article 2, §2, 5° de la loi, porter atteinte à l'ordre public parce qu'elles sont exercées concurrement avec les activités faisant l'objet de l'agrément".*

C) Des permis de port d'arme pour les membres des services de gardiennage.

La consultation préalable de la Sûreté de l'Etat 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 a été, quant à elle, recommandée par l'Administration des affaires criminelles et pénales en 1994.

<u>Commentaires</u>

Le Comité R constate que :

% en ce qui concerne les compétences d'avis évoquées sous a) et b) :

- la dite circulaire 1260/VII/13 du ministre de la Justice datée du 20 septembre 1993 n'est pas reprise dans la liste des textes intégrés à la circulaire coordonnée du 30 octobre 1995;

- cette dernière citée remplace par ailleurs toutes les circulaires rédigées depuis la circulaire 7/SDP/L/1260/I/6 du 23 septembre 1991;

- la procédure d'examen d'une demande d'agrément d'armurier prévue par la circulaire coordonnée du 30 octobre 1995 (point 4.4.4.) ne prévoit plus la consultation préalable de la Sûreté de l'Etat par les gouverneurs de province.

% en ce qui concerne la compétence d'avis évoquées sous c) :

- l'article 31 de l'arrêté royal du 20 septembre 1991 (modifié par l'arrêté royal du 30 mars 1995) prévoit seulement que l'autorité compétente *"vérifie auprès du Ministre de l'Intérieur, direction générale de la Police du Royaume, que cette demande est conforme aux dispositions de l'arrêté royal du 24 mai 1991 relatif aux armes utilisées par les membres du personnel des entreprises de gardiennage et des services internes de gardiennage";*

- ni l'arrêté royal du 20 septembre 1991, ni la circulaire coordonnée du 30 octobre 1995 ne prévoit de manière explicite la consultation de la Sûreté de l'Etat pour les services de gardiennage. Tout au plus, trouve-t-on une mention au point 4.4.4. de cette circulaire qui indique que les avis qu'elle impose au Gouverneur (avis du procureur du Roi, du bourgmestre) ne sont pas limitatifs.

Le Comité R en conclut que la compétence d'avis préalable de la Sûreté de l'Etat à l'égard des gouverneurs de province ne repose pas sur une base réglementaire ou administrative suffisante en ce qui concerne les agréments d'armuriers et les services de gardiennage. Le Comité R estime que cette compétence devrait être officialisée.

5.5.2. Compétence d'avis à l'égard des polices communales pour la délivrance des autorisations de détention d'armes de défense

L'Administrateur général de la Sûreté de l'Etat déclare exercer une compétence d'avis pour la délivrance par les polices communales des autorisations de détention d'armes de défense :

A) Au personnel des représentations diplomatiques non exonéré d'inscription dans les registres communaux ;

Les membres des représentations diplomatiques inscrits dans les registres communaux sont considérés comme domicilié en Belgique pour l'application de la réglementation sur les armes. La compétence de délivrer une autorisation de détention d'armes de défense revient donc à la police communale, (ou à défaut à la Gendarmerie), tandis que celle concernant les armes de guerre revient au gouverneur de la province concernée.

Le point 5.14.2 de la circulaire ministérielle coordonnée du 30 octobre 1995 demande aux polices communales de transmettre dans un délai de huit jours une *copie de l'autorisation à la Sûreté de l'Etat*.

Celle-ci étant chargée de traiter les demandes d'autorisation de détention introduites par des personnes qui ne sont pas inscrites auprès des administrations communales, *"elle pourra donc ainsi avoir une vue d'ensemble sur la détention d'armes par le personnel diplomatique et assimilé"*

B) Aux Belges naturalisés dont les activités concernent la Sûreté de l'Etat

Le point 5.6.4. de la dite circulaire prescrit que l'autorité qui délivre l'autorisation de détention d'une arme de défense fasse procéder à une enquête locale sur la personnalité du demandeur.

Cette enquête doit notamment tenir compte d'une *"éventuelle activité politique violente".* Cette disposition n'oblige pas strictement parlant un service de police à consulter la Sûreté de l'Etat sur ce point.

L'administrateur général estime toutefois que son administration ne peut négliger de répondre à un demande d'information sur ce type d'élément, ceci en toute logique et cohérence avec ses missions. Une telle attitude ne vaut pas seulement à l'égard des belges naturalisés, mais bien à l'égard de toute personne dont les activités concernent la Sûreté de l'Etat.

Commentaires

L'obligation faite aux polices communales de transmettre à la Sûreté de l'Etat une copie des autorisations de détention d'armes de défense qu'elles délivrent au personnel des représentations diplomatiques ne justifie pas en soi une obligation de consulter cette administration au préalable.

Le Comité R reconnaît cependant la pertinence d'une telle consultation et il approuve l'avis de l'administrateur général sur ce point. Il estime néanmoins qu'il serait préférable qu'une telle consultation soit elle aussi officialisée.

5.5.3. Compétence d'avis à l'égard de l'Office des Etrangers pour les demandes introduites par des étrangers résidant en Belgique

Une instruction donnée par le ministre de la Justice en 1964 priait les commissaires de police et commandants de gendarmerie de s'informer auprès de la Sûreté publique (police des étrangers) de la situation administrative de tout étranger demandeur d'une autorisation d'achat d'une arme ainsi que *"des renseignements défavorables que cette administration posséderait à son sujet".*

Cette instruction se référait à un rapport du Sénat (Doc. 99, p. 3 - session 1930/1931) exprimant l'avis que l'autorisation devait être refusée *"si l'acquisition ne se justifie à aucun titre ou si des circonstances spéciales contre-indiquent l'autorisation, notamment, s'il y a lieu de craindre que le requérant ne veuille faire un mauvais usage de l'arme en Belgique ou à l'étranger ou si son casier judiciaire est chargé".*

L'arrêté royal du 31 décembre 1993 relatif à l'organisation du ministère de l'Intérieur et de la Fonction publique a opéré la scission organique des deux branches de la Sûreté publique (Sûreté de l'Etat et Office des étrangers) par le transfert de l'Office des étrangers au ministère de l'Intérieur.

En l'absence de nouvelle instruction en la matière, l'Office des étrangers a cependant continué à consulter la Sûreté de l'Etat en cas de demande introduite par un étranger résidant en Belgique.

Commentaire

Une telle procédure peut à présent se justifier compte tenu des vérifications prescrites par le point 5.6.4. de la circulaire coordonnée du 30 octobre 1995. Une enquête locale doit notamment tenir compte d'une *"éventuelle activité politique violente".*

Ici aussi, le Comité R estime qu'il serait préférable qu'une consultation de la Sûreté de l'Etat soit prévue de manière formelle.

6. LE MODUS OPERANDI DE LA SÛRETÉ DE L'ETAT

6.1. Le service "législation en matière d'armes"

Ce service d'étude est aussi chargé de traiter les matières relatives à la prolifération et aux trafics d'armes. Son responsable (un conseiller-adjoint) représente la Sûreté de l'Etat aux réunions interdépartementales en matière de trafic d'armes et de prolifération.

Ce service est tenu de transmettre toutes les informations utiles aux titulaires des autres matières concernées. La transmission inverse d'informations utiles doit également être assurée.

6.2. Modus operandi applicable tant aux demandes d'autorisation de détention (armes de défense ou arme de guerre) qu'aux permis de port d'arme

Outre les motifs des demandes, la Sûreté de l'Etat vérifie, s'agissant de personnes non domiciliées en Belgique, si elles sont en règle au regard de la législation de l'Etat 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 Etat membre.

Au niveau interne, la Sûreté de l'Etat 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 de l'Etat procède alors à une enquête plus approfondie.

En ce qui concerne les particuliers qui viennent pratiquer le tir sportif ou la chasse occasionnellement en Belgique, la Sûreté de l'Etat 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.

6.3. Modus operandi applicable aux retraits ou aux suspensions d'autorisation de détention (armes de défense ou armes de guerre) et de permis de port d'arme

Les procédures de suspension et de retrait des autorisations ne peuvent bien sûr s'appliquer que pendant les séjours en Belgique des titulaires des dits documents.

En cas de court séjour, l'application de ces procédures semble assez difficile. Ces décisions peuvent faire l'objet d'un recours devant le Conseil d'Etat.

Si la Sûreté de l'Etat a connaissance d'activités violentes de la part d'un titulaire d'un port d'arme, elle en avertit en premier lieu les autorités judiciaires dont la décision peut constituer la base du retrait de l'autorisation.

6.4. Modus operandi applicable aux demandes d'avis

En général, la Sûreté de l'Etat 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.

En ce qui concerne les armuriers, la Sûreté de l'Etat procède à une enquête rapide sur les activités des intéressés. Elle consulte sa documentation générale relative aux trafics d'armes. La police judiciaire procéde aussi à une enquête. Ces deux enquêtes font parfois double emploi.

6.5. Modus operandi applicable à la communication d'informations au Registre central des armes

De la visite et de l'entretien avec le responsable du service compétent à la Sûreté de l'Etat, il ressort que ce service alimente le Registre Central des Armes selon deux procédures distinctes selon qu'il s'agit d'une autorisation de détention d'une arme à feu de défense ou de guerre pour une personne qui n'est pas domiciliée en Belgique (article 9 de l'arrêté royal du 20 septembre 1991) ou de délivrance d'un permis de port d'arme de défense à un étranger non domicilié en Belgique.

Les procédures administratives appliquées par la Sûreté de l'Etat sont décrites dans un rapport du Service d'enquêtes joint au dossier de l'enquête.

7. COMPÉTENCES DE LA SÛRETÉ DE L'ETAT DANS LE CADRE DE LA RÉGLEMENTATION SUR LES ARMES AU REGARD DU PROJET DE LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Le projet de loi organique des services de renseignement et de sécurité adopé par la Chambre des représentants le 23 octobre 1997 ne prévoit pas expressément la compétence de l'Administration de la Sûreté de l'Etat en matière de réglementation relative aux armes.

L'article 7 § 1er, 4E du projet énonce cependant que :

"§ 1er La Sûreté de l'Etat a pour missions : .....
4° d'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi."

Le commentaire de ce texte dispose que :
"Le paragraphe 1er, 4°, vise des missions qui sont ou seraient confiées à la Sûreté de l'Etat par ou en vertu de lois particulières. Par exemple, la loi du 4 août 1955 concernant la sûreté de l'Etat dans le domaine de l'énergie nucléaire, et l'arrêté royal du 14 mars 1956 relatif à l'exécution de cette loi, la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions, modifiée par la loi du 30 janvier 1991 et ses arrêtés d'exécution."

Il appert que la formulation de l'article 7 est très générale et que son commentaire n'y cite la législation sur les armes qu'à titre exemplatif.

8. CONCLUSIONS

L'administration de la Sûreté de l'Etat exerce deux types de compétences en matière d'exécution de la législation sur les armes à feu : des compétences décisionnelles et des compétences d'avis.

Toutes les compétences décisionnelles de la Sûreté de l'Etat à l'égard des personnes n'ayant pas de domicile en Belgique trouvent leur fondement dans la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions, et dans ses arrêtés royaux d'exécution.

C'est pourtant dans des cas exceptionnels et tout-à-fait marginaux que cette administration s'est vue confier par le passé l'exécution de cette législation. Quant au transfert de la compétence à l'égard des étrangers non domiciliés en Belgique, elle résulte du passage de l'Office des Etrangers au Ministère de l'intérieur.

Le Comité R est d'avis que ces compétences décisionnelles n'ont aucun lien avec les activités normales d'un service de renseignement qui consistent à informer les autorités des menaces tant internes qu'externes pouvant peser sur la Belgique.

Par contre, le fondement légal et réglementaire des compétences d'avis de la Sûreté de l'Etat est plus incertain. Ces compétences sont pourtant celles qui entrent le mieux dans le cadre de la mission d'information précitée.

Il convient toutefois de remarquer que les nombreux devoirs que nécessitent l'application de la législation sur les armes (consultation du casier judiciaire, du Registre central des armes, du service Mecano de la Police judiciaire -SGAP-, de l'Office des Etrangers, du Banc d'Epreuve des armes à feu....) relèvent plus d'une mission de police administrative et du maintien de l'ordre public que de la mission de renseignement.

Il paraîtrait dès lors plus adéquat de confier l'ensemble de ces tâches à un seul service dont la vocation réponde à une mission de police administrative.

Ce transfert de compétence peut se réaliser sans qu'il soit nécessaire de modifier la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions. Il suffit en effet que le ministre de la Justice modifie la délégation prévue par les articles 6 §2, 7 alinéa 2 et 11 §1er de cette loi.

Le projet de loi organique des services de renseignement et de sécurité adopté par la Chambre des représentants le 23 octobre 1997 ne prévoit pas expressément la compétence de l'Administration de la Sûreté de l'Etat en matière de réglementation relative aux armes.

9. RECOMMANDATIONS

Le Comité R recommande :

- de retirer à la Sûreté de l'Etat 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'armes de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

Les devoirs que nécessitent l'application de cette compétence d'avis sont la consultation des fichiers de la Sûreté de l'Etat et la consultation de services correspondants étrangers selon le cas. Seuls les personnes connues pour leurs activités violentes devraient faire l'objet d'une enquête plus approfondie de la part de ce service.

L'attribution de cette compétence générale d'avis à la Sûreté de l'Etat nécessitera une adaptation de l'arrêté royal du 20 septembre 1991 exécutant la loi du 3 janvier 1933 précitée.

CHAPITRE 3 : ENQUETE RELATIVE A DES RENSEIGNEMENTS RECUEILLIS OU RECUS PAR LE SGR DANS LE CADRE DE MANOEUVRES MILITAIRES A L'ETRANGER

1. INTRODUCTION

Le 15 mai 1997, paraissaient dans différents journaux (notamment Le Soir, Het Laatste Nieuws, Het Nieuwsblad, ...) des articles se rapportant au fait que trois frégates de l'escadre navale belgo-néerlandaise avaient été attaquées par des habitants de l'île portoricaine de Vieques. Ces derniers ne pouvaient plus supporter que des exercices militaires de tir aient lieu dans leurs zones de pêche. Ils bombardèrent les navires, entre autres de pierres, blessant ainsi deux marins néerlandais.

L'île de Vieques est utilisée comme cible lors d'exercices militaires internationaux.

2. PROCEDURE

Lors de sa réunion du 29 mai 1997, le Comité R a décidé d'ouvrir d'office une enquête de contrôle concernant les renseignements recueillis ou reçus par le SGR, dans le cadre de manoeuvres militaires à l'étranger.

Deux membres du Comité R ont été chargés de suivre et de contrôler cette enquête, et d'en faire régulièrement rapport au Comité R sur son déroulement.

Conformément à l'article 46, § 3 du règlement d'ordre intérieur du Comité R, les présidents de la Chambre et du Sénat ont été avertis, par lettre du 29 mai 1997, de l'ouverture de l'enquête.

Conformément à l'article 43, § 1 de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignements, le Chef du Service d'enquêtes a informé le 3 juillet 1997, le ministre de la Défense nationale de l'ouverture de l'enquête.

Le 30 mai 1997, une apostille a été adressée au chef du Service d'enquêtes, le priant de mener l'enquête auprès du SGR.

3. DEROULEMENT DE L'ENQUETE

3.1. Echange de correspondance

Le 19 septembre 1997, le Service d'enquêtes du Comité R a adressé une lettre à l'Etat-major général, par laquelle il demandait de pouvoir entrer en contact avec un responsable de l'Etat-major général, afin d'obtenir davantage d'informations sur les règles en vigueur en matière de recueil et d'exploitation de renseignements généraux (qui ne relèvent donc ni de la tactique, ni de la stratégie) à l'occasion du déroulement de manoeuvres militaires à l'étranger, dans lesquelles les troupes belges sont placées sous commandement bilatéral.

Le Service d'enquêtes a demandé en même temps de pouvoir rencontrer l'officier responsable de la Force navale ayant pris part à l'exercice 'Mayex 97', afin d'obtenir des éclaircissements à propos des incidents qui s'étaient produits durant cet exercice.

A la date précitée, les questions suivantes ont été adressées au Chef du SGR par le Service d'enquêtes :

1. *"Le protocole d'accord entre le SGR et la Sûreté de l'Etat indique que 'les pays où des militaires belges sont ou pourraient être mis en oeuvre à l'avenir' constituent la première priorité du SGR.*

   Le Comité R désire connaître si cette définition inclut les pays où les militaires belges sont envoyés en manoeuvre ou bien si ces pays sont classés dans la catégorie 'reste du monde'?"

2. *"Le SGR a-t-il reçu mission de rechercher des renseignements sur le contexte dans lequel les manoeuvres navales belgo-néerlandaises allaient se dérouler dans la région de Vieques (Puerto Rico)?"*

3. *"Une collaboration avec le MID hollandais a-t-elle été mise en oeuvre?"*

4. *"Le SGR a-t-il reçu ou collecté des informations préalables sur la situation à Vieques auprès de services de renseignements étrangers?"*
   "Dans l'affirmative, lesquelles? Et a qui le SGR a-t-il transmis ces informations?"

Par lettre du 9 octobre 1997, le ministre de la Défense nationale a informé le Comité R de ce qu'il avait intimé l'ordre au Chef de l'Etat-major général de transmettre tous les renseignements requis au Service d'enquêtes du Comité R.

3.2. Audition du capitaine de frégate

Le 4 novembre 1997, le Service d'enquêtes a procédé à l'audition du commandant de la frégate belge qui avait pris part à l'exercice au cours duquel les incidents se sont produits.

Conjointement aux frégates néerlandaises (6 au total), la frégate belge a participé à un exercice de tir dans les eaux internationales de Puerto Rico. L'intégralité de la flotte était placée sous les ordres d'un officier néerlandais.

Une importante base militaire américaine est située à Puerto Rico (la base de Roosevelt Road qui compte 3.000 hommes). Une grande partie du territoire (environ 80 % de la superficie de l'île de Vieques) est utilisée pour des exercices de tir réels, non seulement par l'armée américaine, mais aussi par celle d'autres pays membres de l'OTAN. Tel fut le cas de la flotte belgo-néerlandaise.

Lorsque, le dimanche 11 mai 1997, la flotte a jeté l'ancre devant l'île de Vieques, avec l'autorisation des autorités américaines responsables, elle fut attaquée par une vingtaine de petits bateaux de pêcheurs, qui ont hurlé des slogans antimilitaristes.

La frégate belge, qui se trouvait le plus près de l'île, a été la toute première à être bombardée avec toutes sortes de projectiles. Le commandant a pris contact avec le commandement de la flotte, qui lui a intimé l'ordre de prendre toutes les mesures nécessaires afin d'éviter toute escalade de l'incident. Le commandant avait remarqué que certains des assaillants étaient en possession de caméras. Il a estimé qu'il s'agissait là d'une provocation d'ordre politique, dont il ignorait les fondements.

L'attaque, qui a duré 45 minutes, a pu être jugulée. Vers 14h15, le commandant a remarqué la présence d'un petit hélicoptère, qui survolait la flotte. Ceci pouvait laisser supposer une nouvelle action, et le commandant en a averti à nouveau le commandement de la flotte. Une nouvelle flottille de petits bateaux a fait son apparition, s'attaquant cette fois à une frégate néerlandaise, et blessant deux néerlandais.

Comme prévu initialement, la flotte a reçu l'ordre de lever l'ancre vers 15 heures.

Durant ces incidents, le commandement a pris contact avec le responsable de la base américaine sur l'île de Puerto Rico, lequel s'est trouvé dans l'impossibilité de donner des informations complémentaires en rapport avec ces événements.

Le commandant estime que c'est par hasard que sa frégate a été attaquée la première, et il suppose en outre que l'incident est le fait d'un mouvement politique d'opposants à la politique de Puerto Rico avec les Etats-Unis.

De plus, le commandant mentionne que le commandement de la flotte, comme de coutume, avait au préalable pris contact avec les responsables militaires américains, afin de s'assurer de la situation générale sur les lieux. Ces derniers n'avaient rien de particulier à signaler à ce propos.

Le FBI mène une enquête.

3.3. Réponses du SGR

Par lettre du 26 septembre 1997, le Chef du SGR a répondu de la manière suivante aux différentes questions posées par le Service d'enquêtes :

"Le texte, tel qu'il est écrit dans le protocole d'accord, vise en principe les pays où des militaires belges sont ou peuvent être mis en opération."
"Toutefois, il se peut que le SGR, dans le cadre de ce que vous appelez 'reste du monde', dispose de renseignements, ou collecte des renseignements utiles pour les militaires qui participent à des manoeuvres dans certaines régions du monde. Ceci se fait alors sur base d'une demande exprimée par l'organisme opérationnel responsable."

"Le SGR n'a pas reçu de mission de rechercher des renseignements sur le contexte dans lequel les manoeuvres navales belgo-néerlandaises allaient se dérouler dans la région de Vieques (Puerto Rico). Une collaboration avec le MID hollandais n'était non plus mise à l'oeuvre. Enfin Le SGR n'a pas reçu ou collecté des informations préalables sur la situation à Vieques auprès des services de renseignements étrangers."

4. CONSTATATIONS

- Lorsqu'il s'agit de manoeuvres à l'étranger auxquelles participent des militaires belges, le SGR ne recueille des renseignements que lorsque ceux-ci lui sont expressément demandés par l'autorité de commandement.

- Etant donné que la question n'a pas été posée dans le cadre de l'exercice 'Mayex 97', le SGR s'est limité à observer la politique générale en la matière.

- Un suivi systématique par le SGR de toutes les manoeuvres à l'étranger impliquant des militaires belges est en pratique irréalisable.

- Selon l'enquête menée, il appert également que les autorités américaines responsables n'étaient pas au courant de possibles incidents.

CHAPITRE 4 : ENQUETE DE CONTROLE SUR L'UTILISATION PAR LES SERVICES DE RENSEIGNEMENT DES POSSIBILITES OFFERTES PAR L'ARTICLE 99 § 3 DE LA CONVENTION D'APPLICATION DE L'ACCORD DE SCHENGEN

1. PROCEDURE

Lors de la réunion du 25 septembre 1997, le Comité R a décidé d'ouvrir d'office une enquête de contrôle sur l'utilisation de l'article 99 § 3 de la Convention d'application de l'accord de Schengen par les services de renseignement.

Deux membres du Comité R ont reçu pour mission de suivre et de contrôler cette enquête et de faire régulièrement rapport au Comité R sur le déroulement de celle-ci.

Par courrier du 29 septembre 1997, Messieurs les Présidents de la Chambre et du Sénat ont été informés, conformément à l'article 46 § 3 du règlement d'ordre intérieur, de l'ouverture de cette enquête de contrôle.

Le 2 octobre 1997, le chef du service d'enquêtes a reçu une apostille l'invitant à procéder aux investigations.

Le 3 octobre 1997, conformément à l'article 43 § 1 de la loi du 18 juillet 1991, le chef du service d'enquêtes a averti les ministres de la Justice et de la Défense nationale de l'ouverture de cette enquête.

Le 15 décembre 1997, le chef du Service d'enquêtes a transmis un questionnaire à l'Administrateur général de la Sûreté de l'Etat et au responsable du SGR.

Respectivement le 18 décembre 1997 et le 9 janvier 1998, le Comité R a reçu la réponse de l'Administrateur général de la Sûreté de l'Etat et du responsable du SGR.

Pour compléter l'enquête, un membre du Comité R s'est entretenu avec un Conseiller de la Sûreté de l'Etat.

Le rapport a été approuvé par le Comité R le 4 juin 1998 et il a été tenu compte pour la publication de ce rapport de la remarque formulée par le ministre de la Défense nationale.

2. MOTIF DE L'ENQUETE

Par courrier du 20 mai 1997, le Comité R a demandé à Monsieur le Directeur a.i. du bureau "Sirène" Belgique dans quelle mesure les services de renseignement faisaient usage de la possibilité de signalement au S.I.S. (Schengen Information System).
En effet, cette possibilité est prévue par l'article 99 §3 de la Convention d'application de l'Accord de Schengen (C.A.S.) qui stipule :

> *"En outre, le signalement peut être effectué conformément au droit national, à la demande des instances compétentes pour la sûreté de l'Etat, lorsque des indices concrets permettent de supposer que les informations visées au paragraphe 4 sont nécessaires à la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'Etat. La Partie Contractante signalante est tenue de consulter préalablement les autres Parties Contractantes.*"

Le 20 juin 1997, Monsieur le Directeur a.i. du bureau "Sirène" Belgique a répondu que les services de renseignement ne faisaient pas usage de la possibilité de signalement sur la base de l'article 99 § 3 de la C.A.S.
Il a indiqué que la principale raison pour laquelle il n'était pas fait usage de cette possibilité s'expliquait par le fait que la procédure prévue est trop lourde.
En effet, la partie signalante est tenue de consulter les autres services frères avant de transmettre tout signalement au S.I.S.

A la suite de ce courrier, le Comité R a tenu à obtenir des explications supplémentaires de la part des services de renseignement nationaux. C'est ainsi que cette enquête de contrôle a débuté.

3. L'INTERET PARLEMENTAIRE POUR LE PROBLEME

Le Comité R n'a aucune connaissance de questions parlementaires relatives à l'application de l'article 99 § 3 de la Convention d'application de l'accord de Schengen.

En ce qui concerne la Convention d'application de l'accord de Schengen, on peut se reporter aux questions parlementaires suivantes :

Question n° 26 de monsieur Vincent Decroly (Ecolo) du 9 août 1995 au ministre de l'Intérieur concernant la Convention de Schengen - Notion "menace pour l'ordre public ou la sécurité et la sûreté nationales" (l'article 96.2 de la C.A.S.).

Question n° 27 de monsieur Vincent Decroly (Ecolo) du 9 août 1995 au ministre de l'Intérieur concernant "Droit d'asile - contrôle aux frontières intérieures." (l'article 96.2 de la C.A.S.)

Question n° 28 de monsieur Vincent Decroly (Ecolo) du 9 août 1995 au ministre de l'Intérieur concernant "Terrorisme - "notion menace pour l'ordre public ou la sécurité et la sûreté nationales" et "contrôles aux frontières intérieures". (l'article 96.2 de la C.A.S.)

4. SYNTHESE DE L'ENQUETE

4.1 Réponse de la Sûreté de l'Etat

Le 17 décembre 1997, Monsieur l'Administrateur général de la Sûreté de l'Etat a envoyé au Comité R une étude succincte relative à cette matière.

Celle-ci décrit clairement quels sont les signalements de la compétence de la Sûreté de l'Etat et quelles sont les personnes pouvant en faire l'objet.

4.1.1. Quels signalements que la Sûreté de l'Etat peut-elle faire ?

L'article 99 § 3 stipule que la Sûreté de l'Etat peut effectuer 2 catégories de signalements :

(1) Signalement pour la sécurité nationale aux fins de surveillance discrète (sans que l'intéressé ne le remarque).

(2) Signalement pour la sécurité nationale aux fins de contrôle spécifique (personnes sur lesquelles des informations doivent être recueillies et qui doivent être fouillées de manière approfondie si possible).

Le but de ces signalements est également décrit.
Les signalements sont effectués pour prévenir une menace grave émanant de la personne signalée ou d'autres menaces graves pour la sécurité intérieure ou extérieure de l'Etat.

Quel critère faut-il appliquer pour procéder aux signalements précités ?
Il doit exister des indices concrets selon lesquels les données demandées au moyen du signalement doivent correspondre au but précité.

En d'autres termes, les renseignements demandés par la Sûreté de l'Etat doivent empêcher la poursuite des faits graves ou éviter que les relations de la Belgique avec l'étranger ou un autre pays de l'espace Schengen soient troublées.

4.2.1. Quelle personne la Sûreté de l'Etat peut-elle signaler ?

Les personnes visées par le signalement de la Sûreté de l'Etat doivent avoir participé ou doivent participer aux faits suivants

- *faits visés aux articles 101 à 124 du Code pénal ;*

- *faits qui représentent une menace pour les relations belges ou celles d'un autre Etat Schengen.*

Dans la note visée plus haut, il est également fait mention des problèmes qui se posent dans l'application de l'article 99 § 3 de la C.A.S.
On peut résumer ces derniers comme suit :

a) Avant la diffusion d'un signalement au niveau du S.I.S. (international), il doit d'abord avoir été effectué au niveau national.
Depuis quelques années, la Sûreté de l'Etat n'a plus la possibilité de faire des signalements nationaux. Auparavant, cela ces signalements étaient effectués dans le fichier informatique de la Gendarmerie à Zaventem.
La Sûreté de l'Etat disposait un fichier dans l'ordinateur de la Gendarmerie, géré par le service extérieur de la Sûreté de l'Etat en poste à Zaventem. Il a été mis fin à cette situation après négociation avec la Gendarmerie.
A cet égard, il faut également relever que le poste de la Sûreté de l'Etat de Zaventem ne fait pas de signalements.

En Belgique, un problème s'est donc posé pour le signalement au niveau national, qui doit intervenir en premier lieu. Il est vrai que, dans la pratique, les services des autres Parties à la Convention n'ont pas fait de problèmes à cet égard.

b) L'article 99 § 3 stipule que la Partie signalante à la Convention est tenue de consulter au préalable les autres Parties à la Convention.
En conclusion, cela revient à dire que la Sûreté de l'Etat ne peut demander un signalement qu'après consultation préalable et obligatoire des services de sécurité concernés des partenaires au traité de Schengen.

Lors des réunions entre les services de sécurité compétents des partenaires au traité de Schengen, qui se sont déroulées voici quelques années, divers problèmes furent exprimés :

a) En République Fédérale d'Allemagne, il n'existe aucune réglementation nationale autorisant le service de renseignement à recueillir de tels signalements.
Ainsi, la base juridique nationale fait également défaut en Allemagne pour donner suite aux signalements visés à l'article 99 §3 effectués par les services de renseignement des autres Etats.
Concrètement, cela signifie qu'aucun service n'est prévu du côté allemand pour se charger de la procédure de consultation préalable obligatoire pour accepter de tels signalements.

Une conséquence importante en est que l'Allemagne indiquera systématiquement les signalements visés à l'article 99 §3, émanant d'autres Etats partenaires, sur la base de l'art. 94 § 4, de sorte que sur cette base aucune action n'est entreprise en Allemagne. (1)

b) les autres partenaires de la convention d'application de l'accord de Schengen, la France en particulier, considéraient cette façon d'agir comme un déficit du niveau de sécurité inacceptable et ont marqué leur désaccord avec le point de vue adopté par l'Allemagne.

c) la délégation 'Française' a fait la déclaration suivante en mars 1995 (quinze jours avant l'entrée en vigueur de la C.A.S.) :
"*La délégation française constate avec regret qu'aucun accord n'a pu être trouvé entre les partenaires Schengen pour la mise en œuvre concrète des dispositions de l'article 99 §3 de la Convention d'application.*
La discussion informelle qui a eu lieu le 13 mars 1995 entre cinq délégations (Belgique, Espagne, Luxembourg, Allemagne, France) a mis en évidence le risque qui subsistait que la France ne puisse avoir la certitude que ses signalements ne fassent pas l'objet de l'opposition systématique d'un indicateur suspendant leur validité sur le territoire d'une autre partie contractante, en l'occurrence l'Allemagne, et cela pour des raisons liées à son droit national.

Prenant en considération la mise en œuvre très prochaine de la Convention d'application, dont la France ne souhaite pas retarder l'échéance, pas plus qu'elle ne souhaite que l'interprétation actuelle de l'article 99§3 ne provoque un ' déficit de sécurité ' .
Les dispositions suivantes seront donc adoptées par ses services :

- *tous les signalements entrant selon ses critères dans le cadre de l'article 99 § 3 seront en fait intégrés dans le SIS (Système Informatique Schengen) sous la rubrique de l'article 99 § 2. Cela ne fait, en pratique, aucune différence pour l'utilisateur final ;*

- *tous ses signalements feront l'objet d'une transmission d'information dans le cadre de la coopération policière aux partenaires Schengen intéressés selon des modalités définies en concertation avec eux .*

La délégation française tient à souligner que cette procédure ne saurait être que transitoire et qu'elle ne préjuge en rien du fond de cette question qui doit être définitivement clarifié ".

A titre de précision, la 'DST' , Direction de la Surveillance du Territoire, est un service de sécurité dont les membres possèdent la qualité d'officier de police judiciaire. Cette qualité leur permet d'appliquer l'article 99 § 2, de sorte qu'aucune consultation des services des autres pays n'est requise, et ils peuvent donc contourner l'article 99 § 3.
A cet égard, indiquons que l'article 99 § 2 porte sur un signalement par un service de police.

---

(1) La possibilité d'indiquer des signalements est décrite globalement à l'art. 94 §4 : "Dans la mesure où une Partie Contractante estime qu'un signalement conformément aux articles 95, 97 ou 99 n'est pas compatible avec son droit national, ses obligations internationales ou des intérêts nationaux essentiels, elle peut faire assortir à posteriori ce signalement dans le fichier de la partie nationale du Système d'Information Schengen d'une indication visant à ce que l'exécution de la conduite à tenir n'ait pas lieu sur son territoire au motif du signalement. (...)"

4.2. Réponse du SGR

Le 9 janvier 1998, le Comité R a reçu la réponse suivante du SGR concernant l'application de l'article 99 § 3 de la C.A.S. :

> *Il est exact, en effet, que le SGR ne figure pas sur les listes des services pouvant signaler des données au S.I.S. (1) ou l'alimenter (2) ou pouvant interroger le système (3). La Sûreté de l'Etat figure bien sur ces trois listes. Cette distinction s'explique, à mon avis, par le fait que le Ministère de la Justice a participé, dès le début, à l'élaboration de l'Accord de Schengen, contrairement au Ministère de la Défense.*
>
> *Par le biais de nos 2 représentants auprès du G.I.A., organisme qui figure bien sur les listes précitées, nous pouvons consulter le S.I.S. le cas échéant.*
>
> *En effet, il serait utile pour le SGR de pouvoir utiliser le S.I.S. dans la même mesure que la Sûreté de l'Etat.*
>
> *Maintenant, si des contrôles transfrontaliers, discrets ou spécifiques doivent intervenir, le SGR s'adresse à leurs services frères dans les pays concernés.*

Le Comité R estime qu'au regard de la lourdeur de la procédure, cet inconvénient vaut également pour le SGR.

5. CONCLUSIONS

- La procédure de signalement prévue par l'article 99 § 3 de la Convention d'application de l'Accord de Schengen est lourde.
  En effet, tous les services des parties contractantes à la Convention doivent être consultés préalablement au signalement. De plus, si une personne signalée est découverte dans un autre pays, le service de sécurité qui a effectué le signalement doit être prévenu via le système "Sirène". Cela suppose que le bureau "Sirène" du pays où l'individu signalé est découvert soit d'abord prévenu. Le bureau "Sirène" informera à son tour le bureau " Sirène" du pays demandeur, qui avisera enfin le service concerné.
  Les services de renseignement des divers pays signataires de la Convention se sont réunis à de multiples reprises à propos de cette procédure et ont toujours constaté que cette procédure n'était pas applicable.

- Pour les raisons précitées, aucun service de sécurité parmi lesquels la Sûreté de l'Etat n'a effectué de signalements au S.I.S. sur la base de l'article 99 §3.

- Les services de renseignement militaires ne sont mentionnés nulle part comme organes pouvant invoquer l'article 99 §3 de la C.A.S. Il s'agit apparemment d'un oubli.

- Le Comité R recommande qu'à l'occasion de la modification de la procédure de signalement, prévue par l'art. 99 § 3 de la C.A.S., un accès au SGR soit prévu.

- Enfin, les services de renseignement et de sécurité disposent de suffisamment de canaux propres pour échanger des données de manière rapide et efficace; liaison télex avec d'autres services, téléphone, etc... . Les services de renseignement semblent collaborer de façon harmonieuse.

6. REMARQUE

On peut se poser la question de savoir si l'échange de données entre les services de renseignement de différents pays, qui s'effectue actuellement au travers de canaux spécifiques ne devrait pas faire l'objet d'un contrôle dans le cadre de la protection de la vie privée.

CHAPITRE 5 : RAPPORT DE L'ENQUÊTE SUR LA PARTICIPATION DES SERVICES DE RENSEIGNEMENT BELGES À DES PROGRAMMES SATELLITAIRES DE RENSEIGNEMENT

1. INTRODUCTION

1.1. Procédure

Le but de la présente enquête est de déterminer la manière dont les services de renseignement belges, principalement le SGR, participent à des programmes de recueil et d'exploitation d'imagerie satellitaire et d'en tirer des recommandations.

Le rapport d'enquête proprement dit est précédé d'une étude théorique sur les satellites d'observation de la terre.

Le Comité R a décidé de mener cette enquête en date du 2 octobre 1997.

Les présidents de la Chambre des représentants et du Sénat, de même que les ministres de la Justice et de la Défense nationale ont été informés de l'ouverture de l'enquête le 8 octobre 1997.

Un questionnaire a été adressé au chef du SGR ainsi qu'à l'administrateur général de la Sûreté de l'Etat.

Le Comité R a désigné Monsieur André Dumoulin, chercheur au GRIP, comme expert afin d'être assisté dans ses recherches théoriques sur ce sujet très technique.

Le Comité R a aussi eu des contacts avec :

- Messieurs Roger Godechoul et Jean-Claude Lacroix, chargés des questions aérospatiales et de défense auprès de l'organisation FABRIMETAL à Bruxelles;

- Madame Frédérique Jacquemin, chargée de mission au cabinet du ministre de la Défense nationale;

- Monsieur Jacques Vanleersberghe, chargé de recherches en applications spatiales au service des affaires scientifiques, techniques et culturelles (SSTC) du Premier ministre;

- le professeur Acheroy de l'Ecole royale militaire;

- des officiers du SGR et de la Force aérienne;

- un commissaire de la Sûreté de l'Etat.

- la firme "Verhaert" de Kruibeke.

Le 14 mai 1998, une délégation du Comité R a visité le Centre satellitaire de l'Union de l'Europe Occidentale à Torrejõn en Espagne.

Le présent rapport a été approuvé le 26 juin 1998.

1. 2. Sources de l'étude sur les satellites

L'étude théorique qui précède ce rapport d'enquête est entièrement basée sur la recherche et l'exploitation de "sources ouvertes" (articles de presse, livres, communiqués et publications de services du gouvernement ou de l'UEO, documents parlementaires, sites internet, etc ...), c'est-à-dire librement accessibles à tout un chacun. Parmi ces sources, seuls les textes légaux, les documents des services gouvernementaux et ceux des organismes de droit international (exemple : les SSTC, l'UEO) ont un caractère officiel.

La liste des sources consultées se trouve en annexe 1 du présent rapport.

1. 3. L'intérêt parlementaire

La politique du gouvernement belge en matière de participation à des programmes de satellites a été discutée à plusieurs reprises; le Comité R a recensé les interventions suivantes :

- Exposé du ministre de la Défense nationale et débat devant la commission des Affaires étrangères du Sénat; 12 février 1996, session 95/96, 1 - 249 / 1.

- Question n° 71 de M. Anciaux (V.U. - Sénat) du 21 juin 1996 au ministre de l'Economie : *utilisation de satellites de navigation permettant de localiser des véhicules - gebruik van navigatiesatellieten waarmee voertuigen kunnen worden gelokaliseerd.*

- Question n° 236 de M. Jan Eeman (V.L.D. - Chambre des représentants) du 6 mai 1997 au ministre des Affaires étrangères : *OTAN et UEO - contribution financière - NAVO en WEU - financiële bijdrage.*

- Introduction du ministre de la Défense nationale au projet de loi organique des services de renseignement et de sécurité - 8 octobre 1997 (638 / 14 - 95 / 96, pp. 3 à 6)

- Question n° 430 de M. Alfons Borginon du 11 décembre 1997 (V.U. - Chambre des représentants) au ministre de la Défense nationale : *participation belge au programme satellite "Hélios 2".*

- Question orale de M. Pierre Lano (V.L.D. - Chambre des représentants) au ministre de la politique scientifique sur les investissements du gouvernement fédéral dans la station spatiale ISS (n° 753 - annales - COM 10.03.1998).

- Question n° 132 de Mme Colen du 29 avril 1998 (Vl. Bl. - Chambre des Représentants) au ministre de la politique scientifique sur le mensuel "Space Connexion" et le projet "Spot".

2. ÉTUDE THÉORIQUE SUR LES SATELLITES D'OBSERVATION DE LA TERRE

2.1. Notions générales

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. Tant dans le domaine civil que dans le domaine militaire et celui du renseignement en particulier, le nombre de puissances à vocation spatiale ne cesse de croître dans le monde. La Belgique elle-même se trouve déjà engagée dans des programmes civils d'observation de la Terre. Elle se trouve aujourd'hui sur le point de s'engager dans un programme militaire européen.

Mais cette situation est de plus en plus marquée par l'intensification de la commercialisation concurrentielle des services spatiaux, ce qui contribue à faciliter l'accès des petits pays, quel que soit leur niveau de développement, aux nouvelles applications de l'espace.

D'autre part, les applications civiles et militaires de l'espace sont de plus en plus interdépendantes. La distinction entre activités spatiales militaires et non militaires n'a jamais été claire; mais aujourd'hui, elle devient de plus en plus floue. En effet, certaines capacités technologiques des satellites civils tendent à se rapprocher des technologies militaires même s'il reste encore des différences qualitatives selon les utilisateurs.

2.2. L'utilisation des satellites d'observation à des fins de renseignement militaire

Evoqués sous l'appellation générique de "National Technical Means" (NTM) dans les traités internationaux, les satellites sont notamment devenus l'un des plus importants moyens de collecte de renseignements des puissances qui en sont dotés.

Les premiers satellites d'observation militaire ont été lancés par les Etat-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 nucléaires américaines : en permettant de réaliser des cartes topographiques précises de l'U.R.S.S., en détectant d'autres objectifs que les villes et en permettant de suivre l'évolution de l'arsenal nucléaire soviétique.

Les satellites d'observation, civils et militaires, connaissent aussi des applications dans le cadre de la surveillance de la mise en oeuvre des traités internationaux de désarmement ou des mesures de sanctions et de désarmement imposées par l'ONU à des pays tels que l'ex-Yougoslavie ou l'Irak.

Actuellement dévolue au renseignement stratégique et opérationnel, l'observation satellitaire devrait aussi offrir dans le futur des possibilités d'exploitation au niveau tactique grâce à des constellations de petits satellites d'observation bon marché, à orbite très basse et donc à durée de vie courte. La qualité de l'imagerie, l'évolution des moyens de transmissions et de l'informatique, permettent à présent d'intégrer le renseignement satellitaire dans les décisions tactiques. Il ne faut cependant pas oublier que si le renseignement satellitaire est important et extrêmement utile, il ne constitue qu'une source d'informations parmi d'autres qui, conjuguées astucieusement, analysées et mises à jour en permanence, permettent de faire une évaluation complète d'une situation donnée en matière de politique étrangère, de sécurité et de défense.

L'imagerie satellitaire permet non seulement de confirmer des informations obtenues par d'autres sources, mais également d'acquérir des informations dans des zones inaccessibles à d'autres sources ou lorsque l'utilisation de sources humaines présente des risques excessifs.

Les satellites d'observation permettent donc, selon leur type, de fournir des informations de base (Basic intelligence) et des informations de situation (Current intelligence).

Les informations de base (Basic intelligence) ne sont pas susceptibles de se modifier à court terme; elles servent généralement à constituer des dossiers de base en vue de décider et de planifier des opérations.

Exemples :

- la localisation d'infrastructures portuaires et aéroportuaires;
- la localisation de systèmes d'armes fixes (bases de lancement de missiles, radars, etc ...);
- l'analyse du terrain (plages de débarquement, zones de sauts, d'atterrissage, etc ...);
- la surveillance de l'environnement pour la prévention et la gestion des risques majeurs naturels et technologiques;
- l'évaluation des ressources naturelles;
- la géodésie;
- la cartographie (réseau routier, ponts, végétation, etc ...)

Ici, la rapidité d'acquisition de ces informations ainsi que leur actualité ne sont généralement pas primordiales. On peut même faire appel à des images d'archives, ne nécessitant pas de nouvelles prises de vues.

Les informations de situation (Current intelligence) concernent une situation à un moment précis susceptibles de se modifier à court terme. Dans ce cas, l'actualité et la rapidité d'acquisition des images sont primordiales.

Exemples :

- l'alerte rapide c'est-à-dire la détection précoce de lancements de missiles ou d'attaques d'avions;

- la détection d'activités nucléaires, biologiques, chimiques et balistiques (NBCB);

- le renseignement électronique (SIGINT), c'est-à-dire la captation des liaisons phoniques (COMINT), des transmissions de données et télémesure des missiles (ELINT) et des signaux radars (RADINT) ;

- la localisation de véhicules, de navires de surface, d'engins militaires, etc ... grâce à un système de balises (Global Positioning System);

- la surveillance de la situation météo;

- l'évaluation des dégâts après une bataille ou un bombardement;

- l'évaluation de la praticabilité d'une infrastructure (un pont, un aéroport), d'un terrain (zone de saut), etc ...

Durant un conflit, ils permettent de localiser avec précision, non seulement les objectif militaires (et d'en connaître la taille, l'équipement), mais aussi les écoles, les centres d'habitation, les hôpitaux, etc ... de manière à permettre aux aviateurs de combattre des objectifs militaires en minimisant les pertes civiles. Cela nécessite le bon choix du satellite survolant la zone d'observation au bon moment, voire la possibilité de reprogrammer la course du satellite en cas d'urgence. C'est ici le domaine des mini-satellites.

Les autres vecteurs de la reconnaissance aérienne.

A l'heure actuelle, la reconnaissance des objectifs militaires repose toujours essentiellement sur les avions de reconnaissance stratégiques (exemple, les U2R) et tactiques (exemple, les F16R), ainsi que sur les UAV (véhicules aériens non-habités) ou drones dont la technologie est en pleine expansion .

Le principal avantage des satellites par rapport aux avions de reconnaissance est de s'affranchir des problèmes de souveraineté nationale et de pouvoir couvrir la totalité du territoire des pays observés. De plus, les satellites ne nécessitent pas de déploiement de moyens à proximité de la zone d'observation comme c'est le cas lors de l'utilisation d'avions de reconnaissance et d'UAV dont le rayon d'action est limité.

2.3. Les capacités des satellites d'observation

Les performances d'un satellite d'observation et la qualité des informations qu'il fournit s'apprécient selon les éléments suivants :

- son orbite;

- la nature de ses instruments d'observation (systèmes appelés "senseurs" ou "capteurs")

- la résolution de ces instruments;

- la durée du cycle d'observation;

- les capacités de transmission des informations au sol;

- les capacités de traitement, d'interprétation et d'exploitation des images reçues;

- la résistance aux effets électromagnétiques et aux interférences LASER.

Chargé de carburant, muni d'un système de propulsion et de son matériel technique, le poids moyen d'un satellite d'observation tourne autour de 1.000 kilos. Les plus gros pèsent de 5 à 6 tonnes. Pour des raisons de coût, on observe à présent une tendance à lancer des satellites de plus en plus légers dans l'espace. Plus ces satellites sont légers, moins bien ils sont équipés (un ou deux capteurs maximum). Ils sont d'une faible durée de vie (vu la faible quantité de carburant qu'ils emportent); ils sont donc généralement destinés à des missions (par exemple scientifiques) très ponctuelles. Sur le plan militaire, des constellations de mini-satellites peuvent être d'un apport utile sur le plan tactique.

2.3.1. Les orbites

Les satellites sont relativement rigides d'emploi sur le plan opérationnel, surtout en matière de changement de plan de l'orbite de plus de quelques degrés, à moins de disposer de réacteurs nucléaires. Lorsqu'un satellite est lancé dans l'espace, il est d'abord placé sur une orbite d'attente par sa fusée porteuse.
Sa mise en orbite opérationnelle se fait au moyen de ses propres moteurs et en consommant une quantité non négligeable de son carburant, ce qui écourte sa durée de vie. Ensuite, subissant l'attraction terrestre, un satellite a naturellement tendance à diminuer son altitude. Il est donc nécessaire de lui faire reprendre de l'altitude de temps à autre, mais ici aussi, au prix de dépenses d'énergie importantes. Ceci explique que la durée de vie d'un satellite soit fonction de la quantité de carburant qu'il emporte avec lui pour alimenter son moteur. Actuellement, la durée de vie moyenne d'un satellite est de sept à huit ans.

En fonction de leurs missions et de leurs senseurs, les satellites d'observation utilisent en effet des orbites spécifiques; il s'agit le plus souvent :

- d'orbites circulaires, c'est-à-dire d'altitude constante au-dessus de la surface de la Terre et formant un plan très incliné par rapport à l'équateur (de 50° à plus de 90°) pour permettre au satellite de survoler toute la terre en un jour par défilement de celle-ci sous l'orbite;

- d'orbites basses, c'est-à-dire à une altitude constante entre 120 et 2.000 km : elles sont utilisées par les satellites de reconnaissance optique, électronique et les satellites de surveillance maritime. Plus il vole bas, plus le satellite est performant, mais aussi plus il est sensible au frottement avec les hautes couches de l'atmosphère, ce qui réduit sa durée de vie à environ 5 ans;

- d'orbites héliosynchrones , c'est-à-dire dont le plan est synchronisé avec le soleil de manière à survoler un point donné toujours à la même heure et de l'observer ainsi dans les mêmes conditions d'éclairement solaire; - c'est le type d'orbite privilégiée pour l'observation terrestre (ex. ERS, SPOT, HÉLIOS);

- d'orbites phasées qui permettent un cycle d'observation de n'importe quel point de la terre à intervalles réguliers.

Les orbites hautes géostationnaires ou géosynchrones se situent à une altitude constante entre 20.000 et 40.000 km. Les satellites tournent sur un plan proche du plan équatorial à la même vitesse de rotation que la Terre; ils sont donc immobiles par rapport à celle-ci. Cette position permet la couverture continue de presque la moitié du globe, vue toujours du même point. Ces orbites sont employées par les satellites de communications (ex. INTELSAT), météorologiques (METEOSAT), d'alerte lointaine (pour la surveillance des missiles et des explosions nucléaires) et de renseignement électronique (MAGNUM et VORTEX). Elles sont aussi utilisées par les satellites de navigation (NAVSTAR pour le GPS - GLONASS).

Les orbites elliptiques ont une trajectoire en forme d'ellipse dont l'altitude la plus basse (périastre) se situe à environ 600 km et l'altitude la plus élevée (apoastre) à environ 40.000 km; elles sont notamment utilisées par les satellites d'alerte lointaine soviétiques / russes MOLNIYA. Sur une orbite elliptique, la vitesse d'avancement du satellite est d'autant plus grande que le satellite est près de la Terre.

En fin de vie, un satellite est soit ramené sur terre, soit propulsé vers une orbite beaucoup plus élevée où il ne peut plus gêner.

2.3.2. Les instruments d'observation

L'imagerie recueillie par les satellites d'observation peut l'être soit par des moyens optiques (IMINT), soit par des moyens électroniques (RADINT). On distingue également les capteurs (ou senseurs) passifs et les capteurs actifs.

Les capteurs passifs sont les appareils photographiques, les caméras visuelles à haute résolution, les caméras électro-optiques, les caméras multispectrales, les (senseurs) capteurs de rayons infrarouges, les capteurs de rayons ultraviolet et gamma ainsi que les détecteurs de pulsations électromagnétiques.

- Les appareils photographiques utilisent des films à haute résolution ainsi qu'un appareillage optique de haute technologie mais ils sont limités à des prises de vues de jour et ils ne permettent pas de voir la nuit et/ou à travers les nuages.

- Les satellites actuels utilisent à présent des caméras électro-optiques (EO) qui enregistrent les données sous forme numérique (c'est-à-dire sous forme de charge électrique) sur des bandes magnétiques. Le stockage de l'information sous forme numérisée permet aussi de traiter les signaux et d'obtenir ainsi une image épurée de perturbation. Elles sont plus flexibles et offrent de bons résultats, même par mauvaises conditions atmosphériques. Par contre, la possibilité de traiter électroniquement ces images offre un risque certain de manipulation dont il faut être conscient.

- Les caméras panchromatiques obtiennent des photos en noir et blanc d'une résolution autour du mètre.

- Les caméras multispectrales sont capables de discriminer plusieurs longueurs d'onde de radiation réfléchies ou émises dans la portion visible du spectre électromagnétique ou dans l'infrarouge. Cette discrimination est rendue possible par l'emploi d'optiques, de filtres et de films spéciaux. Cette technologie permet par exemple de détecter le camouflage grâce à sa capacité de distinguer entre la végétation vivante et la végétation morte. Elle permet aussi de pénétrer dans l'eau, elle est peu sensible aux nuages et aux remous de l'eau.

- Les senseurs à rayons infrarouges (IR) captent la différence de réflexion du rayonnement IR de jour comme de nuit. Ils sont sensibles à l'émission et à la réflexion des ondes thermiques (rayonnements de chaleur). Ils permettent ainsi l'observation de nuit et dans des conditions météorologiques difficiles comme la pluie et le brouillard, mais de manière très limitée. Ils peuvent déceler des moteurs en marche, des gaz de propulsion de missiles ou d'avions. Ils permettent aussi de différencier la végétation naturelle de la végétation artificielle et de percer ainsi les camouflages. Ils peuvent être utilisés pour détecter des mines, des installations souterraines ainsi que des modifications de l'environnement.

  La combinaison d'images panchromatiques, multispectrales et infrarouges permet une analyse plus détaillée du terrain observé.

Les capteurs de rayons ultraviolet et gamma ainsi que les détecteurs de pulsations électromagnétiques servent essentiellement à détecter les explosions nucléaires.

Les capteurs actifs (les radars) ont l'avantage de pouvoir réaliser des observations par tous les temps, à travers la couche des nuages et de détecter des mouvements, ce qui fort important en situation de crise. Ils présentent par contre certains inconvénients :

- ils ont le désavantage de permettre à la cible de savoir qu'elle est observée, moyennant un appareillage adéquat;

- ils consomment beaucoup d'énergie et collectent un flot intense de données; les radars ne fonctionnent que par intermittence et il est difficile d'enregistrer l'abondante moisson de leurs informations;

- ils exigent un personnel hautement qualifié et des technologies beaucoup plus sophistiquées que les capteurs photographiques.

2.3.3. La résolution des appareils d'observation

La résolution est définie comme la plus petite distance entre deux objets qui permet de les distinguer l'un de l'autre.

La résolution des caméras multispectrales en couleurs est moins élevée (plusieurs dizaines de mètres) que celle des caméras panchromatiques (en noir et blanc) dont les photos sont assez précises pour distinguer l'agencement de bâtiments ou de sites industriels. Mais plus la résolution d'un capteur est élevée, moins large est la bande de terrain observée.

La résolution d'un radar est fonction de la taille de son antenne. Ainsi, des radars à haute résolution exigent des antennes d'une grandeur considérable qui peuvent difficilement être emportées à bord de satellites. Ceci explique que la résolution actuelle des radars sur satellites soit plus faible que celle des moyens optiques et infrarouges.

La résolution exacte des satellites d'observation militaires est un secret bien gardé : en 1991, la littérature consultée à ce sujet situait la capacité de résolution d'un satellite d'observation militaire stratégique à 5 mètres. Aujourd'hui, on la fixe entre 15 et 30 cm, ce qui permet l'identification et la description de la plupart des objets militaires. 11 cm semble être la limite actuelle d'observation; celle-ci pourra difficilement être dépassée en raison de l'écran d'humidité ambiante constamment présent dans l'atmosphère.

2.3.4. La durée du cycle d'observation

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.
Les temps de "revisite" prennent toute leur importance lorsqu'il est nécessaire d'obtenir des images à intervalles réguliers 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 meilleure est l'observation. Par contre, la résolution est alors moins grande.

Il peut être remédié aux inconvénients d'un cycle d'observation long par :

- un système de caméras orientables pour accroître le champ d'observation;

- une multiplication des stations réceptrices au sol (fixes ou mobiles) pour raccourcir les délais de réception des données[(1)].

Certains satellites sont manoeuvrables, mais dans des limites assez étroites et, souvent au détriment de leur durée de vie puisque chaque manoeuvre nécessite une grosse consommation de carburant.

2.3.5. La transmission des informations au sol

Autrefois, l'information était enregistrée sur des films développés après le retour sur terre du satellite. Ensuite, les films furent éjectés du satellite dans des cartouches parachutées pour être récupérés en mer ou en vol. Un tel procédé ne permettait pas une information en temps réel.

---

(1) Les satellites civils SPOT, par exemple, survolent le même point tous les 26 jours seulement. Leurs caméras orientables permettent de contourner partiellement le problème en autorisant des prises de vues décalées par rapport à la trace du satellite (chaque point de la surface du globe est ainsi visité en moyenne tous les deux jours). De plus, pas moins de 20 stations réceptrices réparties dans le monde suivent son orbite. Le satellite militaire Helios 1A, grâce à ses caméras orientables de 50°, peut couvrir 70% de la surface du globe toutes les 24 heures. Les satellites militaires américains Key Hole 12, placés sur une orbite plus haute, peuvent par contre survoler le même endroit toutes les douze heures.

L'avantage des caméras électro-optiques est que l'image est à présent transmise par télécommunication à une station réceptrice au sol. La transmission des informations au sol peut être soit immédiate - ce qui permet une information en temps réel - mais à condition que le satellite soit à proximité d'une station de réception, soit différée après stockage à bord sur bandes magnétiques. Les satellites dont le cycle d'observation est long présentent donc aussi le désavantage de n'offrir que des périodes limitées de transmission des données au sol, c'est-à-dire limitées aux moments où les satellites sont en vue d'une station réceptrice.

Les "images" radars recueillies par satellites peuvent être transmises par radio à des stations réceptrices au sol. Cependant, le débit des données transmises est considérable. Pour les exploiter de façon efficace et avec rapidité, il faut disposer, sous la trajectoire des satellites, de stations qui ont des capacités élevées de réception et de traitement des données. Des recherches sont en cours, notamment à l'Ecole Royale Militaire, afin de "concentrer" les paquets de données numériques à transmettre sans toutefois dégrader l'information.

Les stations réceptrices au sol peuvent être fixes ou mobiles.

2.4. Le traitement et l'interprétation des images spatiales

Les images reçues par les stations réceptrices au sol sont ensuite relayées au moyen d'un satellite de communication vers un centre d'interprétation où elles sont analysées et transmises à qui de droit pour exploitation.

Les images spatiales sont stockées sous forme de données numériques et livrées sur bandes magnétiques (Spot Images), par radio (images radar) ou par télécommunication en temps réel (Hélios). Leur traitement et leur interprétation consiste à en extraire l'information utile par une triple démarche : la "lecture" de l'image, son interprétation et l'adaptation de l'information.

La "lecture" de l'image comporte son examen minutieux en vue de détecter, de localiser, de reconnaître et parfois d'identifier des structures ou des objets directement visibles; cette lecture consiste parfois à superposer des images d'un même champ d'observation prises dans des longueurs d'ondes différentes (panchromatiques, multispectrales, infrarouges) mais aussi à des époques différentes. On observe ainsi les évolutions pour en tirer un maximum de renseignements. Ceci suppose d'avoir à sa disposition un stock important d'images d'archives qui peuvent provenir, soit de firmes commerciales, soit de la déclassification d'images militaires.

L'interprétation, c'est l'analyse méthodique qui permet d'obtenir, par déduction et synthèse, des renseignements qui ne sont pas directement visibles sur l'image. Enfin les informations doivent être adaptées en un produit fini utilisable par les décideurs politiques et militaires.

Ces différentes étapes sont effectuées par des analystes d'images spécialisés. Ils mettent généralement en oeuvre des moyens informatiques sophistiqués (par exemple, le logiciel français OCAPI d'aide à la photo interprétation) mais l'opérateur humain reste toujours le maillon le plus important dans le processus. C'est de son oeil et de sa perspicacité que dépend la qualité de l'interprétation .

2.5. Une autre application utile au renseignement satellitaire : les systèmes de radiopositionnement par satellites

Il existe différents systèmes spatiaux offrant la possibilité de déterminer un positionnement géographique : le système américain “Global Positioning System” (GPS) et le système russe “Global Navigation Satellite System (GLONASS). Ces deux systèmes ont des origines militaires mais ils ont maintenant de nombreuses applications civiles.

Ces systèmes permettent de localiser un individu, un objet, un animal ou un véhicule quelconque (voiture, camion, navire, avion, etc...) et, par la suite, de reconstituer ses déplacements. Ils permettent aussi de guider des missiles de croisière vers leurs objectifs. Ces systèmes utilisent la technique de la triangulation. Pour cela, l’objet surveillé doit être équipé d’un appareil d’enregistrement mobile muni d’une antenne. Ce récepteur est aussi petit qu’une carte de crédit. Celui-ci capte les signaux émis par au moins trois des 24 satellites du réseau “Navstar” (pour le GPS). Des stations au sol réparties dans le monde assurent la conduite et le contrôle du système.

Conçue pour des applications militaires et de renseignement , les technologies du GPS et du GLONASS s’étendent à des applications civiles, scientifiques et commerciales de plus en plus nombreuses. On les utilise par exemple pour la navigation en mer, pour la gestion de transports routiers, pour le repérage de cheptels, de véhicules volés, pour les secours aériens, etc ... L’utilisation du GPS reste encore soumise à l’autorisation du Pentagone, son usage sans restriction n’est donc pas garanti, surtout en période de crise internationale.

Le système GPS permet en principe de localiser un objet dans un rayon de 16 mètres. Cependant, cette précision n’a été accessible aux usages civils que jusque fin mars 1990. Depuis la guerre du Golfe, les signaux transmis à usage civil sont en effet cryptés, de manière à dégrader les signaux et ne plus permettre une localisation que dans un rayon approximatif de 90 mètres. Seuls les usages militaires conservent la précision initiale du GPS.

Pour être indépendante des U.S.A., l’Europe a décidé de s’investir dans le développement d’une nouvelle génération de satellites de navigation et de positionnement, entièrement sous contrôle civil : il s’agit du programme “Global Navigation Satellites System” (GNSS) conduit par le groupe tripartite Commission de l’Union Européenne, Eurocontrol et ESA .

La volonté de créer un nouveau réseau GPS tend à disposer à l’échelle de la planète d’un système dont la responsabilité est partagée par tous les Etats et d’éviter ainsi son interruption unilatérale et localisée pour des raisons stratégiques propres aux Etats-Unis pour les utilisateurs civils (compagnies aériennes, véhicules terrestres et ferroviaires).

2.6. Détection et destruction de satellites

Des systèmes de surveillance spatiale ont été déployés en vue de tenir à jour l’inventaire des quelque 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 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.

La surveillance spatiale permet enfin d'évaluer les paramètres de rentrée dans l'atmosphère des gros satellites abandonnés en orbite. La surveillance spatiale est appelée à jouer un rôle crucial si les Etats-Unis décident le déploiement futur de systèmes anti-satellites.

Jusqu'à présent, les satellites ne courent guère de risque d'être détruits. L'importance croissante des systèmes spatiaux dans les dispositifs militaires a cependant conduit à faire de ces installations spatiales des cibles de choix pour des frappes adverses. D'où l'apparition de systèmes de détection et d'armes anti-satellites (ASAT) à l'époque de la guerre froide, tant du côté soviétique que du côté américain. Les armes anti-satellites offrent une très grande diversité d'interférences possibles contre les satellites : depuis des agressions "douces", discrètes et peu visibles destinées à endommager graduellement les dispositifs électroniques des satellites visés, en passant par des "satellites tueurs" et jusqu'à des intercepteurs embarqués à bord d'avions ou d'autres satellites.

Si le déploiement d'armes laser dans l'espace ne viole aucune loi sur l'utilisation de l'espace, (elles ne sont pas en tant que telles des armes de destruction massive), cette initiative violerait malgré tout l'esprit du "traité de l'espace". Si des armes anti-satellite devaient un jour devenir opérationnelle, tout Etat disposant de satellites serait ainsi vulnérable à ces armes aveuglantes et leur autonomie en matière de renseignement via les satellites d'observation serait toujours menacée par cette épée de Damoclès et cette volonté américaine de contrôler l'espace.

2.7. Les enjeux de la surveillance spatiale

2.7.1. L'ouverture de l'espace à la communauté internationale

Longtemps prédominant, le duopole soviéto-américain est depuis longtemps remis en question. D'autres pays, individuellement ou en regroupant leurs efforts, sont parvenus à placer leurs propres satellites d'observation sur orbite. Mais l'ampleur des dépenses d'investissement à engager dans cette voie fait donc que le nombre de puissances spatiales totalement autonomes est encore limité. Cependant, la prolifération des satellites de renseignement va purement et simplement continuer car les voies d'accès à l'espace se multiplient grâce notamment à :

- l'acquisition de satellites et de services de lancement auprès d'un pays producteur d'une telle technologie;

- la coopération internationale et la participation à des organisations intergouvernementales spécialisées dans les services spatiaux : celles-ci permettent à chaque Etat participant de s'engager selon ses besoins et capacités, finançant une part du système global proportionnellement au degré voulu de participation. C'est dans cette double voie que la Belgique s'est engagée, en participant à l'agence spatiale européenne (ESA) d'une part, en collaborant à des programmes multilatéraux tels que SPOT, ou HÉLIOS II, d'autre part.

- la commercialisation des services spatiaux offre aux Etats clients l'avantage de pouvoir accéder à des services spatiaux à des degrés différents en fonction de la nature de leurs besoins, de leurs capacités financières et de leur stade de développement respectif. La supériorité technologique des satellites civils américains a abouti à ce que les Etats-Unis autorisent la construction dans un but commercial de systèmes d'observation spatiale d'une résolution d'un mètre. Déjà, les compagnies privées américaines s'apprêtent à rivaliser avec les satellites SPOT et à terme avec HÉLIOS. En regroupant ces firmes commerciales en une seule agence NIMA, le gouvernement américain cherche à placer les Etats-Unis en situation de quasi monopole pour la fourniture d'images spatiales. Mais les Etats-Unis ne sont pas le seul pays fournisseur d'images spatiales . En fait, les satellites d'observation commerciaux pourraient permettre à de petits pays de briser le monopole des grandes puissances dans ce domaine, mais la bataille commerciale qui s'engage actuellement avec les Etats-Unis risque d'être extrêmement dure.

- la baisse des coûts de production grâce notamment à la technologie des petits satellites.

2.7.2. Satellites d'observation civils ou militaires ?

Les satellites d'observation civils ou commerciaux ont été initialement conçus pour des missions d'observation scientifique. Bien qu'ils soient initialement moins précis que les satellites militaires, les satellites civils sont des moyens complémentaires pour le renseignement militaire en raison des grandes surfaces qu'ils couvrent. De plus, afin de pallier l'insuffisance en moyens satellitaires classifiés, certains gouvernements ont recours aux satellites civils à vocation commerciale comme système d'appoint . Globalement, la course à la haute résolution des firmes commerciales exprime leur volonté d'attirer des clients militaires.

En fait, il n'existe pas de différence fondamentale entre la conception technologique d'un satellite d'observation civil et celle d'un satellite militaire, ce dernier type étant cependant plus performant. En général, les technologies civiles sont moins sophistiquées.

Même si les technologies associées aux satellites civils se rapprochent des capacités satellitaires militaires, il n'en reste pas moins vrai que ces derniers se distinguent des premiers en matière de degré de résolution et de précision géométrique des images, de capacité de surveillance tactique, d'intégration des systèmes d'écoutes électroniques, de confidentialité des informations, de durée de vie, de possibilité de changer d'orbite ainsi que de résister aux effets électromagnétiques. En situation de crise ou de guerre ouverte de haute intensité, ces facteurs font la différence.

Par leur degré de sophistication plus réduit, une grande partie des satellites d'observation militaires russes sont du même niveau technologique que certains satellites civils.

En vérité, bon nombre d'Etats se contentent d'utiliser certaines capacités techniques de satellites civils et commerciaux pour leurs besoins militaires de renseignements ou de communications, nonobstant les risques non négligeables en matière de fragilité, de non-confidentialité, de dépendance, de niveau de qualité de l'offre fournie, de paralysie en cas de crise et d'interdiction gouvernementale de ventes d'image de satellites commerciaux américains, d'effacement discret de certains détails de photos commandées, d'aveuglement des senseurs et de brouillage.

D’autre part, les missions réalisées par les satellites militaires peuvent avoir des répercussions importantes dans le domaine civil, notamment en matière de surveillance de catastrophes naturelles et de protections de civils. La surveillance de l’environnement est aussi un moyen supplémentaire de contribuer à la stabilité et par conséquent à la sécurité internationale, car les risques et les menaces qui pèsent sur l’environnement ont, à l’évidence, dans la majorité des cas, une incidence directe ou indirecte sur la sécurité et peuvent par conséquent affecter les questions touchant à la défense. La surveillance de l’environnement de zones spécifiques d’intérêt est d’ailleurs l’une des missions confiées au Centre satellitaire de l’UEO.
De même, au-delà du renseignement militaire proprement dit, les images satellitaires peuvent servir dans des négociations entre belligérants et contribuer ainsi à limiter la portée des conflits.

Il existe donc un courant de pensée qui considère que les satellites ne doivent pas être des outils exclusivement militaires, placés sous le contrôle total d'un service de renseignement. Ce courant considère que les satellites ne sont pas "civils" ou "militaires"; ils sont "commerciaux" ou "gouvernementaux".

Dans ce dernier cas, ils constituent un "outil de puissance" entre les mains du gouvernement, et ils interviennent en "accompagnement de ses actions de défense", ou en apportant une aide à l'action militaire, mais aussi diplomatique, humanitaire ou de sécurité civile. C’est pour cette raison notamment que les initiatives civiles et militaires ne doivent pas se concurrencer mais plutôt se compléter et rechercher des synergies. Ces synergies sont aussi souhaitables en vue de réduire les coûts élevés des programmes spatiaux et de pouvoir exploiter des technologies déjà éprouvées dans des programmes opérationnels.

Les systèmes de satellites militaires peuvent également devenir des armes de la guerre économique aussi bien que militaire.

En France, le rapport Sillard sur la politique spatiale (novembre 1997) insiste sur la recherche indispensable d’une parfaite complémentarité entre les programmes civils et militaires satellitaires comme c’est le cas aux Etats-Unis. On verra dans la deuxième partie de l’enquête que le SGR demande aussi à pouvoir bénéficier de l’accès aux images commerciales sous certaines conditions.

2.8. L’usage des satellites d’observation et le droit international

2.8.1. Généralités

L’avènement de l’ère spatiale a posé une série de problèmes juridiques nouveaux régis par ce qu’on appelle aujourd’hui le droit de l’espace. Internationales par nature, toutes ces réglementations sont en grande partie l’oeuvre de l’Organisation des Nations Unies (ONU) sous l’égide desquelles cinq traités internationaux ont été élaborés.

Le “traité de l’espace” de 1967 énonce deux grands principes: la liberté de circulation et la liberté d’utilisation des ressources de l’espace circumterrestre. Ce faisant, le traité international de l’espace y établit la possibilité des observations stratégiques, de même que sur les corps célestes. L’absence de toute souveraineté territoriale dans l’espace extra-atmosphérique et son corollaire, 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 .

Le principal avantage des satellites est donc de s'affranchir des problèmes de souveraineté nationale : dans l'espace, chaque engin spatial est exclusivement régi par les lois de l'état dans lequel il est enregistré.

Chaque état qui a accès à l'espace extra-atmosphérique devra y travailler, autant que possible, dans l'intérêt général et à des fins pacifiques. Il est interdit de placer sur orbite des armes nucléaires ou d'autres armes de destruction massive. Cependant, le traité ne prévoit pas la démilitarisation de l'espace extra-atmosphérique au sens large du terme, il n'interdit pas les armes laser anti-satellites (ASAT) qui ne sont pas comprises comme armes de destruction massive. La doctrine et certains pays estiment aussi que ces dispositions n'interdisent pas que l'espace extra-atmosphérique soit utilisé à des fins militaires défensives et de sécurité.

2.8.2. L'usage des satellites d'observation dans le cadre de la surveillance de la mise en oeuvre des traités internationaux de désarmement et d'interdiction d'essais nucléaires

Les satellites d'observation connaissent un regain d'intérêt dans le cadre de la surveillance de la mise en oeuvre des traités internationaux de désarmement et d'interdiction d'essais nucléaires.

En cette matière, la question du contrôle et de la vérification est un facteur essentiel. Elle finit souvent par devenir le thème central des négociations sinon une des clefs permettant la ratification finale des traités; il s'agit d'une garantie importante quant à sa bonne application et évolution, surtout en période de tensions entre les différents Etats parties aux différents traités.

Plusieurs traités contiennent une disposition explicite sur l'obligation de non-interférence face aux moyens techniques nationaux (MTN), dont les satellites d'observation sont un des outils les plus sophistiqués. Il est difficile de s'y dérober, sinon en utilisant diverses techniques de leurrage ou de camouflage, qui révèlent dès lors diverses intentions malveillantes.

Il faut noter à cet égard que l'incapacité des services de renseignement américains à détecter les préparatifs des essais nucléaires indiens au mois de mai 1998 a été qualifiée d' "*échec colossal"* par le président de la commission sénatoriale chargée de superviser ces services. Des analystes ont pu reconstituer les mesures de *"déception passives"* mises en oeuvre par l'Inde pour dissimuler à l'observation des satellites tant la préparation que la réalité de ses cinq tirs nucléaires. Ces manoeuvres ont ceci d'inquiétant qu'elles peuvent rendre caduques les méthodes de contrôle à distance. Ceci indique que le renseignement satellitaire ne remplacera jamais totalement le renseignement humain (Humint).

2.9. L'Europe satellitaire

2.9.1. L'enjeu pour l'Europe : la prépondérance américaine, l'indépendance européenne par quelle coopération et pour quels types de satellites ?

Les américains disposent d'une avance considérable par rapport à tous les autres pays aussi bien dans le domaine spatial militaire que civil. En matière d'observation militaire par satellites, les américains fournissent des images à leurs alliés de l'OTAN et aux pays membres du traité

UKUSA (Grande-Bretagne, Canada, Australie et Nouvelle-Zélande). Cependant, la guerre du golfe en 1990-1991, celle de Bosnie en 1995 et la surveillance de la zone kurde irakienne en 1996-1997 ont montré que les Etats-Unis se réservent effectivement la possibilité de couper ou de censurer les informations obtenues par leurs satellites vis-à-vis de leurs alliés. Les européens ne peuvent donc compter indéfiniment sur la mise à disposition par les Etats-Unis de leurs moyens d'observation pour la mise en oeuvre de leur politique étrangère, de sécurité et de défense commune. D'autre part, des firmes privées américaines commercialisent des images spatiales d'une résolution de plus en plus proche de celle des satellites militaires. Mais ici aussi le gouvernement américain conserve toujours la possibilité d'interdire la vente d'images de certaines zones sensibles, de poser des limitations techniques (notamment sur les angles de prises de vues) ou de couper à tout moment le flot d'images.

Une volonté d'indépendance a conduit plusieurs pays européens à s'associer pour la construction, le lancement et l'exploitation de satellites d'observation civils et militaires. Les nouvelles technologies mises en oeuvre sont en effet bien trop onéreuses pour que les pays puissent les acquérir individuellement.

Dans le domaine civil, les satellites optiques européens SPOT, dont le premier exemplaire a été lancé en février 1986 et le dernier le 24 mars 1998, sont le produit d'une collaboration entre la France, la Belgique et la Suède. Les satellites civils SPOT fournissent des images d'excellente qualité qui sont fort utiles aux services de renseignement mais ces engins conçus pour des usages civils sont malgré tout inadaptés aux besoins spécifiques de ces services.

Les américains voient d'un mauvais oeil la prise d'autonomie de l'Europe dans le domaine spatial. Le département de la Défense U.S. a plusieurs fois proposé aux européens une coopération transatlantique en achetant plutôt des satellites américains, afin d'éviter de "gaspiller de l'argent" dans des programmes indépendants. Dans tous les cas, le croisement des enjeux scientifiques, technologiques, économiques, politiques et stratégiques des applications spatiales aboutit à une concurrence transatlantique malgré la disproportion des budgets spatiaux civils et militaires (960 milliards de FB aux Etats-Unis contre 96 milliards en Europe). Plus précisément, les Etats-Unis dépensent cinq fois plus dans le spatial civil, et vingt fois plus dans le spatial militaire. De toute évidence, l'explosion du marché des satellites tout comme l'identité européenne de sécurité et de défense font apparaître de nombreuses réflexions sur la nécessité de s'allier entre Européens dans ce domaine.

2.9.2. Les satellites militaires européens

A l'initiative de la France, plusieurs pays européens se sont associés pour la construction, le lancement et l'exploitation de satellites d'observation militaires.

Les satellites Hélios I.

Il s'agit d'un satellite optique qui a été lancé le 7 juillet 1995 mais il ne fut opérationnel qu'en octobre de la même année; il ne pratique donc l'observation que par temps clair mais ses utilisateurs se disent satisfaits. Il navigue à une altitude d'environ 680 km d'altitude. Un second satellite Hélios I B a été stocké en 1996 pour une relève éventuelle après 1999. Les évaluations du coût de ce programme oscillent entre 8 et 11 milliards FF (entre 50 et 70 milliards BEF).

Pour la première fois, il ne s'agit plus d'un simple accord pour l'échange d'informations entre services alliés, mais d'un travail commun, dès la conception des objectifs de renseignement. Chacun des pays coopérants a en effet le droit de réaliser des prises de vues au prorata de sa participation financière au programme (France : 78,9%, Italie : 14,1%, Espagne : 7%), grâce à des règles de programmation quotidienne que les états-majors et les services de renseignement des trois pays établissent conjointement.

Chaque pays participant dispose de son centre principal Hélios chargé d'exploiter les images. Chaque jour, chaque pays participant au programme établit un catalogue des images de la terre qu'il souhaite obtenir.

Une fois l'accord des deux autres partenaires obtenu et dès la fusion de l'ensemble des besoins de prises de vues, le centre de Creil élabore le plan de travail tripartite incluant les priorités, les degrés d'urgence et la hiérarchie d'emploi afin de programmer finalement le travail du satellite.

Les trois pays maîtres d'oeuvre d'Hélios 1 ont signé en 1993 un protocole d'accord avec l'Union de l'Europe occidentale (UEO) grâce auquel le "pilier européen de l'alliance atlantique" a accès, sous conditions, aux images d'Hélios.

Les projets Hélios II et Horus.

En 1994, il a été envisagé de lancer, en coopération européenne, le projet Hélios II, qui devrait offrir des capacités d'observation supérieures à Hélios I, notamment l'observation de nuit grâce à des moyens infrarouges, une transmission plus rapide des renseignements recueillis et une précision accrue de ses images pour détecter des cibles d'intérêt tactique. Hélios II devrait remplacer Hélios I en 2002. Trois satellites Hélios II sont programmés. Cette seconde génération de satellites bénéficiera d'une meilleure manoeuvrabilité et de la simultanéité des champs étroit et large.

Les allemands ont d'abord accepté de participer au projet Hélios II, après avoir constaté que les américains étaient loin de leur donner tout le renseignement satellitaire nécessaire sur l'ex-Yougoslavie. La France et l'Allemagne ont donc signé le 7 décembre 1995 un accord à Baden-Baden pour la construction en commun des satellites d'observation Hélios II et Horus. La France devait être le maître d'oeuvre d'Hélios II et l'Allemagne, celui d'Horus (un projet de satellite radar estimé à 15 milliards de francs français anciennement dénommé Osiris et financé à hauteur de 60% par Bonn). L'Espagne et l'Italie ont été associées aux discussions. A ce jour, seule l'Espagne a indiqué qu'elle était prête à participer au projet, à hauteur de 3 à 6 %. La Belgique s'est déclarée intéressée par le projet. Cependant, en avril 1998, l'Allemagne a fait savoir à la France qu'il se retirait du projet Horus.

L'association "Eucosat" qui est un groupe de lobbying des constructeurs européens de satellites (incluant aussi des parlementaires, des chercheurs scientifiques, des hommes politiques européens des sept principaux pays de l'Union européenne) a bien essayé de relancer la coopération entre la France et l'Allemagne en proposant la création d'une instance européenne de coordination en matière d'observation satellitaire. Eucosat préconise aujourd'hui cette approche pragmatique associant Etats européens, l'UEO et l'ESA vu les faiblesses du pilier européen de la défense. Cette instance intergouvernementale aurait pour tâche d'assurer la coordination entre les utilisateurs de satellites, qu'ils soient civils ou militaires, et les centres d'interprétation, en particulier le centre satellitaire de l'UEO à Torrejõn.

La loi de programmation militaire française 1997-2002 a quant à elle prévu une réduction de 10 à 15 % du coût du programme Hélios II. L'arrêt du programme Horus entraîne aussi une économie de 3,8 milliards FF. Selon le rapporteur de la commission des finances de l'Assemblée nationale, *"les programmes spatiaux militaires, comme les programmes scientifiques de l'ESA, devront désormais se rapprocher des programmes civils, en terme de prix, et, par conséquent, en termes de spécifications".*

Sans attendre la décision de Bonn, le ministre français de la Défense nationale avait déjà décidé de commencer la phase de développement et de réalisation du programme Hélios II sur ses seuls crédits, soit quelque 6 milliards FF. Le groupe Matra Marconi Space (MMS) s'est vu officiellement notifié le contrat en décembre 1997. La non-participation de l'Allemagne à Horus ne constitue pas vraiment une menace pour le programme Hélios II puisque la France en reste le principal maître d'oeuvre.

Comme il faut aussi un satellite radar à la France, les technologies civiles à imagerie radar pourraient être une solution de rechange. Le groupe industriel allemand DASA propose de lancer en 2001-2002 un satellite plus petit qu'Horus qui transporterait aussi un radar, mais qui serait moins cher.

Le 27 novembre 1997, les ministres belge et français de la Défense nationale se sont rencontrés à Paris. Ils ont signé un accord selon lequel la Belgique est autorisée à utiliser le système Syracuse II (un satellite français de communication). A cette occasion, le ministre belge a annoncé qu'en 1998, il proposerait à son gouvernement que la Belgique s'associe au projet Hélios II.

2.9.3. La politique satellitaire de l'Union de l'Europe Occidentale

L'Union de l'Europe Occidentale exerce trois fonctions parmi lesquelles la défense collective, la consultation et la réflexion sur les questions de sécurité et de défense européennes. Le développement de capacités opérationnelles autonomes militaires et dans le domaine du renseignement constitue l'une des priorités de l'UEO. Ces éléments ont conduit le Conseil de l'UEO à décider en juin 1991 la mise en place d'un centre d'analyse d'images satellitaires devant l'aider à prendre des décisions en matière de gestion de crises, politiques ou environnementales, et de vérification du respect des traités de maîtrise des armements. En 1995, à Madrid, les ministres de l'UEO ont aussi décidé de participer à un programme européen multilatéral d'observation par satellites en cours de développement en rejetant les solutions d'un système propre à l'UEO.

Situé à Torrejõn (près de Madrid - Espagne), le centre d'analyse d'images satellitaires a été inauguré le 28 avril 1993. Après une phase expérimentale, il a été déclaré "organisme permanent de l'UEO" en 1995. Il travaille au profit des dix états membres et des trois membres associés de l'UEO. Il a pour mission d'analyser des images issues de satellites d'observation civils et militaires à des fins de sécurité et de défense.

Lors de la réunion du Conseil des ministres à Erfurt en novembre 1997, les "pays Hélios" ont offert à l'UEO de renforcer son accès aux images recueillies par ce satellite. Les ministres ont exprimé leur intérêt pour cette offre, de même que pour la proposition de la France de mettre à disposition de l'UEO, lors d'opérations de gestion de crise ou d'exercices, une station mobile au sol en cours de développement, pour la réception directe des images d'Hélios.

Les ministres ont chargé le Conseil permanent d'examiner ces propositions. Ces propositions n'ont pas empêché ces mêmes ministres de confirmer le mandat qu'ils avaient donné à ce même Conseil permanent d'évaluer les possibilités de participation de l'UEO au programme européen multilatéral Hélios II et Horus et ce, en tenant compte de tous les aspects technologiques pertinents.

Par ailleurs, en mai 1998, le Conseil permanent de l'UEO a proposé à l'Union Européenne ainsi qu'à l'OTAN de bénéficier des produits d'interprétation d'images du Centre satellitaire, ce qui représente un pas important vers le renforcement des relations avec ces deux organismes internationaux. Vu la décision de l'UEO de soutenir les Nations Unies et l'organisation pour la sécurité et la coopération en Europe dans leurs activités de gestion de crise, il faut s'attendre à ce que ces organisations internationales puissent elles aussi bénéficier des produits du Centre satellitaire dans un proche avenir.

2.10. La politique spatiale de la Belgique : les programmes gouvernementaux belges d'observation de la Terre par satellites

Il est clair qu'un petit pays, comme la Belgique, ne dispose pas de moyens suffisants pour développer un propre programme spatial totalement autonome. Néanmoins, notre pays dispose de capacités de recherche et de développement non négligeables qui pourraient lui permettre dans un avenir proche de déployer ses propres satellites dans l'espace. La Belgique participe donc à plusieurs programmes spatiaux étrangers et internationaux. Dans ce domaine, notre pays a fait le choix de concentrer ses efforts au plan européen.

2.10.1. Les programmes civils

Depuis 1985, les Services fédéraux des affaires scientifiques, techniques et culturelles (SSTC) ont notamment pour mission de veiller à la mise en oeuvre homogène, à l'échelle du Royaume d'actions et de programmes de recherche sur des thèmes et problématiques ayant une portée nationale ou internationale. D'autres départements fédéraux gèrent des budgets de recherche importants, notamment la Défense nationale.

L'ensemble des moyens mobilisés par l'Etat fédéral en faveur des activités scientifiques et technologiques (AST) est regroupé de manière fonctionnelle dans le Programme budgétaire interdépartemental de la Politique scientifique (PBPS). Avec 1,1 milliards de francs, la Défense nationale a contribué à concurrence de 4,7 % à ce programme budgétaire en 1996.

Dans le cadre de ses compétences, les SSTC gèrent la participation belge aux programmes et activités d'organisations internationales comme l'Agence spatiale européenne (ESA) et EUMETSAT. C'est en effet dans le cadre de ces agences que la Belgique inscrit la quasi-totalité de ses projets technologiques : elle participe au budget de l'ESA (6 milliards de francs) à concurrence de 5% environ.

Dans ce cadre, les SSTC ont mis en oeuvre les programmes gouvernementaux belges destinés à promouvoir l'utilisation des données satellitaires. Il s'agit ici d'une perspective européenne civile qui consiste à développer l'autonomie de l'Europe dans l'espace dans les domaines de l'observation de la Terre, des télécommunications, des prévisions météorologiques, des navigations maritime, aérienne et routière par satellites. Dans un premier temps, ces actions ont porté sur les applications liées aux senseurs optiques à haute résolution. Dans un deuxième temps, ce sont les techniques radar et l'optique à moyenne résolution qui ont été développées.

Le dernier programme en cours est le programme *"observation de la Terre par satellite"* (TELSAT 4) décidé par le Conseil des ministres le 7 mars 1996. Un budget de 323 millions BEF est prévu pour ce programme d'une durée de 5 ans (1996 - 2001). Il a pour but d'assurer la poursuite des programmes précédents et de stimuler plus avant l'exploitation des données satellitaires par les scientifiques, les administrations publiques et les acteurs économiques. Ce faisant, la Belgique adhère aux lignes de force formulées par la Commission européenne quant à l'exploitation de l'imagerie satellitaire, en particulier dans le cadre de la mise en place, par cette dernière, d'un réseau européen d'observation de la Terre (le projet CEO - Center for Earth Observation). Il convient aussi de noter ici le projet "Proba" (Project for On-Board Autonomy) développé par la firme privée "Verhaert" de Kruibeke pour le compte de l'ESA. Il s'agit d'un petit satellite d'observation, pesant 100 kilos, devant fonctionner de manière autonome grâce à son software de bord très perfectionné. Ce satellite doit être lancé dans le courant de l'an 2000 par une fusée de fabrication indienne. Cet engin sera équipé de trois instruments d'observation : l'un destiné à mesurer les radiations radioactives, un autre pour détecter la vitesse et la masse des débris errant dans l'espace, le troisième étant un télescope permettant de prendre des photos d'une résolution de 25 mètres. Ce petit satellite naviguera à une altitude de 820 km en orbite héliosynchrone quasi polaire. Depuis la Terre, les clients pourront directement donner mission au satellite de prendre certaines photos par une simple commande sur internet. L'exécution de ces commandes sera planifiée et gérée par le système informatique avancé du satellite. Contrairement aux satellites classiques, Proba est relativement bon marché : le coût total de son développement (y compris le lancement) tourne autour de 360 millions de BEF. Les responsables de ce projet civil se déclarent parfaitement capables de développer aussi un projet répondant aux exigences de précision et de sécurité requises par des missions d'ordre militaire.

Dans le cadre d'accords bi- ou multilatéraux, notre pays collabore aussi avec certains pays tels que :

- la France et la Suède au programme d'observation de la Terre par les satellites SPOT ;

- la Russie : un spectromètre a été embarqué sur la station orbitale russe MIR;

- l'Argentine : une convention vient d'être signée avec ce pays pour fabriquer des pièces de satellites.

Certains de ces programmes civils peuvent évidemment être utilisés par des départements militaires nationaux ou multinationaux.

2.10.2. Les programmes militaires

Le domaine militaire est extérieur à l'ESA; dans une perspective européenne militaire, la Belgique participe au Centre satellitaire de l'Union de l'Europe Occidentale (UEO). Le gouvernement belge s'est par ailleurs engagé dans une négociation en vue de faire participer la Belgique aux programmes satellitaires militaires Hélios II et Trimilsatcom.

Le ministre de la Défense nationale a aussi proposé le 26 novembre 1997 que les quinze pays de l'Union européenne rédigent un "*livre blanc européen sur la défense*" qui définisse à la fois les missions prioritaires des armées et les types d'armements dont elles devraient disposer : *"un tel document pourrait être particulièrement utile à une meilleure allocation des crédits de défense, au lancement et au développement de programmes d'intérêt commun, dans des domaines jugés prioritaires, comme les satellites d'observation et de surveillance"*, a déclaré le ministre.

Une mise en commun de programmes d'armements, tels les programmes satellitaires, pourrait en effet conduire à d'importantes économies d'échelle. Le commissaire européen Karel Van Miert estime les abaissements possibles de coûts de l'ordre de 20 à 30%.

3. RAPPORT DE L'ENQUÊTE SUR LA PARTICIPATION DES SERVICES DE RENSEIGNEMENT BELGES (SGR et SÛRETÉ DE L'ETAT) À DES PROGRAMMES SATELLITAIRES D'OBSERVATION DE LA TERRE

3.1. La Sûreté de l'Etat

La position de la Sûreté de l'Etat a été communiquée au Comité R par lettre du 5 décembre 1997. Des explications complémentaires ont été obtenues auprès d'un commissaire de première classe le 6 mars 1998.

La Sûreté de l'Etat ne prend part à aucun programme de recueil de renseignements par satellites et n'a aucun accès à ce type de source d'informations.

L'intérêt que peut avoir le service à prendre part à un tel programme doit être suscité par la connaissance des avantages qu'il procure. A ce jour, aucune initiative n'a été prise en la matière, vu le manque de moyens auquel le service est confronté, aussi bien sur le plan matériel que sur le plan du personnel. Le besoin de participer à un tel programme n'est pas clair pour le moment et aucune perspective n'existe en ce sens. Les obstacles ou les difficultés possibles qui pourraient entraver le recours à ces moyens sont les investissements à y consacrer et le manque de capacité d'analyse de l'information.

Les analyses de la Sûreté de l'Etat relatives à l'étranger concernent surtout les conséquences que certains événements s'y déroulant pourraient avoir en Belgique. Dans ce cadre, l'observation satellitaire n'est pas d'un intérêt primordial pour ce service.

Un intérêt potentiel existe pour le recours au Global Positioning System ou à tout autre système équivalent, dans les cas de filatures. Rien de concret n'a encore été mis en oeuvre à cet égard. La Sûreté de l'Etat est à la recherche d'un exemple de législation étrangère qui pourrait servir de modèle à un cadre légal en Belgique pour l'utilisation d'une telle méthode.

La Sûreté de l'Etat est aussi dans l'attente d'une loi permettant les interceptions de sécurité. Dans ce cadre, elle pourrait s'intéresser aux systèmes d'écoutes via des satellites.

3.2. Le SGR

La position du SGR accompagnée d'une étude classifiée "diffusion restreinte" et effectuée par ce service en octobre 1997 a été communiquée au Comité R par lettre du 19 décembre 1997 et développée au cours d'une série de contacts avec des officiers de ce service. D'autre part, une délégation du Comité R a visité le centre satellitaire de l'UEO à Torrejõn le 14 mai 1998. La position du SGR peut être résumé de la manière suivante.

3.2.1. Les besoins du SGR

Les informations satellitaires dont le SGR a besoin sont des informations de base (basic intelligence) et des informations de situation (current intelligence). Le besoin de SGR en imagerie (IMINT ou Imagery Intelligence) est complémentaire aux autres sources de renseignement (OSINT ou Open Sources Intelligence, HUMINT ou Human Intelligence, COMINT ou Communications Intelligence, et ELINT ou Electronic Intelligence). L'imagerie permet non seulement de confirmer des informations obtenues par d'autres sources, mais également d'acquérir des informations dans des zones inaccessibles à d'autres sources ou lorsque l'utilisation de sources humaines présente des risques excessifs. L'acquisition d'images par satellites présente donc, par rapport à d'autres sources d'images (reconnaissance aérienne avec ou sans pilote), l'avantage de ne pas nécessiter de déploiement de moyens à proximité de la zone d'observation.

Les zones à couvrir par l'observation satellitaire doivent correspondre aux territoires où des troupes belges seraient susceptibles d'être engagées dans le cadre d'opérations humanitaires ou de maintien de la paix, aux zones de communication aériennes entre la Belgique et les zones de déploiement de troupes belges, et enfin aux zones de communication maritimes devant être empruntées par les navires de la marine belge. La détermination de ces zones a son importance dans le choix des organismes d'observation satellitaire : ceux-ci doivent être capables de couvrir les zones voulues dans des délais nécessaires à la fourniture d'une information de situation valable.

Les caractéristiques techniques des images doivent être telles qu'on puisse détecter du matériel militaire. Les images doivent pouvoir être prises "en tous temps" (même par temps nuageux), ce qui implique l'utilisation de systèmes de prise de vue infra-rouge ou radar, ce dernier n'étant qu'un complément à d'autres sources.

Les images doivent offrir une qualité maximale et ne pas subir de “dégradation” volontaire (pour camoufler l’origine) ou involontaire (due par exemple à la transmission de celle-ci).

Les images pour l’obtention d’informations de situation doivent pouvoir être disponible dans un délai de 24 heures si possible, 48 heures maximum après la demande; ceci implique une procédure d’acquisition rapide et des moyens de transmission adéquats. Dans le cas d’images répétitives permettant l’analyse de l’évolution d’une situation, les délais de “revisite” d’une zone devraient se situer entre 24 et 72 heures. Les images doivent être mises à disposition pour une durée suffisamment longue et de préférence à titre définitif. La confidentialité du fournisseur doit être assurée de façon à ne pas dévoiler les centres d’intérêts.

Les deux moyens d’accès actuels du SGR aux images satellitaires sont : le Centre satellitaire de l’UEO à Torrejõn et les satellites des services de renseignement U.S.. Ces deux fournisseurs dispensent le SGR d’avoir sa propre structure d’analyse des images puisqu’ils fournissent tous deux des dossiers d’analyse. Les coûts d’acquisition de ces renseignements n’entrent pas dans le budget du SGR puisque :

- d’une part, le financement belge forfaitaire du Centre satellitaire de l’UEO est à charge du ministère des Affaires étrangères;

- l’échange de renseignements avec des services étrangers n’obéit généralement pas à des considérations financières, mais bien au principe du “donnant - donnant”.

3.2.2. Le centre satellitaire de l’Union de l’Europe Occidentale (CSUEO)

Situé à Torrejõn (près de Madrid - Espagne), ce centre a été inauguré le 28 avril 1993. Après une phase expérimentale, il a été déclaré “organisme permanent de l’UEO” en 1995. Il travaille au profit des dix états membres et des trois membres associés de l’UEO. Une soixantaine de personnes de nationalités différentes (parmi lesquelles quelques belges) compose le personnel du Centre. Le budget de ce centre satellitaire s’élève à plus ou moins 400.000.000 BEF par an. Avec les autres Etats membres, la Belgique contribue au fonctionnement du Centre, financièrement et en personnel. La clé de répartition des contributions financières des pays membres est indépendante du taux d’utilisation par les pays concernés. En 1997, la contribution financière de la Belgique à la coopération spatiale de l’UEO s’est élevée à 15.500.000 BEF. Ce montant est inscrit au budget des Affaires étrangères.

Le Centre est investi d’une mission d’exploitation d’images issues de satellites d’observation, à des fins de sécurité et de défense. Ces images sont acquises pour répondre aux questions posées par le Conseil de l’UEO, les Etats membres, les membres associés ou tout autre utilisateur désigné par le Conseil. C’est pourquoi le colonel Molard qualifie le Centre de “politico-militaire” et pas seulement de “militaire”.

Les diverses missions, sont donc :

1. la détection de foyers de tensions et la gestion de crises;
2. la vérification de l'application de traités de désarmement;
3. la maîtrise des armements et de la prolifération;
4. la surveillance maritime et celle des risques majeurs sur l'environnement (risques naturels et risques technologiques);
5. le soutien à des missions de maintien de la paix;
6. le soutien à des missions humanitaires et d'évacuation de ressortissants
7. les opérations militaires de l'UEO.

Le colonel Molard, directeur actuel du centre, résume ainsi sa fonction : "*Evaluer les risques avant qu'ils ne prennent la forme de menaces".*

Le Centre a enfin pour mission de former des analystes d'images spatiales et de développer de nouvelles techniques d'interprétation.

Le Centre de Torrejõn ne dispose pas de satellite propre. Il n'est pas non plus une station réceptrice d'images satellitaires mais bien un centre d'analyse et d'interprétation. Il ne s'agit pas davantage d'un centre de renseignement indépendant; il doit être vu comme l'outil privilégié du Centre de renseignement de l'UEO, mis en place en 1995. Dans une première phase expérimentale, le centre satellitaire travaillait uniquement avec des images acquises sur une base commerciale auprès de diverses sources européennes et étrangères.

Cependant, ce centre intègre à présent des sources ouvertes (images de satellites commerciaux) et des sources classifiées (images de satellites militaires américains et du satellite Hélios I). Une image satellitaire commerciale coûte environ 3.000 dollars (105.000 BEF); un cliché d'Hélios 1 atteint 600.000 BEF.

La procédure de demande d'information satellitaire via Torrejõn est assez lourde : il est prévu cinq jours de délais entre le moment où un Etat membre de l'UEO souhaite demander une telle information et le moment où la demande est officialisée et transmise. Durant ce laps de temps, et en cas de refus d'un autre Etat membre, la question est alors soulevée diplomatiquement au Conseil de l'UEO. Dans tous les cas, la définition des zones géographiques à surveiller suite aux diverses demandes nationales doit rester confidentielle.

L'accès du CSUEO aux images d'Hélios I : les trois pays porteurs du programme Hélios I ont signé en avril 1993 un mémorandum d'entente avec l'UEO qui lui donne accès aux images de ce satellite. Cet accord est devenu opérationnel le 7 mai 1996; il garantit la confidentialité des clichés et leur qualité en matière de haute résolution. L'UEO n'a cependant pas accès à la programmation du satellite qui est gérée exclusivement par les services de renseignement militaires des trois pays membres, à savoir la "Direction du renseignement militaire" (DRM - France), le CESID (Espagne) et le SISMI (Italie). L'UEO peut simplement demander des images, que les trois partenaires, maîtres d'oeuvre, décident ou non de lui donner.

Pour bénéficier d'images provenant d'Hélios I, les treize pays membres de l'UEO dépendent donc d'un accord des trois pays participant au programme (à savoir la France, l'Italie et l'Espagne) ainsi que d'un accord de consensus au sein du Conseil de l'UEO.

Les images du satellite Hélios I commandées par le Conseil de l'UEO sont interprétées à Torrejõn et conservées en deux exemplaires dans ses installations, l'un étant destiné au secrétaire général de l'UEO, l'autre à la Cellule de planification. Les images d'Hélios I classées "très secret" ne quittent pas Torrejõn mais elles peuvent servir à affiner des images commerciales qui, elles, sont transmises à la cellule de planification et au centre de situation de l'UEO à Bruxelles.

Contrairement aux satellites commerciaux, l'UEO n'a pas droit non plus aux "signaux" d'origine issus directement des satellites militaires tels qu'Hélios, mais à leur "interprétation", ce qui ne donne aucune certitude sur l'authenticité des images fournies, notamment sur la date à laquelle une image a été prise.

Analyse et exploitation des images satellitaires .

Le cerveau du Centre s'appuie sur un puissant réseau informatique sur lequel circulent toutes les données que les experts en interprétation, militaires et civils, exploitent et enrichissent de leur savoir-faire: images, cartes, données auxiliaires ou rapports d'analyse. Deux logiciels sont utilisés pour l'exploitation des images : ERDAS, destiné à des applications de portée scientifique générale et OCAPI destiné plus particulièrement aux applications de défense. Ces logiciels permettent notamment la fusion d'images provenant de diverses sources (images optiques et images radars) de même que la production d'images en trois dimensions et de séquences animées. Dans ce domaine, les techniques évoluent à une telle rapidité que l'on change de génération tous les quatre ou cinq ans.

La réponse à une question posée se traduit par la production d'un "dossier" et d'un rapport d'interprétation. Ces dossiers sont constitués sur base d'imagerie satellitaire optique ou radar commerciale achetée par le CSUEO auprès de firmes spécialisées.
Les images sont analysées par les spécialistes du CSUEO qui répondent aux questions spécifiques du demandeur. L'interprétation correcte et pertinente d'une image spatiale exige qu'elle soit accompagnée d'éléments du contexte géographique (cartes, plans, photos, etc ...) et suivant le cas, de données économiques, militaires ou sociales. Cette action humaine apporte la véritable valeur ajoutée à l'image spatiale originelle et représente l'essence même du travail du Centre.

On ne demande cependant pas aux interprètes d'images d'apporter des conclusions à la place de ceux dont le rôle est de faire la synthèse d'un ensemble de sources. Le Centre remet ses rapports à la Cellule de planification et au Centre de situation de l'UEO, situés à Bruxelles. A l'exception de l'imagerie d'Hélios, chaque dossier est aussi transmis à tous les Etats membres, ce qui permet ainsi de partager une "vision commune" de l'information fournie. Les informations sont fournies dans le but d'aider une action diplomatique, économique (embargo) ou militaire.

L'accès du SGR aux dossiers produits par le CSUEO.

Le SGR ne participe pas en son nom à un quelconque programme satellitaire mais représente la Belgique au Comité des Utilisateurs du CSUEO. Le SGR est destinataire de tous les dossiers produits par le CSUEO à l'exception de ceux réalisés sur base d'imagerie HELIOS.

Le SGR ne reçoit donc pas d'images brutes mais uniquement le dossier contenant le résultat de ces analyses et les images les illustrant. En vertu d'un accord entre l'UEO et les pays concernés (France, Espagne et Italie), certains dossiers sont constitués sur base d'images prises par le satellite d'observation militaire Hélios. Ces dossiers ne sont pas distribués aux utilisateurs (et donc pas au SGR directement) mais peuvent être consultés sur demande au siège de l'UEO. Le SGR a accès à ces dossiers dans le cadre de l'UEO.Evaluation

Ce type de coopération internationale tend à l'abandon de la politique habituelle d'échange d'informations entre services de renseignement, basée sur le "donnant-donnant". Dans la pratique, on est encore loin du compte.

Un rapport parlementaire présenté à l'assemblée de l'UEO en juin 1996 a constaté une sous-utilisation de Torrejõn par certains Etats membres de l'UEO. A ce jour, 12 dossiers ont été réalisés suite à une demande belge. Le taux de satisfaction du SGR est bon pour les informations de base, mais totalement insuffisant pour des informations de situation dont les délais d'obtention sont encore trop longs. Cette situation est notamment due à l'extrême lenteur de la procédure de demande et de transmission des données à l'intérieur même de l'UEO en matière d'images satellitaires. Ces déficiences constatées jusqu'en 1995 tenaient aussi aux difficultés d'approvisionnement en images de qualité : une fois la demande reçue par le Centre, il convient en effet :

- de rechercher selon le cas une source disponible appropriée : soit le fond d'archives du Centre, soit un opérateur (civil ou militaire) de satellites;

- de commander les images à l'opérateur choisi et d'attendre les prises de vues : le délai de fourniture dépend du délai que met le satellite à "revisiter" le site à observer (qui peut aller jusqu'à 28 jours) et des conditions météorologiques qui y règnent (les prises de vues optiques sont impossibles en cas de couverture nuageuse, et il faudra attendre une nouvelle "revisite" du satellite).

Le colonel Molard, déclare que le Centre est en mesure de fournir un rapport en cinq jours à partir du moment où il dispose des images demandées.

D'autre part, le fait que les rapports de ce Centre soient fournis automatiquement à tous les pays membres de l'UEO compromet la confidentialité de la démarche. Enfin, les scènes satellitaires originales ne sont pas communiquées au demandeur, mais uniquement des portions de celles-ci dont la qualité est dégradée; d'où l'impossibilité de vérifier l'analyse reçue.

3.2.3. L'accès aux images des satellites des services de renseignement U.S.

La seule nation alliée à laquelle le SGR s'est adressé jusqu'à présent pour obtenir des photos satellitaires sont les USA. Mais ceux-ci ne "donnent" pas de photos : ils les "montrent" et les emportent après consultation. Elles sont souvent accompagnées d'une première analyse mais parfois, les USA ne fournissent que les résultats de l'analyse de ces photos.

Ici aussi les délais de fourniture des informations de situation sont trop longs et la confidentialité de la démarche n'est pas assurée vis-à-vis des Etats-Unis. De plus, les photos montrées font souvent l'objet d'une dégradation volontaire de leur résolution et le SGR n'a pas la possibilité de procéder lui-même à sa propre analyse des images.

3.2.4. L'accès aux images des firmes commerciales

Le SGR n'a encore jamais fait appel aux services de firmes commerciales mais il envisage de le faire en comparant les avantages et les inconvénients de cette source potentielle.

Les avantages sont que les délais de fourniture pourraient être assez courts : de trois à sept jours; une firme belge promet des délais de un à trois jours mais il n'y a pas encore d'expérience à ce jour.

Si la confidentialité est assurée par la firme, les objectifs et les intentions de la Belgique restent inconnus des autres pays, et enfin, les photos originales peuvent être fournies sans dégradation.

Les inconvénients sont par contre les coûts élevés pour le budget du SGR (de 100.000 à 120.000 BEF pour une photo), et la nécessité de disposer d'une capacité d'analyse des photos, (soit une infrastructure informatique adéquate et un personnel très qualifié).

Enfin la confidentialité n'est pas assurée si le fournisseur commercial n'est pas "sûr". Néanmoins, ce problème n'est pas spécifique à l'acquisition d'images satellitaires et le SGR dispose de procédures de vérification à cet égard.

3.3. La décision du Conseil des ministres du 6 mars 1998

Le 6 mars 1998, sur proposition conjointe du Vice-Premier Ministre et Ministre de l'Economie et des télécommunications, des ministres des Affaires étrangères, de la Politique scientifique et de la Défense nationale, le conseil des ministres a donné son accord pour que la Belgique puisse entamer des négociations bilatérales avec les gouvernements français et allemand pours'associer aux programmes Hélios II d'observation optique et Horus[(2)] [(3)] d'observation radar.

(2) Vu l'incertitude existante sur l'implication allemande à ce programme, l'appellation "Horus" (anciennement "Osiris" tend parfois à faire place à l'appellation Radar dans les documents officiels.

(3) Le gouvernement a également décidé de s'associer au programme satellitaire de télécommunication Trimilsatcom/Eumilsatcom, porté par la France, la Grande Bretagne et l'Allemagne et qui pourrait être opérationnel d'ici 2005.

La participation de la Belgique aux programmes satellitaires permet de répondre à trois besoins majeurs du gouvernement :

1) s'assurer d'avoir les moyens nécessaires pour exercer le contrôle politique et le commandement de ses forces armées en temps réel et quel que soit le théâtre dans lequel seront conduites ces opérations (OTAN, UEO, cadre national ou celui d'une coalition ad hoc);

2) participer à la prise de décisions communes en matière de prévention et de gestion de crises conformément aux engagements souscrits (Traités de Bruxelles et de Washington et Déclaration ministérielle de Pétersberg) et, s'il échet, permettre de prendre de telles décisions de manière autonome. Pratiquement, cela consiste à garantir l'accès de la Belgique à la programmation d'images d'observation de la terre pour ses besoins opérationnels;

3) sauvegarder l'accès de l'industrie belge aux activités d'étude, de développement et de production de la nouvelle génération des satellites européens, ceci afin de protéger, voire étendre et diversifier les domaines de compétence dont cette industrie fait montre dans les programmes spatiaux civils et de sauvegarder, voire créer une série de nouveaux emplois.

La participation de la Belgique à ces programmes traduit 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*" [(4)]. Deux objectifs sont recherchés :

- le renforcement de l'idée européenne, en l'occurrence d'une politique commune de défense, d'une part,

- la volonté du gouvernement de pouvoir mener certaines actions autonomes visant à la défense de ses intérêts et / ou à la sécurité de ses ressortissants, d'autre part.

Une telle participation implique aussi la mise en place progressive d'une cellule d'analyse d'images satellitaires pour toute utilisation future ainsi que chaque pays participant au programme Hélios I l'a fait. Un groupe de travail s'est constitué au ministère de la Défense nationale avec pour tâche d'examiner les moyens matériels, humains et financiers à mettre en oeuvre pour constituer cette cellule d'analyse. La dépendance organique de cette cellule au sein des Forces armées n'a pas encore été décidée.

Le montant total de la contribution belge à ce triple programme devrait s'élever à 9,2 milliards de francs sur quinze ans. La décision du Conseil des ministres ne porte cependant que sur les phases 1998 et 1999 des programmes Hélios II et Horus, soit un engagement de 250 millions de francs. Les coûts de participation à Hélios II seront fonction des discussions bilatérales que la Belgique aura avec la France.

---

(4) Extrait de la déclaration gouvernementale du 28 juin 1995

Dans tous les cas, affirme le ministre de la Défense nationale, la participation à ce programme ne sera pas supérieure à la participation belge initialement envisagée pour le programme UEO. Si l'UEO décidait de se joindre ultérieurement aux programmes Hélios II et Horus, la participation de la Belgique sur base bilatérale devrait alors être considérée comme sa contribution au coûts de la participation de l'UEO. La Belgique, tout en considérant une participation via l'UEO comme prioritaire, souhaite donc préserver ses intérêts opérationnels et industriels.

Une clé de répartition interdépartementale provisoire a été répartie entre les quatre départements concernés de la manière suivante : 50 % pour la Défense nationale, 33 % pour les Services fédéraux des Affaires scientifiques, techniques et culturelles, 15 % pour l'Economie et 2 % pour les Affaires étrangères. Cette clé de répartition traduit une volonté de synergie avec des programmes civils comparables. Pour symbolique qu'elle soit sur le plan financier, la participation du ministère des Affaires étrangères à ce programme est aussi politiquement très importante.

Le ministre de la Défense nationale avait déjà inscrit dans la tranche 1998 du plan à moyen terme (PMT) une somme de 70 millions BEF pour les programmes satellitaires d'observation et de télécommunications. Ce crédit fut approuvé au Conseil des ministres du 23 janvier 1998.

Un retour est à attendre pour l'industrie belge en fonction de l'apport financier du gouvernement mais il n'est pas encore possible d'en spécifier la nature qui devra être négociée avec les partenaires européens.

Les capacités industrielles belges dans l'éventail des technologies qui seront mises en oeuvre pour les programmes spatiaux se situent dans les trois régions du pays; les équilibres régionaux devront être respectés [(5)].

La participation à ces programmes satellitaires devrait ouvrir à la Belgique la porte de l' "organisme conjoint de coopération en matière d'armement" (OCCAR) créé en 1996 par l'Allemagne, la France, la Grande Bretagne et l'Italie. L'objectif de cet organisme est de coordonner et d'harmoniser les programmes d'achats militaires des quatre pays concernés. L'OCCAR a repris les programmes satellitaires dans la liste de ses priorités.

Le Conseil des ministres a aussi décidé de créer un comité d'accompagnement, composé de représentants des départements concernés, avec la tâche de suivre l'évolution des programmes.

---

(5) Par exemple, les entreprises liégeoises Spacebel (filiale de Matra et depuis en faillite) et Amos ont testé dans un simulateur spatial l'instrument de prises de vues d'Helios I et de Spot, tandis qu'Alcatel Bell réalisait le banc de tests électriques. Quant à Alcatel Etca (Charleroi) qui a développé le conditionnement d'énergie électrique sur la plate-forme Spot et Helios I, sera probablement partie prenante à Helios II, quelle que soit la décision politique belge, puisque ce nouveau satellite militaire utilisera aussi la plate forme de Spot. Il n'est pas impossible non plus que le Centre spatial liégeois issu de l'Institut d'astrophysique puisse être partie prenante à certains tests d'Helios II, tout comme à l'expertise de la future imagerie radar du satellite Horus. Enfin le "Centrum Voor Teledetectie" du "Vlaamse Instituut voor Technologisch Onderzoek (VITO) implanté à Mol gère le traitement des images "Végétation" de Spot.

4. AVIS SUR UNE EVENTUELLE PARTICIPATION DE LA BELGIQUE AUX PROJETS DE SATELLITES EUROPÉEN HÉLIOS II ET HORUS

4.1. Avis de Monsieur Dumoulin, expert du GRIP

A la demande du Comité R, Monsieur André DUMOULIN, attaché de recherche au "Groupe de Recherche et d'Information sur la Paix" à Bruxelles, a rendu l'avis suivant le 11 février 1998.

"Préalables généraux.

1. *Disposer d'instruments autonomes permettant d'évaluer de façon indépendante, précise et objective la situation générale ou des sites particuliers sur les zones observées et parfois difficile d'accès est l'apanage des satellites d'observation. Liberté de survol, relative invulnérabilité, répétitivité élevée du champ de la surveillance sont aussi associées à ces avantages.*

2. *Ces instruments de surveillance offrent le moyen de fournir des preuves d'agression, de contrôler le respect des accords diplomatiques et de désarmement, de dissuader un Etat-partie de violer ceux-ci, d'observer les zones de crises, de détecter des tensions, d'aider à anticiper, prévenir et désamorcer autant que faire se peut les conflits locaux, régionaux ou inter-étatiques pouvant justifier d'une intervention internationale diplomatique et militaire, d'accompagner des prépositionnement de forces, d'aider à la gestion des crises et de conduire les guerres (détection, ciblage) et parfois de suppléer à l'absence de forces prépositionnées comme outils de renseignement.*

3. *Ces outils de surveillance apportent en partie la garantie de ne pas être entraîné contre son gré dans des opérations multinationales en permettant la vérification de l'argumentaire diplomatique et militaire international (exercice de contre-manipulation et de recoupement d'informations). Aussi, de facto, leur simple existence peut réduire la suspicion parfois bien présente même entre pays alliés.*

4. *La prévention des conflits et la projection de forces qui sont devenues les deux processus diplomatico-militaires majeurs caractérisant le champ stratégique et sécuritaire d'aujourd'hui et plus encore celui de demain requièrent davantage de sources et de moyens de renseignements dont le satellite et ses images sont un des outils et un des vecteurs.*

5. *Le renseignement satellitaire apporte des éléments à interpréter au profit du renseignement militaire, du renseignement d'intérêt militaire et du renseignement de défense global. Il permet d*apporter certaines réponses à certains domaines connexes à la sécurité comme le domaine environnemental ou bio-géographique, tout en offrant l'exemple type du multiplicateur de forces.*

6. *Les pays qui font l'effort de se munir de moyens satellitaires au service de leur défense et de leur diplomatie ont franchi une étape qui les différencie des autres, parce qu'ils les mettent en prise directe avec les événements se déroulant au-delà de l'horizon.*

7. *La multiplication et la redondance des systèmes de surveillance en complémentarité avec l'HUMINT contribuent, lorsqu'ils sont bien gérés et traités, à réduire la possibilité de passer à côté d*indications essentielles du point de vue du renseignement militaire; quand bien même le nombre de données recueillies accroît souvent le risque de ne pas les déceler à temps.*

Considérations nationales particulières.

1. *Plus spécifiquement, les systèmes satellitaires d'observation permettent de réaliser des points de situation sur un théâtre extérieur où sont impliquées les forces armées belges, de réaliser des banques de données géostratégiques comparatives (prévention des conflits) et de réaliser des rapports illustratifs au profit des autorités politiques d'aide à la prise de décision (confirmation, infirmation, pondération du renseignement).*

2. *Entrer en coopération dans un programme spatial d'observation militaire multinational permet d'accroître le volume des renseignements au bénéfice des décideurs nationaux tout en évitant de dépendre totalement d'alliés dominants tentant d'imposer parfois leur propre évaluation du renseignement. L'intégration dans un programme satellitaire est un des moyens permettant d'élargir la voie d'une autonomie de décision.*

3. *S'intégrer dans les programmes satellitaires européens peut avoir un effet de convergence en matière d*identité européenne de sécurité et de défense, dans la mesure où les grandes opérations militaires de maintien ou de rétablissement de la paix seront de plus en plus organisées de manière ad hoc avec quelques Etats qui souhaitent s'impliquer à la carte ou sous un pavillon organisationnel comme l'UEO.*

4. *Dès lors, entrer dans les programmes spatiaux multinationaux comme Hélios-II et Horus est un acte volontariste et stratégique associant une solidarité intra-européenne dans le domaine de la sécurité-défense, tout en réduisant les effets pervers des diplomaties parallèles et des agendas cachés jouant parfois sur la disproportion intra-étatique, le coût prohibitif et l*inégalité d*accès aux moyens de renseignement.*

Eléments pondérateurs, contraintes et limites.

Nonobstant ces éléments favorables à l'intégration dans un processus de coopération d'ordre satellitaire à fonction militaire, il est utile d'intégrer certaines contraintes et facteurs pondérateurs à la participation à ces programmes.

1. *La participation à un système satellitaire dont un des maîtres d'oeuvre a un statut nucléaire implique le constat selon lequel le satellite d'observation a aussi une fonction de cartographie et de détermination des cibles liées à la stratégie de dissuasion. La participation en tant que partenaire aux systèmes satellitaires Hélios II/Horus implique la prise en compte politique de cette capacité gérée par la France.*

2. *La participation à un satellite Hélios II peut éventuellement impliquer - comme pour Hélios I - d*assumer la présence (ou les inconvénients techniques) sur la plate-forme d'un sous-système expérimental ultra-confidentiel français dont la mission pourrait sortir du cadre général de la reconnaissance image et dont les applications d'écoute électronique ont des retombées indirectes sur la stratégie militaire (développement de contre-mesures électroniques afin de contrer les sites radars adverses) et de dissuasion (enregistrement des émissions électromagnétiques des radars antimissiles pour en déduire les aides à la pénétration pour les missiles balistiques nucléaires).*

3. *Les besoins en renseignement imposent à la fois une imagerie à résolution élevée mais aussi moins élevée pour l'examen stratégique de la zone couverte. Aussi, l'intérêt porté par l'apport des satellites civils et commerciaux reste essentiel (Spot, Landsat, Radarsat). La possibilité existe de sous-traiter des images satellitaires via des satellites commerciaux maîtrisant depuis peu la technologie de haute résolution métrique.*
   La question relative aux choix de systèmes satellitaires militaires ou civils de même résolution impose des synergies souples en fonction des besoins, des missions de l'urgence et de l'autonomie, d'une nécessaire confidentialité et des moyens budgétaires.

4. *Dans tous les cas, la dépendance en tant que client à des images satellitaires provenant d'Etats participants au programme pose des problèmes d'autonomie et de contrôle:*

   * *Dans le cas de satellites militaires américains offrant des images, la dépendance technologique et stratégique s'avère évidente. Les Etats-Unis seraient en position de ne pas fournir toutes les images demandées tandis que l'origine temporelle et l'authenticité des images ne seraient pas totalement certaines.*

   ***** *En ce qui touche aux satellites commerciaux américains, il est possible que le gouvernement américain puisse exiger du constructeur le contrôle de l'obturateur vendu à des pays étrangers ou exploités pour eux. Une politique de réquisition ou un verrouillage officiel américain sur les satellites américains pourraient survenir dans le cas où, lors d'une crise, les intérêts vitaux américains seraient en jeu. Durant la guerre du Golfe, les clients privés n'avaient plus accès aux images de la zone moyen-orientale. Le risque relatif à une manipulation de logiciels commercialisés au sein des compagnies productrices de satellites privés n*est pas impossible. Enfin, à la différence des satellites militaires, les satellites commerciaux ne sont pas protégés et durcis aux impulsions électromagnétiques et ne protègent pas le transfert de données vers les stations aux sol (fiabilité, résistance, sûreté). Dès lors, brouillage et interception restent du domaine du possible.*

***** *Dans le cas du système satellitaire Hélios I actuellement opérationnel, le Centre de Torrejõn de l'UEO ne dispose pas du "signal d'origine" issu du satellite, mais d'images déjà "travaillées" et pré-interprétées, ne disposant donc pas des moyens de contrôler l'origine et l*authenticité des documents. Un embargo des photos Hélios-1 en cas de crise impliquant un des Etats participants au programme n'est pas impossible. Par ailleurs, ce sont trois stations françaises qui, en définitive, peuvent contrôler ou modifier l'orbite du satellite de reconnaissance Hélios-1. Finalement, seuls les trois Etats partenaires à Hélios-1 (France, Italie, Espagne) bénéficient de la totalité du cycle du renseignement satellitaire et disposent chacun des images initiales, mais seule la France maîtrise et contrôle, dans l'absolu, le processus technique de contrôle dans toutes ses composantes (maître d*oeuvre principal, représentation principale à Creil, contrôle hexagonal des orbites).*

5. *En dehors de la question de la qualité des images (résolution et précision des paramètres géométriques), du coût d'abonnement aux images et du contrôle du processus d*acquisition en temps de crise, la différence principale entre le satellite militaire intra-européen et le satellite commercial réside, d*une part, dans la capacité de demande d*images immédiate et prioritaire (tenant compte néanmoins du nombre d*Etats membres participants au système satellitaire militaire et au prorata de leur part budgétaire) et, d*autre part, par le caractère confidentiel des demandes relatives aux zones à surveiller. Or, ces deux éléments ne sont pas garantis dans les autres cas de figure.*

   *La question d'une participation nationale aux satellites militaires d*observation Hélios II / Horus n'est pas entièrement dépendant du seul secteur diplomatico-militaire. Elle implique des accords d'ordre gouvernemental entre plusieurs ministères, des choix de répartition de budgets mais aussi l'analyse des éventuelles retombées dans certaines niches technologiques belges et régionales, à différents stades des programmes et de leurs versions ultérieures éventuelles dans le cadre de programme de modernisation ou de saut générationnel.*

Recommandations

- *Tenant compte du rapport technique sur les satellites, des préalables généraux, considérations nationales particulières et des éléments pondérateurs, contraintes et limites aux systèmes satellitaires;*

- *N'ignorant pas que le texte du projet de loi organique des services de renseignement et de sécurité adopté par la Chambre des Représentants de Belgique le 23 octobre 1997 stipule dans son article 9 paragraphe 1er que le SGR a pour missions : 1°) de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer l'intégrité du territoire national, les plans de défense militaires, l'accomplissement des missions des forces armées ou la sécurité des ressortissants belges à l'étranger ou tout autre intérêt fondamental défini par le Comité ministériel, et d'en informer sans délai les ministres compétents;"*

- *Rappelant que le responsable du SGR a défini les notions de "renseignement stratégique"; "renseignement opérationnel" et "renseignement tactique" (où la dimension satellitaire y est sous-jacente) et que le Comité R fait siennes dans le Rapport d'activités du Comité R de 1997 (pp.119-120);*

- *Estimant par ailleurs que l'espace seul ne peut tout apporter et qu'il doit être couplé à une combinaison-intégration de différentes sources d'acquisition aérienne et terrestre, et que le renseignement humain (HUMINT) est bel et bien un secteur à ne pas négliger au sein du SGR afin d'améliorer les volets prévention et intentions dans le cadre de missions extérieures;*

- *Conscient que la décision de s'intégrer dans les systèmes Hélios II puis Horus va dépendre aussi d'aspects budgétaires et technico - industriels, du suivi à moyen terme d'un programme de coopération multinational et de circonstances politiques pouvant réduire, réorienter ou annuler, en tout ou en partie, lesdits programmes spatiaux militaires (réorientation stratégique des autres partenaires, restrictions budgétaires, divergences politiques, révision à la baisse du Plan à moyen terme militaire ...);*

- *Considérant comme acquis par l'argumentation développée ci-dessus que la dépendance aux satellites commerciaux ou militaires américains pourrait potentiellement poser question dans des moments particulièrement délicats où la demande nationale en images s'avérera urgente, prioritaire et non restrictive;*

- *Tenant compte par ailleurs de l'existence de verrous pour les Etats membres de l'UEO non membres participants à Hélios 1 (dont la Belgique) en matière d'acquisition de renseignements via le Centre UEO d'interprétation satellitaire de Torrejõn;*

- *N'ignorant pas qu'une participation à Hélios II devrait être fixée au prorata réel et modeste des besoins évalués dans le futur par les forces armées belges et les services de renseignements et dont le pourcentage ne devrait pas être supérieur à la part espagnole pour Hélios 1;*

- *Tenant compte, comme solution complémentaire (ou de substitut partiel pour des motifs pécuniaires) pour des demandes non prioritaires ou n'exigeant pas de résolution décimétrique, de l'existence du processus national de demande d'images auprès des alliés de l'OTAN pris nationalement (aéronefs et satellites nationaux), des commandes possibles à caractère national via Torrejõn, des accords d'ordre multilatéral entre le Conseil de l'UEO et Hélios 1 et des possibilités de commandes via les satellites commerciaux (en tenant compte, à chaque fois, des limites définies ci plus haut);*

- *Consciente que les récents accords de coopération belgo-français sur la force de projection aérienne et l'abonnement belge pour l'utilisation du système satellitaire de communications militaires français Syracuse participent d'une capacité de déploiement associée à d'éventuelles futures missions de maintien de la paix (en zone européenne, dans ses marges ou en Afrique), tout en révélant quelques lacunes en matière d'autonomie nationale de la Belgique dans le segment du renseignement satellitaire;*

Il peut être conclu de la façon suivante :

1. *La participation belge aux systèmes Hélios II / Horus peut apporter une meilleure qualité du renseignement au profit des forces armées belges et du gouvernement fédéral. Elle exprime le soutien à une européanisation future du renseignement et de l'autonomie stratégique de l'Europe, au soutien aux opérations communes, de la même manière que l'intégration de la Belgique dans le Corps franco-allemand a permis à ce dernier de bénéficier d'une dimension européenne plus affirmée.*

2. *Il est nécessaire pour la Belgique d'insister sur l'intégration des systèmes d'imagerie radar, jugés indispensables et complémentaires, afin de répondre aux conditions météorologiques difficiles de la zone tempérée et de l'Europe continentale et des zones équatoriales, de recouper les analyses électro-optiques, multispectrales et infrarouges, tout en permettant de contrer les leurres et détecter les supercheries.*

3. *En cas de participation au satellite Hélios II et à terme au satellite Horus, plusieurs démarches préalables devraient s'imposer :*

   - *la clarification préalable avec le pays "équipementier" à propos du contenu éventuel (et des éventuelles interférences) de la plate-forme satellitaire accueillant certains sous-systèmes militaires ultra-confidentiels;*

   - *la refonte des moyens d'analyses et d'interprétation nationaux afin de bien gérer les nouveaux flux d'informations satellitaires (formation d'analystes et de photos-interprètes, cellule ad hoc d'interprétation satellitaire);*

   - *l'acquisition comme les autres partenaires d'un centre de réception d'images digitales et d'un centre d'exploitation et d'interprétation national interconnectés;*

   - *la création d'une cellule de suivi mixte, intégrant des techniciens et des conseillers des Affaires étrangères et de la Défense.*

4. *Il sera indispensable de clarifier le processus de demande d'images entre les Affaires étrangères et la Défense nationale (sachant que déjà le budget national à la coopération spatiale de l'UEO est inscrit au budget des Affaires étrangères), la politique éventuelle de banque de données d'images satellitaires, les procédures de sécurité dans la diffusion des images interprétées ainsi que du contrôle d'authentification des images transférées au ministère des Affaires étrangères lorsque ce dernier doit alimenter sa réflexion, sa diplomatie ou ses interventions politiques et parfois préventives grâce à une imagerie fournie et interprétée par Evere.*

5. *La diplomatie belge sera attentive et volontariste en matière de Traité d'interdiction des armes anti-satellites, parallèlement au choix d'intégration dans des programmes satellitaires militaires intra-européens.*

6. *L'objectif final de la diplomatie belge sera de faire évoluer à terme les programmes Hélios II et Horus vers un système authentiquement européen intégré davantage à l'UEO, en faisant du système satellitaire d'observation une véritable "Force relevant de l'UEO" (FRUEO), au service de l'Union de l'Europe occidentale et, à plus long terme, du Centre de prévention des crises et d'alerte rapide de l'Union européenne dans un cadre moins restrictif.*"

4.2. Avis de Monsieur Roger Godechoul, directeur du Belgian Defence & Security Industry Group (B.D.I.G.) de FABRIMETAL

Au cours d'un entretien qui s'est tenu le 17 mars 1998, Monsieur Godechoul, colonel e.r., chargé des questions aérospatiales et de défense au B.D.I.G. a émis l'avis suivant :

"La capacité belge Hélios et Horus est la seule solution pour obtenir des informations sensibles en temps de crise. C'est une excellente décision du gouvernement. Parallèlement, l'accès à l'imagerie commerciale est également essentielle car l'interprétation s'appuie sur l'image en situation opérationnelle que l'on compare aux images en "bibliothèque" qui peuvent être commerciales, donc moins chères et en plus grand nombre. Les deux sources sont donc complémentaires".

5. CONCLUSIONS

Dans le contexte actuel d'après-guerre froide, les satellites sont appelés à jouer un rôle de plus en plus important en matière de prévention des conflits et de gestion de crises, parallèlement à leurs autres missions traditionnelles que sont la surveillance du respect des accords de réduction des armements et de désarmement et le soutien aux missions de combat.

Le besoin de disposer d'imagerie satellitaire est un complément d'informations essentiel pour le SGR, comme pour tout service de renseignement. Dans certains cas, les photos satellitaires peuvent constituer la seule source d'informations disponible.

Les sources satellitaires actuelles du SGR ont leurs avantages mais aussi beaucoup d'inconvénients, à savoir la dépendance de puissances étrangères et la lenteur de l'approvisionnement. En plus des possibilités existantes auprès de l'UEO et auprès des services américains, le SGR a exprimé le besoin d'avoir un accès direct et autonome à des images satellitaires surtout pour le soutien à des opérations où la Belgique agit et prend ses décisions seule dans un cadre national. A cette fin, le SGR envisage l'acquisition directe d'images satellitaires auprès de firmes commerciales à conditions que certaines conditions soient remplies sur les plans de la confidentialité des demandes, du respect de délais très courts en cas d'urgence, de la qualité technique des produits fournis (images non dégradées d'une résolution d'au moins un mètre).

La volonté du gouvernement de faire participer la Belgique au programme européen Hélios II est de nature à fournir au SGR l'accès confidentiel à des images de haute qualité et dans des délais assez courts, ce qui correspond à un de ses besoins.

Dans cette perspective, l'Etat-major des Forces armées a chargé un groupe de travail de la mise en place progressive d'une cellule d'analyse d'images satellitaires. Des membres du SGR participent à ce groupe de travail mais aucune décision n'a encore été prise concernant le rattachement et la dépendance hiérarchique de cette cellule par rapport au SGR.

6. RECOMMANDATIONS

Compte tenu des missions que la prochaine loi organique des services de renseignement et de sécurité attribue au SGR, et compte-tenu des besoins exprimés par ce service,

- le Comité R recommande d'accorder au SGR des possibilités d'accès rapide et autonome à des images spatiales de haute résolution.

Faisant siens les avis de Messieurs Godechoul et Dumoulin et, moyennant la prise en compte des éléments pondérateurs, des contraintes et des limites indiquées par ce dernier,

- le Comité R approuve la recherche d'une participation de la Belgique au programme européen Hélios II.

Le Comité R recommande également :

En tenant compte des avantages et des inconvénients de chacune d'elles, de ne pas négliger pour autant d'autres sources d'images spatiales qui, actuellement ou dans un futur proche, sont:

- les services de renseignement des pays alliés;

- les images acquises auprès de firmes commerciales dont la qualité se rapproche de plus en plus de celle des images des satellites militaires;

- les petits satellites d'observation dont les développements peuvent constituer une alternative intéressante aux coûts des satellites actuels, notamment dans le domaine des satellites radars. A cet égard, on ne peut négliger les projets en cours ni les capacités de recherche et de développement des entreprises belges.

Que le recours au Centre satellitaire de l'UEO soit réservé à la formation, à l'entraînement, à l'information de base et aux missions décidées dans l'intérêt commun des pays européens, là où la coopération internationale en la matière devrait marquer le début de l'abandon de la politique habituelle d'échange d'informations entre services de renseignement, basée sur le "donnant-donnant".

Le Comité R recommande en outre de considérer les images spatiales :

- comme un moyen d'aide à la prise de décisions politico-militaires (et non exclusivement militaires) en vue de la prévention des conflits et de la gestion de crises quelle que soient leurs natures (conflits internationaux, guerres civiles, catastrophes environnementales, etc ...);

- comme un moyen complémentaire par rapport aux autres méthodes habituelles de recueil du renseignement qui ne doivent pas non plus être négligées pour la cause.

Le Comité R recommande enfin de mettre en place un centre d'analyse d'images satellitaires indépendant et de former du personnel qualifié à cette fin, ce qui signifie la mise en oeuvre de moyens matériels et humains adéquats.

A cet égard, le Comité R recommande :

- que cette cellule d'analyse dépende du SGR, ou qu'elle soit tout au moins en contact étroit avec ce service, de manière à ce qu'elle puisse bénéficier de ses autres sources d'information;

- que le personnel qualifié de cette cellule soit constitué à part égale de militaires et de civils, ces derniers devant alors bénéficier d'un statut stable ou tout-au-moins d'un contrat à durée indéterminée au sein de cette nouvelle structure.

Le Comité R attire en outre l'attention du SGR et de la Sûreté de l'Etat sur l'intérêt que peuvent présenter pour leurs missions les systèmes de radio-positionnement par satellites (global positionning system, Glonass, et autres futurs systèmes européens). L'usage de ces systèmes à des fins de filatures devra cependant être réglementé par la loi.

7. SOURCES D'INFORMATIONS UTILISÉES POUR L'ÉTUDE SUR LES SATELLITES

Traités internationaux :

- le "traité de l'espace" du 27 janvier 1967;
- le traité du 26 mai 1972 sur la limitation des missiles anti-balistiques;
- le traité du 26 mai 1972 sur la limitation des armes offensives stratégiques;
- le Document du 19 septembre 1986 de la conférence de Stockholm sur les mesures de confiance et de sécurité et sur le désarmement en Europe;
- le traité du 8 décembre 1987 sur l*élimination des forces nucléaires à portée intermédiaires;
- le traité du 19 novembre 1990 sur les forces conventionnelles en Europe;
- le traité d'Helsinki du 24 mars 1992 sur le régime "ciel ouvert" ratifié par la loi du 15 mai 1995 (Moniteur belge 12 décembre 1995);
- le traité sur l'interdiction complète des essais nucléaires signé à New York le 24 septembre 1996;

Publications du Parlement belge :

- Exposé du ministre de la Défense nationale et débat devant la commission des Affaires étrangères du Sénat; 12 février 1996, session 95/96, 1 - 249 / 1.
- Question n° 71 de M. Anciaux (Sénat) du 21 juin 1996 au ministre de l'Economie : *utilisation de satellites de navigation permettant de localiser des véhicules - gebruik van navigatiesatellieten waarmee voertuigen kunnen worden gelokaliseerd.*
- Question n° 236 de M. Jan Eeman (Chambre des représentants) du 6 mai 1997 au ministre des Affaires étrangères : *OTAN et UEO - contribution financière - NAVO en WEU - financiële bijdrage.*
- Introduction du ministre de la défense nationale au projet de loi organique des services de renseignement et de sécurité - 8 octobre 1997 (638 / 14 - 95 / 96, pp. 3 à 6)
- Question n° 430 de M. Alfons Borginon du 11 décembre 1997 (Chambre des représentants) au ministre de la Défense nationale : *participation belge au programme satellite "Hélios 2".*
- Question orale de M. Pierre Lano au ministre de la politique scientifique sur les investissements du gouvernement fédéral dans la station spatiale ISS (n° 753 - annales - COM 10.03.1998).

Documents et avis officiels du gouvernement belge :

- Communiqué de presse du ministère des Affaires étrangères du 3 octobre 1997 (Belga) : “Argentinie en België gaan samenwerken in de ruimte”.

- Communiqué de presse du Ministère de la Défense nationale du 23 janvier 1998 à propos de la tranche 1998 du Plan à moyen terme approuvé par le Conseil des ministres du 23 janvier 1998.

- Communiqué de presse du Conseil des ministres du 6 mars 1998.

Publications des Services fédéraux des Affaires scientifiques, techniques et culturelles (S.S.T.C).

- Avis officiel de participation au programme “Observation de la terre par satellite” du plan d’appui scientifque à une politique de développement durable - Moniteur Belge 03/08/1996.

- Brochure de présentation des missions et activités des services fédéraux des affaires scientifiques, techniques et culturelles (services du Premier ministre) - 1997.

- Lettre d’information “Space connexion” contenant des informations sur les réalisations récentes dans le domaine spatial.

Publications de l’Assemblée nationale et du Sénat français.

- Rapport n° 3030 d*Arthur Paecht fait au nom de la Commission des finances, de l*économie générale et du plan sur le projet de loi de finances pour 1997, annexe 40, Défense. Equipement, AN (10 octobre 1996);

- Avis n° 3033 de Jean-Michel Boucheron fait au nom de la Commission de la Défense nationale et des forces armées sur le projet de loi de finances pour 1997, tome V, Défense. Espace et Communication, AN (10 octobre 1996);

S Avis n ° 89 de Jean Faurre fait au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur le projet de loi de finances pour 1997 adopté par l*Assemblée nationale, tome IV, Défense-nucléaire-espace et services communs, Sénat (21 novembre 1996);

- Avis n° 308 de Bernard Grasset au nom de la Commission de la Défense nationale et des forces armées sur le projet de loi de finances pour 1998, tome III. Défense. Espace, communications et renseignement, Assemblée nationale, Paris, 9 octobre 1997;

- Rapport n° 305 de Jean-Michel Boucheron, au nom de la Commission des Finances, de l*économie générale et du plan sur le projet de loi de finances pour 1998, annexe n^0 40, Défense, AN, Paris, 9 octobre 1997.

Publications de l'Agence Spatiale Européenne (ESA) :

- Etude sur les évolutions du cadre sécuritaire européen, ses implications dans le domaine spatial et les orientations pour l*Agence spatiale européenne (ESA), ESA, Division des relations internationales, juin-septembre 1995;

- ERS-1 : 500 jours en orbite;

- de ERS-1 à ERS-2;

- les programmes de l'ESA, BR - 14 août 1995;

- rapport annuel de 1996;

- global Navigation Satellite System (European GNSS office);

- l'Europe dans l'Espace : vue d'ensemble des activités de l'ESA (janvier 1997);

- Intellectuel property rights and space activities in Europe (février 1997);

Documents et rapports de l'Union de l'Europe Occidentale.

- Wilkinson, Les utilisations militaires de l'espace, document 993, Assemblée de l'UEO, Paris, 8 novembre 1984;

- "Le défi spatial pour l'Europe", colloque de l*Assemblée de l*UEO, Munich, 18-20 septembre 1985;

- Fourré, Vérification: une future agence européenne de satellites, document 1159, Assemblée de l*UEO, Paris, 3 novembre 1988;

- Malfatti, "Aspects scientifiques et techniques de la vérification par satellite du contrôle des armements", document 1160, Assemblée de l*UEO, Paris, 7 novembre 1988;

- "Les satellites d*observation - Un instrument européen pour la vérification du désarmement", Colloque de l*Assemblée de l*UEO, Rome, 27 et 28 mars 1990;

- Valleix, Le développement d*un système européen d*observation spatiale, document 1436, Assemblée de l*UEO, Paris, 9 novembre 1994;

- "Pour un système européen d*observation spatiale", Colloque de l*Assemblée de l*UEO, San Agustin, 24-25 mars 1995;

- Lenzer et Valleix, Pour un système européen d*observation spatiale, document 1454, Assemblée de l*UEO, Paris, 2 mai 1995;

- Lenzer, l*UEO et Hélios 2, document 1525, Assemblée de l*UEO, Paris, 14 mai 1996;

- “Une politique européenne de renseignement” - rapport présenté le 3 juin 1996 à l’assemblée de l’UEO au nom de la Commission de défense (document 1517);

- Satellite Centre satellitaire, Plaquette du Centre satellitaire de Torrejon, Madrid, s.d;

- “L’UEO et l’utilisation de moyens satellitaires dans la prévention et la gestion des risques majeurs” - rapport présenté le 12 mai 1997 à l’assemblée de l’UEO au nom de la Commission technique et aérospatiale (document 1570).

- Séminaire sur le “Développement d*une politique européenne du renseignement”, Institut d*études de sécurité de l*UEO, Paris, 16 juin 1997;

- “La coopération transatlantique dans le domaine de la défense antimissile européenne” rapport présenté à l’Assemblée de l’UEO au nom de la commission technique et aérospatiale; (document 1588 - 4 novembre 1997);

- Colonel Dillen, Le centre de situation UEO. Finalités et structures, UEO, Bruxelles, 17 novembre 1997;

- “Déclaration d’Erfurt” du Conseil des ministres de l’UEO, publiée à l’issue de leur réunion du 18 novembre 1997.

- Recommandation n° 619 de l’assemblée de l’UEO sur le rôle de l’Europe dans les Balkans en matière de prévention et de gestion des crises (43ème session ordinaire - du 1er au 4 décembre 1997).

- Recommandation n° 623 de l’assemblée de l’UEO sur le Comité militaire de l’UEO (43ème session ordinaire - du 1er au 4 décembre 1997).

- Conseil des ministres - réunion des 11 et 12 mai 1998 - Déclaration de Rhodes.

Presse quotidienne :

Le Monde :

- 31/10/91- 13/02/92 -26/06/92 - 29/09/93 - 05/11/93 - 12/09/94 - 12/10/94 - 16/10/94 - 19/10/94 - 15/01/95-07/04/95 - 17/04/95 - 08/07/95 - 06/12/95 - 20/12/95 - 28/12/95 -10/07/95 - 10/01/96 - 25/01/96 - 02/05/96- 04/10/97 - 08/10/97 - 15/10/96 - 12/02/97 - 22/04/97 - 18/09/97 - 12/10/97 - 21/10/97 - 23/10/97 - 25/10/97-14/11/97 - 29/11/97 - 14/12/97 - 18/12/97 - 24/12/97 - 26/12/97 - 29/12/97 - 14/02/98 - 03/03/98 - 06/04/98 - 11/04/98 - 14/05/98 - 21/05/98

Le Soir :

- 30/01/95 - 07/04/95 - 09/07/95 - 03/10/97 - 30/10/97- 07/02/98 - 05/02/98 - 07/03/98 - 13/04/98 - 21/04/98-14/05/98

La Libre Belgique : 04/10/97 - 17/10/97 - 19/11/97 - 28/11/97

La Dernière Heure : 15/10/97

L'Echo : 27/11/97 - 28/11/97

La Nouvelle Gazette : 10/02/98

De Standaard : 28/11/97 - 02/03/98

Het Nieuwsblad : 27/02/98

De Gazet Van Antwerpen : 15/12/97

Libération : 13/02/92 - 06/09/95

Le Figaro : 12/10/94

Die Welt : 30/11/94

Presse périodique :

Nouvelles atlantiques : 28/10/94 - 19/01/95 - 29/3/95 - 12/7/95

Air et Cosmos : 01/12/91 - 27/04/92 - 13/07/92 - 24/07/92 - 01/02/93 - 22/02/93 - 24/05/93 - 20/12/93 - 09/05/94 - 04/07/94- 30/09/94 - 04/11/94 - 20/01/95 - 14/04/95 - 21/04/95 - 14/07/95 - 15/12/95 - 12/01/96 - 08/03/96 - 12/04/96 - 18/10/96 - 17/01/97 - 28/03/97 - 18/10/96 - 31/01/97 - 05/09/97 - 31/10/97 - 28/11/97 - 12/12/97- 19/12/97- 09/01/98 - 16/01/98 - 23/01/98

Jane's Defence Weekly : 24/11/90 - 21/09/91 - 16/11/91 - 05/11/94 - 10/12/94 - 29/04/95 - 17/06/95 - 05/11/97 - 15/10/97

Jane's News Brief : 29/10/97

TIME : 10/11/97

Le Monde du Renseignement, publication Indigo, Paris :

222 (28/07/93) - 232 (12/01/94) - 240 (04/05/94) - 256 (19/01/95) - 258 (16/02/95) - 259 (02/03/95)- 261 (30/03/95) - 263 (27/04/95) - 266 (15/06/95) - 267 (29/06/95)- 269 (27/07/95) - 272 (28/09/95)- 274 (26/10/95) - 277 (07/12/95) - 278 (21/12/95) - 282 (22/02/96) - 283 (07/03/96) - 288 (23/05/96)- 290 (20/06/96) - 294 (05/09/96) - 308 (27/03/97) - 312 (29/05/97) - 313 (12/06/97) - 315 (10/07/97)- 320 (09/10/97) - 325 (18/12/97) - 326 (08/01/98) - 328 (05/02/98) - 329 (19/02/98) - 335 (21/05/98)

Le Vif / L'express : 25/11/94 - 18/07/97 - 07/11/97-

Vox : n° 9631 - 9640 - 9738 - 9801

Science et vie : n° hors série d'octobre 1984 et mars 1996;
n° 959 (août 1997) - n° 965 (février 1998);

International Defence Review : juin 1988 - juin 1990 - avril 1991 - mai 1991 - août 1991 - janvier 1992 - juillet 1992 - janvier 1995- mai 1995 - septembre 1995 -

Defense News : 25/04/94 - 21/11/94 - 16/01/95 - 27/11/95 - 24/06/96

Armées d*aujourd'hui : mai 1991 - mai 1992 - avril 1993 - juillet 1995 -

Aviation Week and Space Technology : 08/04/91 - 17/07/95 - 27/11/95 - 18/12/95 - 06/05/96 - 17/06/96 - 01/09/97 - 22/09/97 - 03/11/97- 12/01/98

Defense and Technologie International : septembre 90

Défense et armement & Héraclès International octobre 1988 - février 1989 - juillet-août 1990, septembre 1992

Avianews international : avril 1989 - juillet 1990 - septembre 1990 - mai 1991 septembre 1991 - décembre 1991

Trust and Verify : juin 1991-

Revue de Défense nationale : décembre 1985 - mai 1991 - juillet 1991 - mars 1996 - mai 1997- janvier 1998

Eurostratégie : décembre 1990

Relations internationales et stratégiques : l^{er} trimestre 1991 - hiver 1992 - été 1993

Air fan : août 1992

Space News : octobre 1993 - août 1994

TTU : 13 octobre 1994

Arms Control Today : septembre 1995 - décembre 1995 - janvier 1996 - juillet 1996- août 1996 - octobre 1997

The Bulletin of the Atomic Scientist : septembre/octobre 1994, juillet - août 1997

Damoclès : novembre 1991

Pour la science : mai 1985

Stratégique : n°44 (1989) - n° 47 (1990)

La Recherche : janvier 1974 - février 1982

Revue de l'OTAN : novembre-décembre 1997

Le débat stratégique : novembre 1995 - mai 1996 - juillet 1996

Athéna : juin 1995 - octobre 1996 - mai 1997

Problèmes politiques et sociaux : n° 521-522, 18 octobre 1985

The Letter Eucosat : janvier 1998

Rapport de ISIS : avril 1996

Défense, IHEDN : septembre 1996

RUSI Journal : avril 1997.

Ouvrages spécialisés :

- "Dictionnaire de géopolitique", Pierre Lacoste, Flammarion, 1993;
- "International law and spionage", John Kish (University of Kent, UK), éditions Martinus Nijhoff;
- "Guerre et contre-guerre", Alvin et Heidi Toffler - éditions Fayard - 1994;
- "Au coeur du secret", Claude Silberzahn, ancien chef de la DGSE, France - éditions Fayard - 1995;
- "Secret Intelligence and Public Policy - a dilemma of democracy", Pat M. Holt - CQ Press - 1995;
- "Encyclopédie du renseignement et des services secrets", Jacques Baud, éd.Lavauzelle, 1997;

Etudes, rapports :

- La guerre des satellites : enjeux pour la communauté internationale - rapport de l'Institut français des relations internationales préparé sous la direction de Pierre Lellouche - 1987;
- Colloque international sur la militarisation de l*espace extra-atmosphérique, éditions Bruylant, Bruxelles, 1988
- Livre blanc sur la Défense., Paris, 1994

- Collectif, La guerre secrète moderne, Bordas, 1983

- Collectif, L*exploration de l*espace, Bordas, 1981

- The Military Balance 1997-1998, IISS, 1997.

- Collectif, Satellites for arms control and crisis monitoring, Sipri, 1987

- André Dumoulin et Eric Remacle, L'Union de l'Europe occidentale. Phénix de la défense européenne, Bruylant (parution en mars 1998)

- Collectif, Verification Report, éditions 1991, 1992 et 1995

- L'UEO et la présidence belge du second semestre 1996 - courrier hebdomadaire du CRISP, n° 1560 - 1561 - 1997;

- Collectif, Sipri Yearbook, éditions 1995,1996 et 1997

- Collectif, La vérification d*ici l*an 2000, Affaires extérieures et commerce extérieur, Canada, 1991

- Collectif, Etat des accords multilatéraux en matière de désarmement et de contrôle des armements, Nations unies, 1987

- Collectif, Verification of a Comprehensive Test Ban Treaty from Space: A Preliminary Study, Unidir, 1994

- Collectif, Technical Problems in the Verification of a Ban on Space Weapons, Unidir, 1993

- Collectif, Access to Outer Space technologies: Implications for International Security, Unidir, 1992

- Collectif, La vérification des accords sur le désarmement et la limitation des armements: moyens, méthodes et pratiques, Unidir, 1991

- Collectif, Vérification du désarmement ou de la limitation des armements: instruments, négociations, propositions, Unidir, 1994

- Collectif, La résolution 687 (3 avril 1991) du Conseil de sécurité dans l*affaire du Golfe: problèmes de rétablissement et de garantie de la paix, Unidir, 1992.

Publication du Groupe de recherche et d'information sur la paix et la sécurité (GRIP).

- Eléments pondérateurs à la frappe nucléaire stratégique (publication n^0 135/136 - juillet-août 1989);

- Vers un satellite européen de vérification du désarmement (publication n^0 122-123, juin-juillet 1988);

- La vérification des accords de maîtrise des armements (publication n^{0}105, janvier 1987);

- Annuaire memento défense-désarmement, éditions 1989 et 1990;

- Essais nucléaires - fin de partie - le CTBT (traité sur l'interdiction complète des essais nucléaires) : son histoire - les enjeux politiques et stratégiques - la vérification (publication n° 214);

- L'Europe et la sécurité internationale - mémento défense désarmement 1997 (Publication n° 218 / 221);

Sites Internet :

- http://www.fas.org/spp/military/program/index.html
- http://ls7pm3.gsfc.nasa.gov
- http://www.fleximage.fr/communic/9302f.htm (Air & Cosmos 01/02/93)
- http://www.ofd.ac.at/ofd
- http://www.spot.com/anglaise
- http://www.spotimage.fr
- http://www.aerospatiale.fr/produits/espace
- http://www. aerospatiale.fr/produits/espace/eutels2a.htm
- http://solar.rtd.utk.edu/-mwade/project/eutelsat.htm
- http://webeecs.ent.ohiou.edu/avn
- http://sgiot2.wwb.noaa.gov/COASTWATCH
- http://www.quebecscience.qc.ca/radarsat.htm
- http://www.eurimage.it/Products/KVR_1000.html
- http://www.afa.org
- http://www.hq.nasa.gov/osf/1996
- http://www.nro.odci.gov/background.htm
- http://www.nro.odci.gov/corona/pioneers.htm
- http://www.odci.gov/ic
- http://www.lmco.com/contact
- http://www.spacevest.com/companies
- http://www.autodesk.com/solution/gis/geodysey/spaceimg.htm
- http://www.glasnet.ru/~kiberso/list1_e.htm
- http://www.esa.int/esa/descrip/descrip.htm
- http://www.spaceimaging.com
- http://www.eucosat.com
- http://www.digitalglobe.com

CHAPITRE 6 : RAPPORT CONCERNANT UNE DÉNONCIATION DE NON-APPLICATION PAR LA SÛRETÉ DE L'ETAT DE L'ARTICLE 33, ALINÉA 2 DE LA LOI DU 18 JUILLET 1991 ORGANIQUE DU CONTRÔLE DES SERVICES DE POLICE ET DE RENSEIGNEMENTS

1. PROCÉDURE

Aux termes de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, les services de renseignement transmettent d'initiative au Comité R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services. Le Comité R et le Service d'enquêtes des services de renseignement ont le droit de se faire communiquer les textes qu'ils estiment nécessaires à l'accomplissement de leur mission.

Depuis 1994, le Comité R fait rapport sur la manière dont les services de renseignement se sont acquittés de cette obligation légale au cours de l'année écoulée. En date du 25 septembre 1997, le Comité R a décidé d'ouvrir une enquête permanente à ce sujet. Le Comité R estimait que cette initiative répondait parfaitement à sa mission légale et à l'esprit de la loi de 1991.

Les ministres compétents et le Parlement en ont été averti par lettres du 1er octobre 1997.

Le 17 octobre 1997, Messieurs Swaelen et Delathouwer, présidents des commissions chargées du suivi parlementaire du Comité R lui ont demandé de mettre fin à cette enquête (voir pt. 4).

Malgré cette lettre, le Comité R a décidé de poursuivre son enquête en lui retirant toutefois la qualification de "permanente" qui, effectivement ne correspond pas à la procédure prévue par la loi du 18 juillet 1991. Cette décision était motivée par la réception d'une dénonciation au Comité R (voir pt. 5).

La présente enquête a été clôturée le 22 décembre 1997 par l'approbation du présent rapport.

2. LES DOCUMENTS TRANSMIS D'INITIATIVE

Entre le 26 juin 1997 [(1)] et le 22 décembre 1997, l'administrateur général de la Sûreté de l'Etat a transmis d'initiative au Comité R six notes internes.

3. LES DOCUMENTS TRANSMIS SUR DEMANDE DU COMITÉ R

3.1. Dans le cadre de sa mission de surveillance générale

Par lettre du 4 septembre 1997, le Comité R a prié l'administrateur général de la Sûreté de l'Etat de lui transmettre quatre ordres de service qui, à son estime, ne lui avaient pas été communiqués d'initiative.

Après vérification, le Comité R a reconnu avoir réclamé un des documents par erreur (la note de service n° 428); celui-ci lui avait bien été adressé d'office et en temps voulu. Le Comité R a bien reçu les trois autres documents qu'il réclamait par courrier du 9 septembre 1997.

3.2. Dans le cadre de certaines enquêtes

Dans le cadre de certaines enquêtes, le Comité R a sollicité et reçu les documents suivants de la Sûreté de l'Etat :

- le document de présentation de la Sûreté de l'Etat établi dans le cadre de la publicité active de l'administration (loi du 11 avril 1994) dans le cadre de l'enquête sur les devoirs de secret des services de renseignement - ce document date du 27/08/97.

- les décisions ministérielles des 20 octobre 1976, 3 octobre 1986 et 14 octobre 1986 et par lesquelles la Sûreté de l'Etat, alors branche de l'Administration de la Sûreté Publique du ministère de la Justice avec l'Office des Etrangers, avait été chargée d'accorder respectivement à des ressortissants belges non domiciliés en Belgique l'autorisation d'importer ou de porter, dans le pays, des armes;

- la directive 91/477/CEE du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes;

---

(1) Date du dernier envoi de documents par la Sûreté de l'Etat mentionnée dans le rapport d'activités du Comité pour l'année 1997.

- la note de service du 16 mars 1992 qui réglait l'application de la nouvelle réglementation sur les armes à l'égard de la Sûreté de l'Etat;

- la décision ministérielle du 7 janvier 1993 par laquelle fut décidé le transfert de la compétence "armes" de l'Office des Etrangers à l'égard des étrangers non domiciliés en Belgique à la Sûreté de l'Etat.

- la circulaire ministérielle coordonnée du 30 octobre 1995 relative à l'application des dispositions légales et réglementaires sur les armes. Ces documents ont été demandés dans le cadre de l'enquête sur les compétences de la Sûreté de l'Etat en matière d'armes.

4. LA DISCUSSION DES CONCLUSIONS DU RAPPORT DE 1997

La conclusion du chapitre 3 de la première partie du titre II du rapport d'activités de 1997 (page 79) mentionnait un malentendu persistant entre le Comité R et la Sûreté de l'Etat à propos de l'interprétation de l'article 33, alinéa 2 de la loi du 18 juillet 1991.

Le Comité R regrettait que les autorités responsables n'aient pris aucune mesure pour résoudre ce problème d'interprétation de la loi.

Le 17 octobre 1997, Messieurs Swaelen et Delathouwer, présidents des commissions chargées du suivi parlementaire du Comité R lui ont adressé la lettre suivante :

"Madame la Présidente,

Vous nous avez fait savoir que le Comité R vient d'ouvrir une enquête "permanente" concernant l'application de l'article 33 de la loi du 18 juillet 1991. Cette initiative appelle plusieurs observations. Tout d'abord, le procédé de l'enquête "permanente" ne nous parait pas conforme à l'esprit de la loi de 1991.

Ensuite, nous avions clairement indiqué, lors de notre réunion du 23 septembre 1997, qu'en ce qui nous concerne, l'interprétation que nous avions donnée de l'article 33 le 28 avril 1996, devrait pouvoir éviter que de nouvelles difficultés majeures ne surgissent à ce sujet entre le Comité R et la Sûreté de l'Etat.

Dès lors, si un malentendu persistant subsiste, cela n'est certainement pas dû au fait que les autorités responsables n'auraient pris aucune mesure pour résoudre ce problème d'interprétation de la loi, contrairement à ce que vous écrivez dans votre rapport d'activités 1997.

Nous constatons par ailleurs que les points de vue des commissions parlementaires d'accompagnement et de l'administrateur de la Sûreté de l'Etat y sont incorrectement rendus.

En conclusion, nous estimons qu'il doit être mis fin à l'enquête "permanente" sur l'interprétation de l'article 33 ainsi qu'à la polémique inutile dont elle fait l'objet depuis trop longtemps déjà.

Veuillez agréer, ...".

Effectivement, la conclusion du Comité R était en contradiction avec l'exposé du problème dans le rapport.

Cet exposé avait été rectifié suite à la réunion avec les commissions parlementaires tenue le 23 septembre 1997[(2)]

Ceci résulte du fait qu'au moment de sa rédaction, le Comité R n'avait pas encore eu connaissance de la position des commissions chargées de l'accompagnement parlementaire des Comités P et R.
Le Comité R assume la responsabilité de cette erreur : il confirme que les commissions lui ont répondu ce qui suit : *"De commissies zijn van oordeel dat voormeld artikel niet extensief moet worden uitgelegd. Uit de parlementaire voorbereiding (inzonderheid het antwoord van de minister in stuk Senaat nr 1258/2-90/91, bl. 57) blijkt duidelijk welke draagwijdte volgens de wetgever aan het artikel toekomt".*

[Traduction libre : "Les commissions estiment que l'article précité ne doit pas être interprété de manière extensive. Les travaux préparatoires parlementaires (en particulier la réponse du ministre au Sénat mentionnée dans la pièce n° 1258/2-90/91, page 57 : *"Le Ministre répond qu'il appartiendra aux services de renseignement d'apprécier si un document règle le comportement des membres de ces services. Le Ministre renvoie à l'examen de l'article 9. Il cite à titre d'exemple les directives réglant les filatures, l'utilisation de véhicules, la façon de s'adresser aux personnes, la mise en oeuvre d'instruments techniques d'observation ou d'écoute. Il est clair qu'en cas de doute, il y a lieu de communiquer les documents au Comité)* font clairement apparaître la portée que le législateur accorde à cet article"].

5. LA DÉNONCIATION PARVENUE AU COMITÉ R

Un membre a reçu d'une personne, qui désirait garder l'anonymat, copie d'une note de service de la Sûreté de l'Etat; ce document semblait dater de mai 1997; il est relatif à la manière dont les rapports internes doivent être rédigés dans ce service. Le membre en question a fait vérifier qu'il s'agissait bien d'un document interne à la Sûreté de l'Etat mais il ne put dire s'il s'agissait d'un projet de note ou d'une note déjà en application. En tout état de cause, il s'agissait bien d'un document réglant le comportement des membres des services de renseignement.

(2) Rapport d'activité 1997 p. 76 voir point 2.4.

Après discussion, le Comité R décida de traiter ce cas comme une dénonciation d'une personne désirant conserver l'anonymat (articles 48 et 49 du règlement d'ordre intérieur) et de poursuivre l'enquête sur l'application de l'article 33, alinéa 2 de la loi organique, malgré l'injonction des présidents des commissions d'accompagnement. Il fut convenu que l'identité du dénonciateur ne serait connue que du membre ayant reçu la dénonciation.

Ignorant s'il s'agissait d'un projet de note interne ou d'un document déjà en vigueur, le Comité R décida d'attendre et de ne pas réagir sur ce cas avant d'avoir reçu la réponse de l'administrateur général de la Sûreté de l'Etat à sa proposition de tenir un inventaire des notes de service (voir point 6).

6. ECHANGES DE VUES ENTRE LA SÛRETÉ DE L'ETAT ET LE COMITÉ R

Dans son rapport d'activités de 1997, le Comité R se demandait pourquoi il avait été mis fin à la numérotation des notes et ordres de service de la Sûreté de l'Etat.

Dans sa lettre du 9 septembre 1997, l'administrateur général de la Sûreté de l'Etat a expliqué qu'il avait été mis fin à cette numérotation pour des raisons pratiques. Dans sa lettre du 15 septembre 1997, le Comité R a demandé à connaître ces raisons pratiques. Il a aussi demandé si un inventaire de ces documents était tenu par la Sûreté de l'Etat. Si oui, le Comité R désirait en obtenir une copie. Dans une lettre adressée le 22 septembre 1997 au ministre de la Justice, le Comité R lui a proposé un échange de vues pour résoudre cette question. Le 3 octobre 1997, le ministre a simplement répondu : *"je ne vois pas d'objection à la publication de ce texte".*

Le 25 septembre 1997, l'administrateur général de la Sûreté de l'Etat déclare que *"toutes les notes importantes sont transmises scrupuleusement* (au Comité) *et qu'il n'y a, par conséquent, aucun problème en la matière".* Il confirme cependant qu'un inventaire des notes de service n'est pas tenu dans son service. Il explique aussi que toutes les notes ne sont pas conservées de façon centralisée, certaines ayant trait à des choses anodines, et que c'est d'ailleurs une raison qui est à la base de l'abandon du système de numérotation.

Au cours de sa réunion du 10 octobre 1997, le Comité R a effectivement estimé que les documents internes de la Sûreté de l'Etat ayant trait à des choses anodines telles que l'achat de crayons, le nettoyage des tapis, etc ... ne devaient pas lui être systématiquement adressés. Le Comité R a estimé cependant qu'il était le seul à pouvoir juger de l'intérêt que représentait pour lui une note ou un document interne à la Sûreté de l'Etat.

C'est pourquoi, le 20 octobre 1997, le Comité R a proposé à l'administrateur général de la Sûreté de l'Etat de lui faire parvenir périodiquement un inventaire tenu à jour des notes et ordres de service qui y sont en vigueur avec un sommaire de ces documents. Sur base de cet inventaire, le Comité serait en mesure d'indiquer les documents qu'il estime utile de recevoir.

Se référant à cette proposition, l'administrateur général de la Sûreté de l'Etat propose le 23 octobre 1997 au Comité R d'organiser un échange de vues sur base de la décision prise en cette matière par les commissions parlementaires d'accompagnement.

Le 25 novembre 1997, il fit savoir par écrit qu'il acceptait la proposition du Comité R et adressa une première liste reprenant les notes de service à partir du 26 juin 1997.

La mise en oeuvre de cet accord fut discutée entre le Comité et l'administrateur général de la Sûreté de l'Etat au cours d'une réunion tenue le 2 décembre 1997 au siège du Comité R : une liste chronologique indiquant la date et l'objet de chaque note de service sera envoyée au Comité trois fois par an.

Au cours de la même réunion, il fut aussi question de la dénonciation parvenue au Comité : le document fut présenté à l'administrateur général de la Sûreté de l'Etat. Celui-ci reconnut qu'il s'agissait bien d'une note de service en vigueur dans son service. Il déclara qu'il avait estimé que ce document ne présentait pas à ses yeux une importance suffisante pour être envoyé au Comité R mais que si celui-ci le lui avait demandé, il n'aurait eu aucune objection à le lui transmettre. Il fut répondu que le Comité ne pouvait être en mesure de demander la production d'un document dont il ignorait l'existence.

Le Comité R et l'administrateur général de la Sûreté de l'Etat ont convenu que la tenue d'un inventaire permanent des notes de service et sa communication au Comité R était de nature à permettre une application raisonnable de l'article 33, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, ainsi qu'un contrôle efficace.

C. A L'INITIATIVE DU SERVICE D'ENQUETES

CHAPITRE 1 : RAPPORT DE L'ENQUETE SUR LES CARTES DE SERVICES DE LA SURETE DE L'ETAT ET DU SGR

1. PROCÉDURE

Appliquant l'article 47 de son règlement d'ordre intérieur, le Comité R a décidé le 7 mars 1996 d'autoriser la poursuite de cette enquête qui avait été ouverte d'initiative par le chef du Service d'enquêtes, ceci en application des articles 1er et 40, alinéa 1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le 14 mars 1996, en application de l'article 43 alinéa 1er de la loi organique du 18 juillet 1991, les ministres compétents ont été informés par le chef du Service d'enquêtes qu'une enquête était ouverte sur les cartes de services utilisées par les membres du personnel de la Sûreté de l'Etat d'une part, du SGR d'autre part.

Le 22 avril 1996, en application de l'article 46, alinéa 3 du règlement d'ordre intérieur, les présidents de la Chambre des représentants et du Sénat ont été informés qu'une enquête était en cours sur certains aspects du fonctionnement des services de renseignement.

Le Service d'enquêtes a remis deux rapports d'enquête au Comité R, le premier le 25 février 1997, le second le 30 avril 1997.

Le Comité R s'est adressé au secrétaire général du ministère de la Justice les 21 mai et 20 juin 1997 pour obtenir quelques explications complémentaires. Ce haut fonctionnaire a fourni les explications demandées par le Comité R dans sa lettre du 24 juillet 1997.

Une apostille complémentaire a aussi été adressée au Service d'enquêtes le 26 juin 1997. Les questions posées ont été adressées à l'Administrateur général de la Sûreté de l'Etat le 1er juillet 1997; la réponse est parvenue le 13 août 1997. Le rapport du Service d'enquêtes a été déposé le 5 septembre 1997.

Le Comité R a approuvé en date du 2 octobre 1997 le rapport d'enquête établi.

Il a été tenu compte pour la publication de ce rapport de la remarque formulée par le Ministre de la Justice.

2. MOTIF ET OBJET DE L'ENQUÊTE

Il s'agit donc pour le Service d'enquêtes, confronté le cas échéant à une plainte d'un particulier au sujet d'agissements imputés à un membre d'un service de renseignement (soit Sûreté de l'Etat, soit SGR) d'être en mesure de déterminer si cette personne est effectivement membre d'un de ces services ou un imposteur (auteur éventuel d'un des crimes et délits prévus aux chapitres IV (section 2) et VI du titre III du livre II du code pénal - *"des crimes et délits contre la foi publique - des faux commis dans les passeports, ports d'armes, livrets, feuilles de route et certificats"*) .

Après délibération le 7 mars 1996, le Comité R a estimé qu'une telle enquête trouvait bien son fondement dans l'article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements. Cet article donne notamment comme missions au Comité R de garantir la protection des droits que la Constitution et la loi confèrent aux personnes et d'assurer l'efficacité des services de renseignement.

Le Comité R a donc décidé d'autoriser cette enquête tout en précisant son objet comme suit :

1. vérifier quelles sont les cartes de services existantes pour les différentes catégories du personnel des services de renseignement et obtenir un spécimen de chacun de ces documents;

2. quelles sont les bases légales et réglementaires à ces cartes de services, en particulier lorsqu'elles contiennent des mentions à l'égard de tiers;

3. examiner la nécessité et l'emploi de ces cartes.

3. L'INTÉRÊT PARLEMENTAIRE POUR LE PROBLÈME

Le Comité R n'a relevé qu'une seule question parlementaire relative aux cartes d'identité de service et/ou de légitimation des militaires.

Il s'agit de la question n° 284 posée le 24 mars 1989 au ministre de la Défense nationale par monsieur Lefeber (SP); elle comporte les volets suivants :

1. *"Quels militaires reçoivent une carte d'identité de service ?"*

2. *"Quelles dispositions légales et/ou quelles instructions règlent la délivrance d'une carte d'identité de service aux militaires ?"*

3. *"Quelles différences y a-t-il entre les cartes d'identité de service délivrées aux militaires néerlandophones, francophones et germanophones ?"*

4. *"Quels militaires reçoivent une carte de légitimation, pour quelles fonctions ou missions ?"*

5. "Les cartes visées à la question 4 sont-elles également pourvues d'une photo du titulaire ?"

Réponses

1. La réponse du ministre mentionne 20 catégories de militaires et civils auxquels des cartes d'identité de service sont délivrées. Les membres du SGR ne sont pas cités; par contre, sont cités les *" personnes civiles assimilées à un rang de militaire"* qui désignent sans doute les agents civils du Service de sécurité militaire.

2. *"Il n'existe pas de dispositions légales quant à la délivrance d'une carte d'identité de service aux militaires. Les instructions actuelles en la matière sont contenues dans le règlement A8 relatif à l'administration du personnel militaire".*

3. *"Il n'existe pas de différence entre les cartes d'identité de service délivrées aux militaires néerlandophones, francophones et germanophones autre que le fait que le document est unilingue et que la langue du document est la même que celle de l'intéressé".*

4. "Une carte de légitimation est délivrée aux militaires travaillant, temporairement ou en permanence, dans une zone ou une installation de sécurité. Cette carte, d'une durée de validité limitée, est émise par l'organisme assurant la sécurité et n'est valable que dans cette zone bien précise. Il n'existe pas de données centralisées sur le nombre de fonctions ou de missions pour lesquelles une carte de légitimation est requise".

5. *"Dans pratiquement tous les cas, ces cartes sont munies d'une photo du bénéficiaire".*

4. LES CARTES DE SERVICE DE LA SURETE DE L'ETAT

4.1. Fondements

La délivrance des cartes de service, signes de fonctions et laissez-passer de la Sûreté de l'Etat, trouve son fondement légal et/ou réglementaire dans les dispositions suivantes :

- l'article 34 de l'arrêté royal du 29 avril 1966 *"portant le statut du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique"*;

- l'article 10 de l'arrêté ministériel du 4 décembre 1992 *"déterminant les armes faisant partie de l'équipement réglementaire des agents des services extérieurs de la Sûreté de l'Etat et fixant les dispositions particulières relatives à la détention, à la garde et au port de ces armes"*.

A. Le statut "du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique"

L'article 34 de l'arrêté royal du 29 avril 1966 *"portant le statut du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique"* (modifié par l'arrêté royal du 22 décembre 1993) dispose : *"Les agents des services extérieurs de la Sûreté de l'Etat sont toujours munis d'une médaille en métal argenté, de quarante millimètres de diamètre, portant sur la face les armes du Royaume et au revers les mots "Sûreté publique - Openbare Veiligheid" ainsi que leur nom et les initiales de leurs prénoms et leur qualité."*

Cette disposition ne s'applique qu'aux agents des services extérieurs de la Sûreté de l'Etat. Contrairement à l'article 33 de l'arrêté royal du 20 août 1969 portant le statut des agents civils du Service de sécurité militaire, le statut des agents des services extérieurs de la Sûreté de l'Etat ne prévoit pas qu'ils sont porteurs d'une carte d'identité de service, délivrée par le ministre de la Justice.

Une note interne de ce service mentionne cependant l'existence d'un laissez-passer pour les agents des services extérieurs de la Sûreté de l'Etat.

B. L'arrêté ministériel du 4 décembre 1992 "déterminant les armes faisant partie de l'équipement réglementaire des agents des services extérieurs de la Sûreté de l'Etat et fixant les dispositions particulières relatives à la détention, à la garde et au port de ces armes".

L'article 10 de cet arrêté ministériel dispose : *"Chaque agent des services extérieurs de la Sûreté de l'Etat porteur d'une arme de service détient une carte d'identification attestant l'autorisation réglementaire de port d'arme dans l'accomplissement de ses missions. Ce document mentionne les nom, prénoms, lieu et date de naissance ainsi que le grade de l'agent. Il porte, en outre, une photo de l'intéressé et la signature du ministre de la Justice ou de son délégué".*

Cet arrêté ministériel a été pris en exécution de l'article 2 de l'arrêté royal du 11 septembre 1991 *"relatif à la détention et au port d'armes par les services de l'autorité ou de la force publique"*. Cet article attribue au ministre de la Justice la compétence :

- de déterminer les armes faisant partie de l'équipement réglementaire des agents des services extérieurs de la Sûreté de l'Etat, d'une part;

- d'arrêter les dispositions particulières relatives à la détention, à la garde et au port de ces armes.

Cet arrêté royal du 11 septembre 1991 repose lui-même sur la loi du 3 janvier 1933 *"relative à la fabrication, au commerce et au port des armes et au commerce des munitions"* (modifiée par les lois des 24 juillet 1934, 4 mai 1936 et 30 janvier 1991).

4.2. Description des cartes - contenu - fonction

A. La "carte de service" blanche

Il s'agit de la carte d'identification prévue par l'article 10 de l'arrêté ministériel du 4 décembre 1992. Celle-ci remplace les anciens laissez-passer et le permis individuel de port d'arme. Elle constitue la nouvelle carte de service depuis 1993. Elle indique que son titulaire est autorisé à porter une arme réglementaire dans l'exercice de ses fonctions. Tous les agents des services extérieurs en sont titulaires.

B. La carte des services administratifs centraux

Le Service d'enquêtes a pu prendre connaissance d'une photocopie de cette carte qui avait été exhibée aux forces de gendarmerie. Cette carte, délivrée par le secrétaire général du ministère de la Justice, indique l'identité de son titulaire ainsi que son grade à la Sûreté de l'Etat. Elle porte aussi la mention : *"Les autorités constituées le reconnaissent en cette qualité; elles sont* (illisible [(1)]) *à prêter aide et protection dans l'exercice de ses fonctions".*

Invité à fournir quelques explications sur la délivrance de cartes de service aux membres des services centraux de la Sûreté de l'Etat, le secrétaire général du ministère de la Justice a déclaré *"Certains fonctionnaires des services administratifs centraux ont reçu des cartes de service destinées à attester leur appartenance au ministère de la Justice. Il n'y a pas de base légale ou réglementaire pour ces cartes. Ces cartes ont comme seul but d'attester l'origine de nos fonctionnaires vis-à-vis d'autres organismes publics par exemple dans les bibliothèques des ministères ou au Parlement. Cette carte permet aux fonctionnaires d'être exemptés de quelques prescriptions purement administratives ou de passer facilement dans la zone neutre en cas de manifestations"*.

Le secrétaire général du ministère de la Justice a été invité à fournir au Comité R quelques explications complémentaires, à savoir :

- Quels sont ces *"certains fonctionnaires"* des services administratifs de la Sûreté de l'Etat à qui une carte de service a été délivrée ?

- Cette délivrance est-elle liée à une fonction précise ou non ?

(1) La photocopie de la carte n'était pas de bonne qualité.

Ce haut fonctionnaire a répondu ce qui suit :

"(...) j'ai l'honneur de vous informer que je fixerai l'usage, le modèle et les conditions d'octroi de la carte de service. A ce sujet, j'accorderai une attention particulière aux mentions qui y figurent. Celles-ci doivent être limitées au but pour lequel les cartes sont délivrées à certains fonctionnaires, notamment pouvoir prouver d'une manière simple la fonction exercée, dans des situations professionnelles déterminées".

Questionné sur les mesures prises suite à l'exhibition intempestive d'une de ces cartes de service aux forces de gendarmerie, l'Administrateur général de la Sûreté de l'Etat a fait savoir au Comité R qu'aucun dossier disciplinaire n'avait été ouvert à charge de l'intéressé et qu'aucune nouvelle note de service n'avait été rédigée.

C. La médaille en métal argenté des agents des services extérieurs

Celle-ci est décrite par l'article 34 de l'arrêté royal du 29 avril 1966 *"portant le statut du personnel de la section Sûreté de l'Etat de l'Administration de la Sûreté publique"* (voir point 4.1. A).

Un ordre de service de 1956 indique ce qui suit : *"Lorsque le personnel doit prendre contact avec des autorités judiciaires ou administratives pour l'exécution de ses missions ou devoirs prescrits, il est tenu de donner explicitement connaissance de son appartenance à l'Administration de la Sûreté Publique - section Sûreté de l'Etat - en exhibant soit la médaille, soit le laissez-passer de service. Ceci afin d'éviter qu'éventuellement un membre de l'autorité judiciaire ou administrative puisse s'imaginer avoir affaire, par exemple, à un ou des membres de la police communale ou police judiciaire du Parquet, confusion qui peut donner lieu à l'ouverture éventuelle d'une information du chef d'immixtion dans les fonctions publiques".*

L'arrêté royal du 31 décembre 1993 relatif à l'organisation du ministère de l'Intérieur et de la Fonction publique a opéré la scission organique des deux branches de la Sûreté publique par le transfert de l'Office des étrangers au ministère de l'Intérieur. Depuis lors, la dénomination "section Sûreté de l'Etat de l'Administration de la Sûreté publique" a fait place à la dénomination "Administration de la Sûreté de l'Etat". Les mentions figurant sur la médaille en métal argenté ne correspondent donc plus à la nouvelle dénomination officielle du service.

4.3. Le titre de légitimation prévu par le projet de loi organique des services de renseignements et de sécurité

La section 2 de ce projet de loi contient des dispositions particulières à l'exercice des missions de protection des personnes par des agents des Services extérieurs de la Sûreté de l'Etat appelés "*officiers de protection".*

Ces dispositions s'inspirent de la loi du 5 août 1992 sur la fonction de police : elles confèrent aux officiers de protection certains pouvoirs d'officier de police administrative, notamment les droits de pénétrer dans des immeubles abandonnés, de fouiller des personnes, des véhicules, de saisir certains objets dangereux, de retenir brièvement une personne, de contrôler son identité, de faire un usage limité de la force, d'armes à feu, et même de requérir l'aide ou l'assistance de personnes présentes sur place en cas de danger. L'usage des moyens de contrainte est toutefois limité à l'exercice des missions de protection.

L'article 21 prévoit donc que dans l'exercice de leurs missions, *"sauf si les circonstances ne le permettent pas, les officiers de protection, ou au moins l'un d'entre eux, qui interviennent à l'égard d'une personne ou qui se présentent au domicile d'une personne, justifient de leur qualité au moyen du titre de légitimation dont ils sont porteurs".*

Cette disposition s'inspire en effet de l'article 41 de la loi du 5 août 1992 sur la fonction de police qui dispose : *"Sauf si les circonstances ne le permettent pas, les fonctionnaires de police qui interviennent en habits civils à l'égard d'une personne, ou au moins l'un d'entre eux, justifient de leur qualité au moyen du titre de légitimation dont ils sont porteurs. Il en est de même lorsque des fonctionnaires de police en uniforme se présentent au domicile d'une personne".*

4.4. Le titre de légitimation prévu par le projet de loi relatif aux habilitations de sécurité

Ce projet de loi déposé le 17 septembre 1997 [(2)] a pour principal objectif de conférer un fondement légal aux enquêtes préalables à la délivrance d'une habilitation de sécurité, c'est-à-dire d'une autorisation officielle d'accès à des données classifiées. Le chapitre III de ce projet de loi est consacré aux enquêtes de sécurité; celles-ci sont effectuées par des agents des Services extérieurs de la Sûreté de l'Etat et par des membres du Service général du renseignement et de la sécurité spécialement désignés pour effectuer cette mission.

Le projet prévoit que lors de leur désignation, ces agents reçoivent une "*carte de légitimation*" dont le modèle est fixé selon le cas par le ministre de la Justice ou par le ministre de la Défense nationale. Sur présentation de cette carte, les agents concernés pourront, dans le cadre des enquêtes de sécurité, et uniquement à cette fin, accéder au casier judiciaire central, aux casiers judiciaires, au registre national, aux registres de la population et des étrangers, au registre d'attente des étrangers, ainsi qu'à certaines données policières.

Les agents des services de renseignement seront aussi tenus d'exhiber leur carte de légitimation à toute personne dont ils sollicitent le concours dans le cadre des enquêtes de sécurité.

Cette carte ne pourra être utilisée que dans le cadre des enquêtes de sécurité et elle devra être immédiatement restituée à l'autorité qui l'a délivrée lorsque la désignation ministérielle pour effectuer ces enquêtes aura pris fin.

---

(2) Chambre des représentants - 1193 / 1 - 96 / 97

4.5. Commentaires

Aussi bien la médaille argentée que la carte d'identification des agents des services extérieurs trouvent leur fondement dans des textes réglementaires opposables à tous, à savoir un arrêté royal et un arrêté ministériel.

Deux projets de loi visent notamment à conférer une base légale à l'octroi de tels documents:

- le projet de loi organique des services de renseignement et de sécurité prévoit un "titre de légitimation" dont seront porteurs les agents des services extérieurs de la Sûreté de l'Etat chargés des missions de protection des personnes;

- le projet de loi relatif aux habilitations de sécurité prévoit la délivrance d'une "carte de légitimation" aux agents des Services extérieurs de la Sûreté de l'Etat et aux membres du Service général du renseignement et de la sécurité spécialement désignés pour effectuer les enquêtes de sécurité.

L'octroi d'une carte de service à *"certains fonctionnaires des services administratifs centraux"* ne repose sur aucune base légale ou réglementaire. L'octroi de cette carte est décidé par le secrétaire général du ministère de la Justice qui s'est engagé à en fixer lui-même l'usage, le modèle et les conditions d'octroi.

Il accordera une attention particulière aux mentions qui y figurent. *"Celles-ci doivent être limitées au but pour lequel les cartes sont délivrées à certains fonctionnaires, notamment pouvoir prouver d'une manière simple la fonction exercée, dans des situations professionnelles déterminées"*.

Le Comité R estime que l'indication *"les autorités constituées le reconnaissent en cette qualité; elles sont* (illisible) *à prêter aide et protection dans l'exercice de ses fonctions"* est sujette aux mêmes critiques que celles formulées à l'égard des cartes du SGR [(3)] car trop générale. Cette mention n'a en effet aucune force obligatoire à l'égard des autorités civiles et des citoyens. Sous réserve du projet de loi organique des services de renseignement et de sécurité, il n'existe aucun texte légal ou réglementaire qui confère aux agents de la Sûreté de l'Etat un quelconque pouvoir de contrainte ou de réquisition à l'égard de ces derniers. Produire ce document à des civils, à des fonctionnaires ou à des policiers ne les astreint à aucune obligation spécifique à l'égard de son titulaire.

Le Comité R estime donc que la carte de service des fonctionnaires des services centraux de la Sûreté de l'Etat ne doit pas avoir d'autre fonction que de certifier l'identité, le grade et la qualité de son porteur.

---

(3) Voir point 5.3. ci-après.

Cette position est d'ailleurs celle exposée par M. Caeymaex, ancien administrateur directeur général de la Sûreté de l'Etat, dans un article paru en septembre 1964 dans la revue "l'officier de police" : *"La médaille et le laissez-passer dont il* (l'agent de la Sûreté de l'Etat) *est porteur sont garants de son identité et de ses fonctions particulières au profit du Pouvoir Exécutif, mais ne lui confèrent pas d'autres droits que ceux consentis à tous les agents de ce Pouvoir. Aussi devra-t-il compter sur le concours que peuvent et voudront bien lui accorder tous ceux qui, comme lui, participent à l'exercice de l'autorité publique, Police Communale, Police Judiciaire et Gendarmerie notamment".*

Le Comité R n'a pas encore connaissance des modèles et des mentions que porteront les "titres de légitimation" et "cartes de légitimation" prévus par le projet de loi organique des services de renseignement et de sécurité d'une part, par le projet de loi relatif aux habilitations de sécurité d'autre part.

Le Comité R estime qu'il sera nécessaire de bien distinguer ces titres et cartes de légitimation, les seuls documents à justifier d'un pouvoir de contrainte à l'égard de personnes, de tout autre document (carte de service, laissez-passer, etc...) attribué aux fonctionnaires de la Sûreté de l'Etat.

Cette distinction devra être opérée notamment :

- dans la forme de présentation des dites cartes;

- dans l'expression des droits qu'elles confèrent à leur titulaire.

5. LES CARTES DE SERVICE DU SGR

5.1. Fondements

La délivrance des cartes de service, signes de fonctions et laissez-passer du SGR trouve son fondement légal et/ou réglementaire dans les dispositions suivantes :

- l'article 33 de l'arrêté royal du 20 août 1969 portant le statut des agents civils du Service de sécurité militaire;

- le "règlement sur la sécurité militaire";

- la "directive territoriale de sécurité" relative à la sécurité des quartiers militaires et à l'accès aux quartiers.

Les deux derniers documents cités sont classifiés "diffusion restreinte".

A. Le statut des agents civils du Service de sécurité militaire

L'article 33 de l'arrêté royal du 20 août 1969 portant le statut des agents civils du Service de sécurité militaire (modifié par les arrêtés royaux des 1er juillet 1971, 18 décembre 1987 et 22 décembre 1989) dispose : *"Les fonctionnaires civils du Service de sécurité militaire sont toujours munis d'une médaille en métal argenté, de quarante millimètres de diamètre, portant sur la face les armes du Royaume et au revers les mots "ministère de la Défense nationale - ministerie van Landsverdediging - Service de sécurité militaire - Dienst militaire veiligheid" ainsi que leur nom et les initiales de leurs prénoms. En outre, ils sont porteurs d'une carte d'identité de service, délivrée par le ministre de la Défense nationale".*

Cette disposition ne s'applique qu'aux agents civils du Service de sécurité militaire du SGR.

B. Le "règlement sur la sécurité militaire"

La dernière version dont le Comité R est en possession date du 15 juillet 1992. Il s'agit d'un manuel fixant les *"normes de sécurité pour bâtiments et installations militaires"* applicables à toutes les nouvelles constructions destinées aux organismes ressortant du ministère de la Défense nationale. Le chef d'Etat-major a chargé le SGR de réactualiser ce document. La rédaction et la mise à jour de ce document fait partie intégrante des missions de sécurité du SGR.

La nouvelle version du règlement devrait prochainement entrer en vigueur.

C. La "directive territoriale de sécurité" relative à la sécurité des quartiers militaires et à l'accès aux quartiers

Les "directives territoriales de sécurité" (DTS) sont élaborées par l'Etat-major des Forces armées à l'intention des unités et organismes militaires belges. Elles regroupent toutes les prescriptions existant en matière de sécurité et sont notamment basées sur le "règlement sur la sécurité militaire" . Toutes ces directives sont préparées par la section "sécurité" du SGR.

Le but de la DTS en question est d'assumer la sécurité des quartiers militaires en règle générale, mais surtout la sécurité des zones protégées situées au sein des quartiers. Elle prévoit le principe du contrôle des entrées et des sorties à l'aide de cartes d'accès parmi lesquelles :

- la carte d'identité militaire de service que reçoit chaque militaire (y compris ceux du SGR): elle leur donne en principe le libre accès à leur quartier;

- la carte d'accès permanent au quartier que reçoit le personnel civil (y compris celui du SGR);

- les cartes d'identité spéciales et les cartes de libre accès : c'est dans cette catégorie de documents que l'on trouve les cartes de services propres au SGR.

5.2. Description des cartes - contenu - fonction

A. Le laissez-passer "lie de vin"

Cette carte est délivrée aux membres du SGR qui, dans l'exercice de leur fonction, doivent avoir accès aux installations militaires, zones de sécurité comprises, sans autre forme de contrôle. Cette carte a aussi pour but de confirmer envers les autorités civiles et militaires l'appartenance de son porteur au personnel du SGR. Ce document porte notamment les mentions suivantes:

"Le porteur de la présente n'est PAS soumis aux mesures de contrôle de sécurité et a droit de libre accès aux installations militaires".
"Drager dezer is NIET onderworpen aan de veiligheidskontrolemaatregelen en heeft recht op vrije toegang tot de militaire inrichtingen".
"Les autorités civiles et militaires sont priées de lui prêter aide et assistance".
"De Burgerlijke en Militaire overheden worden verzocht hem hulp en bijstand te verlenen".

La carte doit être numérotée et porter la signature du ministre de la Défense nationale.

B. La carte permanente d'accès du ministère de la Défense nationale

Il s'agit d'une carte qui n'est délivrée qu'aux chauffeurs du SGR; elle donne accès à tous les quartiers militaires, après identification du porteur. Elle a aussi pour but de confirmer aux autorités civiles et militaires l'appartenance de son porteur au personnel du SGR. La carte porte notamment la mention suivante :

"Les autorités constituées le reconnaîtront en cette qualité; elles sont invitées à lui prêter aide et protection dans l'exercice de ses fonctions. De gestelde overheden zullen hem in die hoedanigheid erkennen en hem hulp en bescherming verlenen in de uitoefening van zijn ambt. Die bestehende Behörden haben ihn in dieser Eigenschaft zu erkennen und ihm in der Ausübung seines Amtes Hilfe und Schutz zu gewähren."

La carte doit être numérotée et porter la signature du chef du SGR *"au nom du Ministre - namens de Minister - namens des Ministers"* (de la Défense nationale).

C. Le laissez-passer "couleur crème"

Ce laissez-passer est en fait la carte d'identité des agents civils du Service de sécurité militaire prévue par l'article 33 de l'arrêté royal du 20 août 1969 portant le statut des agents civils du Service de sécurité militaire.

Le document ne comporte en effet aucune mention relative aux droits d'accès de son titulaire aux installations militaires. Outre les données d'identification du porteur, figure au dos de la carte la mention : *"le titulaire du présent laissez-passer est autorisé, en cas de besoin à requérir aide et assistance des autorités civiles et militaires. - De titularis van deze vrijgeleide is er toe gemachtigd, wanneer de noodzakelijkheid zich voordoet, hulp en bijstand te vragen van de burgerlijke en militaire overheden. - Der Inhaber dieses Passierscheines ist ermächtigt nötigenfalls, die Zivil- und Militärbehörden um Hilfe und Beistand zu ersuchen".* La carte doit être numérotée et porter la signature du ministre de la Défense nationale.

Cette carte n'a cependant pour seul but que de confirmer envers les autorités civiles et militaires l'appartenance de son porteur au personnel du Service de sécurité militaire.

D. La médaille en métal argenté des agents civils du Service de sécurité militaire

La médaille produite à un membre du Comité R correspond bien aux prescriptions de l'article 33 de l'arrêté royal du 20 août 1969 portant le statut des agents civils du Service de sécurité militaire. Celle-ci a pour seul but de confirmer envers les autorités civiles et militaires l'appartenance de son porteur au personnel du Service de sécurité militaire.

L'usage de cette médaille est quelquefois jugé comme étant désuet. D'autres agents éprouvent par contre une certaine fierté à posséder ce symbole.

E. Port d'armes

Le personnel du SGR ne dispose pas d'une carte équivalente à celle qui atteste que les agents des services extérieurs de la Sûreté de l'Etat sont autorisés à porter une arme réglementaire dans l'exercice de leurs fonctions (cf. point 4.2. A : la "carte de service" blanche).

Au SGR, chaque autorisation de port d'arme ne peut être accordée que pour les nécessités du service, dans le cadre et pour la durée de certaines missions spécifiques. Dès lors, le porteur d'une arme en vêtements civils doit toujours être en possession d'un document qui l'y autorise, à savoir, - pour une arme qui appartient à l'unité, soit un ordre de marche signé par le chef de corps, soit une mention sur la carte d'identité militaire signée par le chef de corps; - pour une armé privée, une autorisation de port d'arme signée par SGR. En vêtements militaires, seul le port d'une arme privée exige une autorisation de port d'arme signée par le SGR.

Une enquête spécifique est en cours sur cette problématique.

5.3. Commentaires

Seules la médaille argentée et la carte de couleur "crème" trouvent leur fondement dans un texte réglementaire opposable à tous, à savoir un arrêté royal.

La carte “crème” est la seule vraie “carte de service” que l’on trouve au SGR mais elle n’est attribuée qu’aux agents civils du Service de sécurité militaire. Les autres cartes (la “lie-de-vin” et la “carte permanente d’accès du ministère de la Défense nationale”) ne sont que des cartes d’accès aux quartiers militaires. Elles trouvent leur fondement dans des règlements internes aux Forces armées; elles n’ont aucune fonction dans la vie civile.

La seule obligation que puisse entraîner la production d’un de ces documents est une obligation pour les militaires de laisser entrer le porteur dans un quartier militaire pour y accomplir sa mission.

Pourtant, toutes ces cartes portent des mentions telles que *“les autorités civiles et militaires sont priées de lui prêter aide et assistance”* (lie-de-vin), *“les autorités constituées le reconnaîtront en cette qualité; elles sont invitées à lui prêter aide et protection dans l’exercice de ses fonctions”* (carte permanente d’accès du ministère de la Défense nationale) ou bien encore *“le titulaire du présent laissez-passer est autorisé, en cas de besoin à requérir aide et assistance des autorités civiles et militaires”* (laissez-passer de couleur “crème”).

Ces mentions n’ont aucune force obligatoire à l’égard des autorités civiles et des citoyens puisqu’il n’existe aucun texte légal ou réglementaire, ni projet de loi, qui confère aux agents du SGR un quelconque pouvoir de contrainte ou de réquisition à l’égard de tiers. Produire l’un de ces documents à des civils ne les astreint à aucune obligation spécifique à l’égard de leur titulaire. Il faut donc comprendre ces mentions comme une simple invitation à prêter aide et assistance.

Les mots en français*“requérir aide et assistance”* qui figurent sur la carte des agents civils du Service de sécurité militaire sont particulièrement mal venus puisqu’ils laissent supposer un pouvoir de réquisition qui n’existe pas.

Le Comité R est d’avis que toutes les formules précitées sont trop générales et qu’elles doivent être revues de manière à les distinguer clairement de la future “carte de légitimation” prévue pour les membres du SGR spécialement désignés pour effectuer les enquêtes de sécurité (voir point 4.4.). Le document précité sera en effet le seul au SGR à justifier d’un pouvoir légal de son titulaire à l’égard de personnes.

Cette distinction devra être opérée notamment :

- dans la forme de présentation des dites cartes;
- dans l’expression des droits qu’elles confèrent à leur titulaire.

6. LA CARTE D’IDENTITÉ DES “SERVICES DE RENSEIGNEMENTS ET D’ACTION”

Le Comité R a pu prendre connaissance de l’existence d’une carte d’identité des *“services de renseignements et d’action*” dont était titulaire un ancien résistant, membre d’un réseau de renseignements pendant la dernière guerre mondiale. Cette personne était également titulaire d’une carte de membre de *“l’Union des services de renseignements et d’action”*.

Le Comité a souhaité en savoir plus à propos de l'octroi de ces cartes.

6.1. Fondements

Par sa lettre du 13 août 1997, l'administrateur général de la Sûreté de l'Etat a fourni au Service d'enquêtes les explications suivantes concernant la carte d'identité d'agent des Services de Renseignements et d'Action.

Ce document a été attribué à d'anciens résistants qui en avaient demandé le statut. Après la seconde guerre mondiale, ce statut a été accordé individuellement par l'Administrateur directeur général de la Sûreté de l'Etat en fonction des missions effectuées en territoire occupé par l'ennemi pour le compte de ce service qui travaillait alors à Londres, en collaboration avec les autorités britanniques.

L'octroi de ce statut emportait des avantages financiers en matière de pension de retraite. Ce statut a été officialisé par un arrêté-loi du 1er septembre 1944 et complété par un arrêté-loi du 16 février 1946. Une note de service de cette époque signée par "l'Administrateur de la Sûreté de l'Etat" explicite quelque peu les mesures d'application de ce statut mais aucune mention de l'existence d'une carte d'identité spéciale n'y a été trouvée.

Le Service d'enquêtes a par ailleurs trouvé dans les annexes du Moniteur belge du 1er décembre 1945 les statuts de "l'Union des Services de Renseignement et d'Action", en abrégé "U.S.R.A.". Cette association sans but lucratif, qui a pour objet social de gérer les intérêts matériels et moraux de ses membres, est encore active puisque le Moniteur belge du 4 novembre 1994 publie la désignation de ses nouveaux administrateurs.

6.2. Description de la carte d'identité

Un ancien résistant a bien voulu communiquer au Comité R une photocopie de sa carte d'identité d'agent des Services de Renseignements et d'Action. S'agissant d'un document personnel, il ne figure pas en annexe du présent rapport.

Il s'agit d'un document intitulé "Carte d'identité - Eenzelvigheidskaart - S.R.A." L'intérieur mentionne l'identité du titulaire en regard de sa photo et de son empreinte digitale. La carte porte un cachet de la Sûreté de l'Etat ainsi que la signature de "l'administrateur de la Sûreté de l'Etat", ce qui confère à ce document un caractère officiel.

6.3. Commentaires

Malgré son titre de "carte d'identité", le dit document ne paraît avoir eu aucune fonction "opérationnelle" ou même d'identification de son titulaire par rapport aux autorités ou à l'un des services de renseignements nationaux.

Cette carte d'identité constitue la simple reconnaissance qu'un ancien résistant est titulaire du statut d'agent de renseignement et d'action tel que fixé par les arrêtés-lois des 1er septembre 1944 et 16 février 1946.

7. RECOMMANDATIONS

En l'absence d'un pouvoir légal de contrainte, le Comité R estime que les cartes de service (ou cartes d'identité) des membres des services de renseignement ne peuvent avoir pour seule fonction que :

- de certifier l'identité du titulaire, son grade et sa qualité au sein du dit service;
- de lui permettre l'accès sans autre forme de contrôle à certains établissements militaires ou officiels;
- d'attester, le cas échéant, qu'il est autorisé à porter une arme réglementaire dans l'exercice de ses fonctions.

Un seul document pourrait, le cas échéant, remplir ces trois fonctions.

A défaut d'un texte légal ou réglementaire (un arrêté royal ou un arrêté ministériel), le Comité R recommande :

- qu'à tout le moins une directive interne ou un ordre permanent fonde l'existence de toute espèce de carte de service ou de laissez-passer mis en circulation;
- que ce document définisse quelle est la fonction et l'usage de la carte ou du laissez-passer;
- que soient précisés les catégories et éventuellement les grades des membres du personnel à qui une carte de service ou un laissez-passer est délivré;
- que chaque carte ou laissez-passer soit numéroté.

Le Comité R recommande également qu'un registre soit tenu indiquant toutes les personnes à qui une carte de service ou un laissez-passer a été délivré.

A défaut d'obligation légale ou de protocole d'accord et de collaboration entre autorités civiles et militaires, les mentions destinées aux autorités civiles *"requises", "invitées"* ou *"priées"* de *"prêter aide, assistance"* et *"protection"* au titulaire ne devraient plus figurer sur aucune carte d'un service de renseignement.

Deux projets de loi visent notamment à conférer une base légale à l'octroi de tels documents:

- le projet de loi organique des services de renseignement et de sécurité prévoit un "titre de légitimation" dont seront porteurs les agents des services extérieurs de la Sûreté de l'Etat chargés des missions de protection des personnes;

- le projet de loi relatif aux habilitations de sécurité prévoit la délivrance d'une "carte de légitimation" aux agents des Services extérieurs de la Sûreté de l'Etat et aux membres du Service général du renseignement et de la sécurité spécialement désignés pour effectuer les enquêtes de sécurité.

Seuls ces documents justifieront réellement d'un pouvoir de contrainte ou d'un pouvoir légal à l'égard de particuliers ou de fonctionnaires; seuls ces documents pourront donc contenir une mention signalant les pouvoirs légaux de son titulaire.

Le Comité R recommande aussi que chaque carte et laissez-passer fasse apparaître clairement, et sans ambiguïté, les pouvoirs que détient son titulaire, et à l'égard de quelles autorités. La forme et le contenu de ces autres documents devront bien les distinguer du "titre de légitimation" des officiers de protection de la Sûreté de l'Etat d'une part, de la "carte de légitimation" des agents chargés d'effectuer les enquêtes de sécurité d'autre part.

Pour autant que l'usage de la médaille argentée soit encore jugé utile, le Comité R recommande d'adapter les mentions qui figurent sur celle des services extérieurs de la Sûreté de l'Etat; les mentions actuelles ne correspondent plus en effet à la nouvelle dénomination officielle de ce service.

Le Comité R recommande enfin :

- un contrôle interne rigoureux sur l'octroi et l'usage des cartes et laissez-passer;

- l'établissement des prochaines cartes sous forme plastifiée et infalsifiable.

CHAPITRE 2 : RESPECT ET APPLICATION PAR LE SGR DES DIRECTIVES TERRITORIALES DE SECURITE ET EN PARTICULIER CELLES QUI REGISSENT L'ACCES A LEURS QUARTIERS

1. PROCEDURE

Fin septembre 1997, le Service d'enquêtes a été mis en possession d'une carte d'accès à un quartier militaire, délivrée par le SGR à l'un de ses collaborateurs. Selon toute vraisemblance, cette carte a été perdue par son titulaire.

Le Service d'enquêtes a posé une question informelle à ce sujet et a constaté, sur base de la réponse obtenue, que les directives en vigueur au SGR n'ont pas été (suffisamment) appliquées.

Le Service d'enquêtes a décidé, conformément à l'article 40 § 1 de la loi du 18 juillet 1991 régissant le contrôle des services de police et de renseignements, d'ouvrir d'office une enquête sur le thème "*Respect et application par le SGR des directives territoriales de sécurité et en particulier celles qui régissent l'accès à leurs quartiers*".

La Présidente du Comité R a été informée de cette initiative, laquelle a été entérinée lors de la réunion plénière du Comité R, le 16 octobre 1997.

En application de l'article 46, alinéa 3 du règlement d'ordre intérieur, les Présidents de la Chambre et du Sénat ont été informés, par écrit, le 20 octobre 1997 de l'ouverture de cette enquête.

Le ministre de la Défense nationale a été à son tour informé par un courrier du 14 octobre 1997.

Le rapport a été approuvé lors de la réunion du Comité R le 12 février 1998.

2. BASE LEGALE OU REGLEMENTAIRE

2.1 Généralités

L'accès et le contrôle des quartiers militaires sont régis par :

- les "directives territoriales de sécurité" (DTS);
- les "ordres permanents" (OP).

Les DTS ont été élaborées conjointement par les Etats-Majors des forces armées belges et les forces armées belges en Allemagne, pour les unités belges et les organismes militaires, stationnés ou résidant en Belgique ou en Allemagne.

Elles visent essentiellement à garantir la "sécurité militaire". Les DTS comprennent toutes les dispositions existantes dans le domaine de la sécurité et se fondent, entre autres, sur le règlement IF-5, dont les principes fondamentaux restent valables, même si certaines de ses données ne semblent plus actuelles.

La manière dont ces directives doivent être appliquées au sein d'une unité est déterminée par cette unité elle-même dans les "ordres permanents" qu'elle a établis.

En général, les cartes d'accès octroyées aux personnes relevant du ministère de la Défense nationale peuvent être considérées comme une facilité d'accès dans les quartiers militaires qui ne sont pas catalogués à risque. Nonobstant cette facilité d'accès, chaque personne doit être en mesure de justifier, à tout instant, sa présence dans les quartiers au moyen soit d'une carte de légitimation militaire soit d'une carte de service. Cette obligation est destinée à assurer la sécurité des zones à protéger se trouvant dans les quartiers.

2.2 Les différents types de cartes d'accès

Les DTS-34 prévoient deux types de cartes d'identification et d'accès, à savoir :

2.2.1. La carte d'accès permanent – CIDA-P

Celle-ci est destinée au personnel qui peut avoir accès à une ou plusieurs zones protégées situées dans un quartier. Cette carte est munie d'une photo.

2.2.2. La carte d'accès visiteur – CIDA-V

Celle-ci est destinée à tout membre du personnel qui ne possède pas une CIDA-P et dont la présence est nécessaire dans la zone protégée. Cette carte n'est pas munie d'une photo.

2.2.3. Différence entre ces deux cartes

Le titulaire d'une CIDA-P bénéficie d'un libre accès au quartier; le porteur d'une CIDA-V doit être accompagné.

2.2.4. Qui délivre ces cartes ?

La CIDA-P est délivrée par l'officier de sécurité et fait l'objet d'une transcription dans un registre. La CIDA-V est délivrée par le personnel de contrôle à l'entrée, en échange d'une carte de service ou d'une carte d'identité civile.

2.2.5. Procédure de contrôle

CIDA-P : contrôle visuel par le personnel de contrôle.

CIDA-V : * le visiteur est annoncé à l'autorité demandée par le personnel de contrôle
* le visiteur est pris en charge par l'autorité au poste de contrôle
* l'autorité visitée est responsable de l'accompagnement permanent.

2.2.6. Dispositions en cas de perte

Le Commandant de quartier doit :

* prendre des mesures préventives contre les abus;
* prévenir l'Etat-Major provincial;
* remplacer la CIDA-P;
* compléter la liste des CIDA en mentionnant :
  - la perte de la carte originale et de la référence du duplicata;
  - l'inscription du duplicata.

2.3. Ordres permanents en vigueur au SGR

Au SGR, la problématique relative aux "cartes d'accès" est régie par son *"Ordre Permanent 20.5*".

2.3.1. Généralités

Le personnel, prévu à l'ordre de bataille du SGR, est en possession d'une carte d'accès personnelle. Cette carte correspond entièrement à la CIDA-P décrite dans les DTS.

2.3.2. Types de cartes

Le SGR délivre trois types de cartes, à savoir :

* la carte "SGR".
* la carte "QRE-040"
* la carte "VIP"

2.3.3. La carte "SGR"

Le personnel administré par le SGR qui doit avoir régulièrement accès au bloc 1 et aux blocs 14 A ou B, dispose d'une carte d'accès personnelle SGR, munie d'une photo.

Cette carte donne accès au QRE (Quartier Reine Elisabeth), y compris les blocs 1 et les blocs SGR.

2.3.4. La carte "QRE-SP040"

Il s'agit d'une carte d'accès provisoire, d'une durée de validité d'un an. La carte est réservée à des visiteurs réguliers du SGR et permet uniquement l'accès au Quartier Reine Elisabeth.[(1)]

2.2.5. La carte "VIP"

Cette carte ne donne accès qu'au Quartier Reine Elisabeth.

2.2.6. Gestion de ces cartes d'accès

La gestion et la distribution de ces cartes ressort de la compétence du G1.[(2)]

2.4. Motifs de l'ouverture de l'enquête de contrôle

Comme nous l'avons déjà indiqué précédemment, le Service d'enquêtes a été mis en possession d'une "carte d'accès à un quartier militaire", délivrée par le SGR à l'un de ses collaborateurs.

Lors de l'une de ses visites au SGR, le Service d'enquêtes a posé une question informelle concernant les circonstances de la perte de cette carte.

Bien que la perte fut signalée récemment, le Service d'enquêtes est arrivé à la conclusion qu'aucun responsable désigné pour cette problématique n'a été en mesure d'apporter une explication valable à ce sujet.

Ainsi, le Service d'enquêtes a constaté que la déclaration écrite, faite par son titulaire quant à la perte de sa carte n'a pu être présentée et qu'une nouvelle carte d'accès a été délivrée, en violation de certaines dispositions.

---

(1) Remarque : un visiteur régulier, qui doit se rendre au bloc 1, reçoit une carte visiteur en échange de sa carte d'accès à l'accueil du bloc 1.

(2) Voir point 2.5.3. - *"Entretien avec le responsable du Secrétariat Central du SGR"*

2.5. L'enquête proprement dite

2.5.1. Courrier au C/SGR

Le 14 octobre 1997, le Service d'enquêtes a adressé un courrier au Commandant du SGR, en posant un certain nombre de questions relatives à la procédure suivie après le signalement de la perte de la carte d'accès concernée.

Le 21 octobre 1997 le général Simons a répondu par écrit à ce questionnaire.

Commentaires

De l'analyse de cette réponse, le Service d'enquêtes constate qu'une plus-value est attribuée à la carte visée.

Alors que "l'OP 20.05" ne parle que de l'accès au Quartier Reine Elisabeth et aux bâtiments du SGR situés dans ce quartier, la lettre du Commandant du SGR indique que cette carte donne également accès aux quartiers "Molenbeek-Wersbeek" et "Sous-lieutenant Vilain (Casteau)", où travaillent également des collaborateurs du SGR.

Ces quartiers peuvent être considérés comme des annexes du SGR. Il est donc logique que la carte rouge y donne accès. Ce système sera modifié par l'introduction des cartes informatisées.

D'autre part, ce courrier souligne que

"(...) *De plus, ces cartes sont les seules à présenter une couleur rouge très voyante, ce qui doit inévitablement attirer l'attention du personnel de garde à l'entrée du quartier où l'on tente d'entrer et qui doit les inciter à une plus grande vigilance*".

Cette argumentation laisse le Service d'enquêtes perplexe. La couleur très voyante de cette carte peut effectivement avoir pour but d'attirer l'attention du personnel de garde, mais dans la pratique on observe généralement une réaction inverse.

Il est un fait que la carte d'accès ne mentionne pas que son titulaire est membre du SGR, mais c'est un "secret de polichinelle", du point de vue du Service d'enquêtes en tout cas. La mention au verso des anciennes cartes concerne effectivement l'adresse à laquelle le document éventuellement trouvé doit être renvoyé et l'abréviation y figurant stipule qu'il s'agit du SGR. Que cette mention n'apparaisse plus sur les nouvelles cartes témoigne du fait que les responsables du SGR ont conclu à l'inutilité de cette mention.

Dans le dernier paragraphe de son courrier, le Commandant du SGR attire l'attention sur le fait que

"*(...) L'importance de la perte d'une carte d'accès ne peut évidemment être minimalisée. Cependant, il faut souligner qu'une telle carte ne vise qu'à faciliter l'accès au quartier, où l'intéressé exerce son service normal. Utiliser cette carte à d'autres fins relève de l'abus*".

En fait, le C/SGR admet ici qu'une "personne mal intentionnée" qui entre en possession d'une telle carte, se verrait faciliter l'accès au quartier.

En ce qui concerne la procédure en cas de perte, le titulaire de la carte doit signaler ce fait à sa hiérarchie. En fait, cette formalité n'est pas imposée par les instructions, mais s'inspire de la logique. Pour le titulaire, cette carte est un "instrument de travail".

Au SGR, cette formalité s'effectue normalement par écrit. Si les circonstances de la perte ne semblent pas suspectes selon les déclarations du titulaire, aucun examen supplémentaire n'est effectué à cet égard.

En règle générale les déclarations de perte sont conservées, ce qui n'a pas été le cas en l'espèce

De l'avis du Service d'enquêtes, il s'agit, en ce qui concerne la destruction de la déclaration, d'une lacune, en contradiction avec d'autres directives des DTS, qui prévoient pour d'autres documents (entre autres, la carte visiteur) un délai de conservation de 10 ans.

Le Service d'enquêtes estime donc pouvoir affirmer que, pour ce qui concerne la perte d'une carte d'accès personnelle, les déclarations relatives aux circonstances de la perte devraient également faire l'objet d'un délai de conservation raisonnable.

Dans le cas où il appert, à un stade ultérieur, qu'une fausse déclaration a été faite et que l'affaire doit être réexaminée, on pourrait ainsi prendre connaissance de la déclaration faite. De l'avis du Service d'enquêtes l'incident qui est l'origine de cette enquête est un cas d'école.

Que la perte de la carte d'accès n'ait pas été portée à la connaissance des autorités compétentes est contraire à la directive en la matière. Les DTS prévoient que l'Etat-Major provincial doit en être informé, pour lui permettre de signaler cette perte à toutes les personnes chargées de veiller à la sécurité militaire (entre autres les locaux de garde).

Comment peut-on faire preuve d'une vigilance accrue si les personnes compétentes ne sont pas informées des faits qui peuvent et doivent susciter cette vigilance?

Le Secrétariat Central du SGR tient le registre des cartes distribuées et effectue les démarches nécessaires pour la délivrance d'une première carte ou pour remplacer des cartes perdues ou endommagées. Toutes les cartes sont signées personnellement et exclusivement par l'officier de sécurité du SGR/G. La procédure est contrôlée par l'officier S1 qui est à son tour placé sous le contrôle de l'officier de sécurité.

2.5.2. Audition du titulaire de la carte perdue

L'intéressé a été invité à une audition par le Service d'enquêtes. Préalablement à cette audition, l'intéressé a été clairement informé du motif de sa convocation. D'autre part, il a été informé du contenu de l'article 48 de la loi du 18 juillet 1991 relatif au secret professionnel.

L'intéressé travaille au SGR pour le compte du Ministère de la Défense.

Dans le courant du mois de septembre 1997, sans pouvoir déterminer la date exacte, il a constaté qu'il avait perdu la carte d'accès délivrée par le SGR. Il a supposé que cette perte était intervenue au moment où il effectuait une opération bancaire.

Il en a informé par écrit le Secrétariat Central du SGR. Une carte VIP provisoire lui a été remise contre accusé de réception. Une nouvelle carte d'accès lui fut délivrée à une date ultérieure.

En marge de son activité principale, l'intéressé mène également une activité accessoire. Il distribue, dans sa région des journaux publicitaires. Il n'exclut donc pas la possibilité d'avoir perdu sa carte d'accès au cours de cette activité.

Sa dernière mission opérationnelle pour le SGR, sur le terrain, a pris fin en mars 1997.

Des circonstances familiales l'ont contraint pendant une longue période à loger au Quartier Reine Elisabeth à Evere. Officiellement, il s'est installé chez ses parents. Ensuite, il a déménagé dans une autre commune.

2.5.3. Entretien avec le responsable du Secrétariat Central du SGR

L'intéressé a été invité à un entretien par le Service d'enquêtes. Le motif de l'entretien lui était connu. L'intéressé est le responsable du Secrétariat Central du SGR. Il est un des responsables de la distribution et de la délivrance des cartes d'accès.

Pour entrer en possession d'une carte d'accès, il faut respecter une procédure déterminée. Les chefs de section respectifs font établir une demande d'obtention d'une carte d'accès par la personne qui en a besoin. Cette demande motivée est transmise au Secrétariat Central du SGR, qui la transmet à son tour à l'officier de sécurité (SGR/G).

Si l'officier de sécurité donne son accord pour la délivrance de la carte, la demande retourne au Secrétariat Central, où l'on confectionne et numérote une carte d'accès. Une fois cette opération effectuée, la carte est signée par le titulaire. Ensuite, cette carte retourne à l'officier de sécurité, qui la signe à son tour. Enfin, la carte revient une nouvelle fois au Secrétariat Central où elle est plastifiée et enregistrée. Arrivée en fin de parcours, elle est remise au titulaire.

Le registre, dont il est question dans les DTS, fait partie d'une entité dans le PC au Secrétariat Central du SGR. Toutes les cartes d'accès délivrées y sont mentionnées par numéro d'ordre.

Dans le cas où un titulaire perd sa carte d'accès, il en fait la déclaration à sa hiérarchie. Bien que le règlement ne prévoit rien à cet égard, il est de coutume au SGR d'effectuer cette déclaration par écrit. La déclaration contient un bref exposé des circonstances de la perte.

La délivrance d'un duplicata est liée à la procédure décrite supra. La déclaration écrite n'est pas conservée plus longtemps que nécessaire, ce qui signifie, dans la pratique jusqu'à la délivrance du duplicata.

Notons qu'une procédure est actuellement en cours pour donner à chaque membre du personnel de la défense nationale une carte d'accès informatisée, laquelle lui donnera accès au quartier programmé sur la carte informatisée. Tout type de cartes d'accès à l'exception des cartes d'identité militaires seront bientôt supprimées.

Commentaire

On peut retenir de l'entretien du Service d'enquêtes avec le responsable du Secrétariat Central que la mise en place prévue de la carte informatisée pourrait être à l'origine d'une application moins stricte des directives de sécurité prévues pour la délivrance des cartes non informatisées, étant donné que cette nouvelle carte aurait déjà dû être utilisée six mois plus tôt. Des problèmes techniques en ont apparemment décidé autrement.

La carte informatisée est officiellement entrée en vigueur le 15 janvier 1998. Cette carte ne donne pas uniquement accès au quartier, mais également de manière sélective à des zones ou bâtiments protégés.

Une liste nominative des personnes et de leurs accès a été établie.

En cas de perte, et pour éviter tout abus, la carte est alors désactivée.

3. CONCLUSIONS

L'accès aux quartiers militaires est régi depuis le 15 janvier 1998, pour les militaires et le personnel civil de la Défense Nationale, par la mise en place d'une "carte informatisée".

Le Service d'enquêtes se pose la question de savoir pourquoi le SGR a estimé utile d'indiquer sur cette carte informatisée, qui est finalement une "clé" moderne, les mentions qui y figurent. Cette carte n'est pas une "carte d'identité" ni une "carte d'identité de service". Elle ne peut donc être utilisée comme telle.

De par les mentions qui y figurent, on démantèle de fait en grande partie la protection efficace que représente l'anonymat de la carte. Plus le nombre d'informations qu'elle reprend est important, plus un abus éventuel est facilité.

En réalité, les données administratives du titulaire d'une telle carte sont connues de l'autorité qui délivre la carte.

Pourquoi dès lors les rendre une fois encore publiques ? Une clé perdue ne peut tout de même pas reprendre des mentions qui permettent à un voleur de savoir à quel bâtiment ou serrure cette clé donne accès !

On peut estimer que cette carte, en cas de perte, sera rendue "inutilisable", mais seulement après avoir constaté la perte de la carte. La période entre la perte et son constat est une période critique qui peut entraîner de graves conséquences en cas d'abus.

Le SGR a fait les remarques suivantes suite au rapport d'enquêtes qui lui a été transmis par le ministre de la Défense nationale :

"On peut accepter le principe d'une carte anonyme pour un nombre limité de personnes comme c'est le cas pour ceux qui travaillent dans le bâtiment des Comités de contrôle, puisqu'il s'agit d'un seul bâtiment avec une seule entrée où tout le monde connaît tout le monde. Cela n'est cependant pas réalisable pour des unités où plus de mille personnes se déplacent dans plusieurs bâtiments et où un service de garde permanent doit pouvoir vérifier à chaque instant si la présence d'une personne est justifiée en comparant les éléments figurant sur la carte (phot, nom, prénoms, date de naissance, N° de matricule) aux éléments repris sur la carte d'identité militaire."

Pour le service d'enquêtes il ne s'agit pas de préconiser la généralisation de l'anonymat des cartes informatisées pour tout le personnel mais seulement pour les collaborateurs du SGR (petite unité par la taille mais importante par sa mission) en se basant sur le système en vigueur au Ministère de la Justice et à la Sûreté de l'Etat.

En cas de besoin un collaborateur du SGR peut toujours se légitimer vis-à-vis d'un organe de contrôle via sa carte d'identité de service.

En dépit des mentions indiquées sur la nouvelle carte celle-ci offre évidemment une plus grande sécurité que dans le passé et bien que cette carte apporte une protection plus adéquate de l'accès au quartier militaire, il ne faut pas perdre de vue qu'au moment des constatations, le Service d'enquêtes a dû noter que l'autorité administrative responsable au SGR avait commis une erreur.

En ne respectant pas rigoureusement les directives de sécurité, l'autorité responsable a pris un risque inutile et s'est exposée à un abus éventuel. On peut relativiser quelque peu l'incident par le fait que la mise en place de la carte informatisée s'est fait attendre pendant six mois en raison de problèmes techniques.

4. RECOMMANDATIONS

Le Service d'enquêtes espère que le SGR accordera à l'avenir l'attention nécessaire à une stricte application de toutes les directives de sécurité qui régissent l'accès aux quartiers et aux bâtiments en attirant l'attention de ses collaborateurs sur les directives d'application en la matière.

Afin de limiter autant que possible tout abus, la déclaration de la perte d'une carte d'accès devrait intervenir aussi rapidement que possible avec une description des circonstances de la perte, par l'établissement d'une déclaration écrite qui devrait être conservée pendant un délai raisonnable.

Suite à l'introduction du système des cartes informatisées, le Service d'enquêtes souhaite attirer l'attention sur le risque encouru lorsque sur cette carte normalement "anonyme" figurent des données personnelles qui peuvent permettre à la personne qui la trouve ou la subtilise de déterminer les sites auxquels la carte donne accès.

D. PLAINTES DE PARTICULIERS OU DENONCIATION

CHAPITRE 1 : ENQUETE DE CONTRÔLE RELATIVE A MONSIEUR Y

1. PROCEDURE

Par lettre du 16 avril 1997, un syndicat transmettait à la présidente du Comité R une plainte à l'encontre du SGR, se rapportant au retrait injustifié d'un certificat de sécurité, et à l'atteinte portée aux droits constitutionnels et légitimes d'un militaire.

Le syndicat dont il est question ci-dessus a été consulté par Monsieur Y. Agissant au titre d'organisation syndicale, celle-ci a déposé une plainte à l'encontre du SGR au nom de l'intéressé, pour le motif que ces services lui avaient injustement retiré son certificat de sécurité, tout en refusant de lui faire part des motifs de ce retrait.

Le 21 novembre 1996, pour des raisons administratives, l'intéressé a été démis de ses fonctions auprès d'une organisation internationale.

Par une apostille du 30 avril 1997, le Comité R priait le chef du Service d'enquêtes d'inviter Monsieur Y à déposer plainte personnellement auprès du Comité R.

Les 13 juin et 4 novembre 1997, Monsieur Y a été entendu par le chef du Service d'enquêtes.

Durant sa réunion du 26 juin 1997, le Comité R ouvrait une enquête de contrôle, en se fondant sur la plainte d'un particulier relative au refus/retrait d'un certificat de sécurité.

A cette même date, le Comité R chargeait deux de ses membres de mener cette enquête, et de tenir régulièrement le Comité R au courant de son déroulement.

Le 1er juillet 1997, une apostille était transmise au chef du Service d'enquêtes, le priant de prendre connaissance du dossier de l'intéressé au SGR et d'examiner en profondeur la manière dont cette enquête de sécurité avait été menée.

Conformément à l'article 46, § 3 du règlement d'ordre intérieur du Comité R, les présidents de la Chambre et du Sénat ont été avertis, par lettre du 2 juillet 1997, de l'ouverture de l'enquête.

Conformément à l'article 43, § 1 de la loi organique du 18 juillet 1991 organisant le contrôle des services de police et de renseignements, le chef du Service d'enquêtes a averti, le 3 juillet 1997, le Ministre de la Défense nationale de l'ouverture de l'enquête.

Le 8 juillet 1997, un accusé de réception a été adressé à Monsieur Y. Cet avis mentionnait que le Comité R allait examiner le bien-fondé de sa plainte, et qu'après le déroulement de l'enquête, la décision prise par le Comité R en la matière lui serait communiquée.

Conformément à l'article 57 du règlement d'ordre intérieur du Comité R, le chef du Service d'enquêtes avertissait, le 9 juillet 1997, la présidente du Comité R de ce que le Service d'enquêtes allait se rendre le 10 juillet 1997 auprès du SGR, afin d'exécuter la mission qui lui avait été ordonnée.

Par lettre du 9 juillet 1998, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'a pas d'objection à formuler concernant la publication de ce rapport.

2. DIRECTIVES

Pour l'exécution de l'enquête de sécurité, le SGR s'est basé sur un document émanant de l'OTAN, destiné à régir la "sécurité" au sein de l'Organisation du Traité de l'Atlantique Nord.

Ce document prévoit des critères précis auxquels le candidat doit satisfaire. Il appartient à l'autorité émettrice du certificat de sécurité de vérifier si ces critères sont respectés.

Etant donné que Monsieur Y avait postulé un emploi auprès d'une organisation internationale, pour lequel un certificat de sécurité "Nato Cosmic Très Secret Atomal" était exigé, il convenait, conformément à cette directive, de diriger également l'enquête sur son épouse.

Il n'y a pas d'enquête au sujet du comportement sexuel d'une personne. Au cas où, au cours d'une enquête, il apparaîtrait que ce comportement serait de nature à engendrer un risque supérieur à la normale, il en sera néanmoins tenu compte [(1)].

3. DEROULEMENT DE L'ENQUETE

3.1. Documents transmis par le syndicat

Différentes pièces ont été jointes en annexe à la lettre du 16 avril 1997 émanant du syndicat.

3.2. Audition de Monsieur Y le 13 juin 1997

3.2.1. Carrière

Monsieur Y a pris son service dans les forces armées en 1977. Dès le début de sa carrière, et en raison des fonctions dont il avait été investi, il a été confronté à la problématique des certificats de sécurité.

(1) Voir rapport d'activités - Comité R - 1995 p. 121.

Lorsqu'il avait rempli sa demande d'obtention d'un certificat de sécurité, il savait qu'une enquête de sécurité serait menée, et que le résultat de celle-ci serait déterminant pour obtenir un accès à une fonction classifiée.

Dans l'exercice de toutes ses fonctions, il lui fallait en tout temps disposer d'un certificat de sécurité. Après sa formation, il a rempli une fonction pour laquelle il avait obtenu un certificat de sécurité du niveau "secret".

Le 29 juillet 1996, il a été muté, à sa demande, vers une fonction pour laquelle un certificat de sécurité "Nato Cosmic Très Secret Atomal" était exigé.

Le 21 novembre 1996, son certificat de sécurité lui était retiré.

L'intéressé occupe à présent une fonction pour laquelle aucun certificat de sécurité n'est exigé. Il n'a jamais eu de démêlés avec la justice, ni fait l'objet de sévères mesures disciplinaires.

3.2.2. Situation familiale

Il s'est produit une modification de sa situation familiale. Il a été tenu d'en faire part à sa hiérarchie et, à cet égard, il a dû remplir une nouvelle demande d'obtention du certificat de sécurité.

3.2.3. Préjudice invoqué

En raison du retrait de son certificat de sécurité et de la perte de son emploi dans une organisation internationale, Monsieur Y déclare subir un préjudice d'un montant de 20.000 FB par mois, sans tenu compte des avantages accordés par des magasins hors taxes, dans lesquels il pouvait effectuer des achats.

Sur le plan moral, il se sent lésé par le fait qu'il ne peut plus exercer l'activité pour laquelle il a été formé, tout en ne sachant pas ce qui lui est reproché. En même temps, il a perdu l'estime de ses connaissances, tant à l'intérieur qu'à l'extérieur de l'armée.

Il a tenté de découvrir les raisons du retrait de son certificat de sécurité, mais sans y parvenir.

Il en a conclu qu'une injustice avait été commise à son encontre, et que ses droits de citoyen avaient été bafoués. Il a donné au syndicat l'autorisation d'entamer une procédure.

3.3. Le dossier détenu par le SGR/S

Le dossier de Monsieur Y en la possession du SGR a été examiné par le Service d'enquêtes du Comité R.

Monsieur Y est un soldat appartenant aux forces armées.

Tous les documents se réfèrent aux enquêtes de sécurité menées au fil des années.

3.4. Mode d'exécution de l'enquête de sécurité par le SGR/Gd et le SGR/CI

Sur requête du Comité R, le Service d'enquêtes a effectué des recherches sur la manière dont l'enquête de sécurité avait été menée.

4. CONSTATATIONS

1. Compte tenu du certificat de sécurité "Nato Cosmic Très Secret Atomal" nécessaire à Monsieur Y pour l'exercice de sa fonction dans une organisation internationale, la Sécurité Militaire s'est strictement conformée au document émanant de l'OTAN, qui régit la "sécurité" au sein de l'Organisation du Traité de l'Atlantique Nord.

2. Le fait que le certificat de sécurité a été retiré à Monsieur Y entraîne des répercussions sur la fonction qu'il a exercée précédemment, pour laquelle ce certificat de sécurité était également exigé. C'est pourquoi il a été muté dans une autre unité, pour y être investi d'une fonction pour laquelle aucun certificat de sécurité n'était requis.

3. Le retrait du certificat de sécurité de Monsieur Y n'a aucune influence sur la sécurité de son emploi dans les forces armées. Monsieur Y se plaint cependant qu'en raison de son changement de fonction, il perd environ 20.000 BEF par mois en avantages divers.

4. Le retrait du certificat de sécurité ne signifie pas pour autant que l'intéressé ne pourra plus jamais accéder à une fonction classifiée. Il est libre de postuler à l'avenir un poste pour lequel, après enquête, un nouveau certificat de sécurité pourra éventuellement lui être délivré.

5. En cas de refus ou de retrait d'un certificat de sécurité, la loi ne prévoit aucune procédure d'appel pour l'intéressé. Seule une requête introduite devant un tribunal compétent aurait pu contraindre l'Etat belge à communiquer à l'intéressé les raisons précises ayant motivé le retrait du certificat de sécurité[(2)].

6. D'après l'enquête de contrôle, il appert que les pièces figurant au dossier de Monsieur Y ne sont ni numérotées, ni inventoriées. Le SGR envisage de le faire après leur informatisation, actuellement en cours.

---

(2) Voir rapport d'activités du Comité R - 1995 - p. 133

5. CONCLUSIONS

- Le Comité R estime que le SGR n'a nullement porté atteinte, de manière illégitime ou injustifiée, aux droits et aux libertés du plaignant.

- Le syndicat fait remarquer, à juste titre, que les enquêtes de sécurité, lorsqu'elles ne sont pas menées sous le couvert de la loi, contreviennent à l'article 8 du Traité Européen des Droits de l'homme et à l'article 22 de la Constitution et que, par conséquent, il y a violation de la vie privée.

  En outre, le syndicat se plaint du fait que l'intéressé ne dispose d'aucune possibilité de recours contre le refus ou le retrait d'un certificat de sécurité. En ce qui concerne les arguments avancés par le syndicat, le Comité R se réfère à son rapport d'activités de 1995, plus particulièrement en ce qui concerne les enquêtes de contrôle en matière de certificats de sécurité[(3)].

- Le Comité R a recommandé que ces matières fassent d'urgence l'objet d'une législation, et qu'en cas de refus ou de retrait d'un certificat de sécurité, une procédure d'appel soit prévue.

- Le Comité R a connaissance de deux projets de loi se référant à ces matières, et il espère qu'une législation adaptée sera mise en place le plus rapidement possible.

(3) Voir rapport d'activités du Comité R - 1995 - pp. 112 à 137

CHAPITRE 2 : RAPPORT D'ENQUÊTE SUR LA DÉNONCIATION D'UN MEMBRE DE LA COMMISSION "SIRÈNE"

Avertissement

Les passages {...} figurant entre crochets concernent soit l'identité de personnes physiques qui, conformément à l'article 79 alinéa 2 du règlement d'ordre intérieur ne peuvent pas apparaître dans le rapport général d'activités du Comité R, soit des renseignements classifiés TRES SECRET, SECRET ou CONFIDENTIEL, lesquels ont été portés à la connaissance des ministres concernés par l'enquête de contrôle.

1. PROCÉDURE

Le 16 décembre 1997, M. {...} de la Commission Sirène adressa un écrit à la présidente du Comité R afin de dénoncer l'attitude de la Sûreté de l'Etat qui avait accordé "*un certificat de sécurité*" au nommé {X}, placé en détention préventive et inculpé de vol de documents.

Le Comité R décida d'ouvrir une enquête sur base de cette dénonciation en réunion du 18 décembre 1997.

Deux membres du Comité furent chargés de suivre cette enquête et d'informer régulièrement le Comité R de son suivi.

Le 30 décembre 1997, en application de l'article 46 § 3 du règlement d'ordre intérieur les présidents du Sénat et de la Chambre ont été avertis de l'ouverture de cette enquête.

Par apostille du 19 décembre 1997, le Comité R a chargé le chef du Service d'enquêtes de vérifier les conditions de l'octroi du certificat de sécurité, notamment en se renseignant auprès des responsables de la Commission "SIRENE", de l'Autorité Nationale de Sécurité et de la Sûreté de l'Etat.

Le 3 février 1998, l'enquête a été élargie en commun avec le Comité P. Cette enquête est toujours en cours. Elle concerne l'efficacité du S.G.A.P en matière de sécurité.

Le 6 février 1998, en application de l'article 43.1 de la loi du 18 juillet 1991, les ministres de la Justice et de la Défense nationale, ont été avisés de l'ouverture de l'enquête.

Le rapport d'enquête a été approuvé le 26 juin 1998 par le Comité R et transmis aux ministres compétents.

Malgré l'objection soulevée par le ministre de la Justice le Comité R a décidé en réunion du 17 août 1998 de publier le rapport.

2. PRINCIPAUX ACTES POSÉS PAR LE SERVICE D'ENQUÊTES

Plusieurs responsables des services de renseignement, du S.G.A.P, de l'Autorité Nationale de sécurité et de la Commission pour les Problèmes Nationaux de Défense ont été contactés ou interrogés par le Service d'enquêtes du Comité R.

3. INTÉRÊT PARLEMENTAIRE

Le 11 septembre 1996 - question n° 353 : Monsieur le député Jean Barzin(PRL) interpelle le ministre de la Justice afin de connaître les moyens de sécurité exigés par l'article 118 de la Convention d'Application de l'Accord de Schengen, destinés à assurer la protection de la vie privée dans le Système d'information Schengen. Il était également demandé de préciser si le Directeur de la Commission "SIRENE" "*dispose des moyens nécessaires pour régler les problèmes de sécurité et s'il dispose de l'autorité nécessaire à cet effet* " ?

Le 21 novembre 1997 - question n° 632 : Monsieur le sénateur Boutmans (AGALEV)demande au ministre de l'Intérieur de l'éclairer sur le statut des groupes de travail dont question dans le rapport de l'Autorité de Contrôle commune de Schengen.

Le 26 novembre 1997 - question n° 642 : le même parlementaire s'inquiète encore de la sécurité informatique, tant au niveau du C-S.I.S. qu'au niveau du N-S.I.S.

Le 15 décembre 1997 - interpellation n° 1.638 : Monsieur le député Frans Lozie (AGALEV) interpelle le ministre de la Justice sur "la découverte du fait que des informations du système "SIRENE" ont été transmises pendant une longue période aux milieux criminels".
Ce parlementaire déclare que" *le système est devenu incontrôlable notamment à la suite de la création du Service Général d'appui policier* ".

Le 8 décembre 1997, question orale n° 506 de Monsieur le député Marc van den Abeelen (VLD) au ministre de la Justice et au vice-premier ministre des Affaires étrangères sur “les conséquences de la fuite au sein du service belge d’appui policier SGAP”.
Le ministre de la Justice a fait la réponse suivante : “*La Sûreté de l’Etat n’a pas fait d’enquête sur l’intéressé. En revanche, un certificat OTAN a bien été délivré. L’affaire est actuellement à l’étude”.*

Le 2 mars 1998, question orale n° 701 de Monsieur Marc van den Abeelen au ministre de la Justice sur “*une (nouvelle ?) fuite au sein du SGAP”.*

4. NORME APPLICABLE À LA PROBLÉMATIQUE

Le 14 juin 1985, la Belgique, l’Allemagne, la France, le Grand Duché de Luxembourg et les Pays-Bas signent “***l’accord de Schengen***” destiné à assurer le libre franchissement des frontières par tous les ressortissants des Etats membres ainsi que la libre circulation des marchandises et des services.

Il faudra cinq années supplémentaires pour que cet accord devienne réalité dans le cadre de la signature de la “Convention d’Application de l’Accord de Schengen”, intervenue le 19 juin 1990. Cette convention du 19 juin 1990 a été ratifiée par la Belgique le 18 mars 1993.[(1)]

L’article 118-3° de la Convention d’Application de l’Accord de Schengen prévoit :

Version française :

“ **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****.”*

Version néerlandaise :

“ **3.** *Iedere Overeenkomstsluitende Partij wijst ten behoeve van de gegevensverwerking in het nationale deel van het Schengen-informatiesysteem slechts personen aan die een passende opleiding hebben genoten en een* ***veiligheidsonderzoek*** *hebben ondergaan.”*

(1) Moniteur Belge du 15 octobre 1993

Version allemande *:*

" **3.** *Jede Vertragspartei darf mit der Datenverbeitung in ihrem nationalen Teil des Schengerner Informationssystems nur Personen beauftragen, die besonder geschult und einer* ***Sicherheitsüberprüfung*** *unterzogen worden sind.*".

L'article 118 n'indique pas de quelle manière ni selon quels critères ce contrôle de sécurité est effectué. L'exécution de cette mesure est laissée à l'initiative et à l'application des autorités nationales.

La Convention d'Application de l'Accord de Schengen signée le 19 juin 1990 destiné à assurer le libre franchissement des frontières par tous les ressortissants des Etats membres ainsi que la libre circulation des marchandises et des services a été ratifiée par la Belgique le 31 mars 1993(2).

Auparavant, la Belgique a consacré cet accord international dans un protocole d'accord signé entre les ministres de la Justice et de l'Intérieur, intitulé "**mise en application du système d'information**", et ce, en date du 9 août 1991. Le protocole traduit les exigences consacrées dans l'article 108 de l'accord. Il est important de rappeler que ces règles internationales communes sont supérieures aux normes internes lesquelles ne peuvent interférer dans l'organisation, le fonctionnement et les missions de la commission "SIRENE", pour les matières qui ne relèvent pas de la compétence exclusive de chaque Etat signataire.

Dans ce protocole, les missions des diverses instances créées au sein du Système National d'Information Schengen (en abrégé N- S.I.S.) ont été définies et attribuées. Plus précisément, la part importante de la tâche fut attribuée à la Commission "SIRENE" et ce, en application de l'article 108 de la Convention d'application dont question ci-dessus.

La mission essentielle consiste à mettre , grâce à une procédure d'interrogation automatisée, des signalements de personnes, de véhicules ou d'objets à la disposition des autorités compétentes pour :

- assurer les contrôles frontaliers aux limites de l'espace Schengen;
- assurer les autres vérifications de police et de douanes exercées à l'intérieur de chaque pays membre et assurer la coordination de celles-ci;
- assurer la délivrance des visas, des titres de séjour et l'administration des étrangers.

(2) Moniteur Belge du 15 octobre 1993

Pour être plus précis, voici ce que prévoyait le protocole du 9 août 1991 en ce qui concerne la problématique de la présente enquête :

"Il est créé une commission chargée de la mise en oeuvre du système d'information. La commission est chargée des missions suivantes :

©…ª

9.- <u>Transférer les règles de sécurité physique et techniques prévues à l'article 118 de la convention dans le règlement d'exploitation du S.I.C.N (Système d'Informations Criminelles National) et de veiller, avec les services à leur application.</u>

Le 26 mars 1995, la Convention d'application de l'Accord de Schengen fut réellement d'application; la Commission "SIRENE", opérationnelle, est dotée d' une permanence de 24 heures sur 24.

Le 1er août 1994, l'arrêté royal du 11 juillet 1994, créant le Service général d'Appui Policier, entrait en vigueur. La Commission "SIRENE" était déjà intégrée dans cette nouvelle structure. Elle ne fut dès lors jamais autonome.

Le personnel qui relève du S.G.A.P est composé de :

1° *de* fonctionnaires de police ou de recherche spécialisés y désignés ou y détachés ;
Ils restent soumis à leur statut d'origine et conservent tous leurs droits de promotion dans le service dont ils sont détachés; lesquels ne font pas l'objet d'un contrôle de sécurité.

2° de personnel non fonctionnaire de police <u>statutaire ou contractuel</u> mis à disposition, en ce compris le personnel administratif et technique (...); lesquels par contre font l'objet d'un contrôle de sécurité.

M. {X} appartenait à cette dernière catégorie.

Le Service d'enquêtes a examiné de quelle manière cette norme avait été appliquée lors de l'engagement de {X} en qualité de juriste contractuel.

Le Service d'enquêtes n' a pas trouvé pour l'heure d'autres dispositions normatives sur le principe et le déroulement des enquêtes de sécurité demandées par la Commission "SIRENE", que ce soit dans le premier protocole du 9 août 1991, signé par les ministres de la Justice et de l'Intérieur instituant la Commission "SIRENE"., ou dans celui du 10 mars 1997 qui règle l'intégration définitive de la Commission "SIRENE" au sein de la division "***C****oopération* ***P****olicière* ***I****nternationale* " du Service Général d'Appui Policier.

Conformément à la philosophie de la Convention cette disposition allait donc être interprétée et appliquée souverainement par les responsables des diverses Commissions “SIRENE” des états membres.

En ce qui concerne la Commission “SIRENE” belge, les constatations du Service d’enquêtes sont les suivantes :

a) la traduction du texte de l’article 118-3° dans nos trois langues nationales permet déjà une interprétation très différente de la norme. En effet, le texte en langue française parle explicitement de “personnes spécialement qualifiées et soumises à un contrôle de sécurité” tandis que le texte néerlandais, tout comme la version allemande d’ailleurs, exige des “personnes ayant fait l’objet d’une enquête de sécurité” (“veiligheidsonderzoek”).

   On se rapportera utilement aux développements de l’enquête de contrôle du Comité R et de l’étude qu’il a menée au sujet du projet de loi relatif aux habilitations de sécurité à propos de l’importance de la définition exacte d’une enquête de sécurité.(3)

   Il est toutefois évident qu’un contrôle de sécurité peut être légitimement effectué par l’organisme recruteur lui-même et selon ses propres critères tandis qu’une enquête de sécurité présuppose un organisme indépendant , spécialisé dans la problématique et doté d’une vision plus générale au niveau des critères d’octroi ou de retrait d’habilitation de sécurité selon le niveau de l’habilitation.

   Conscient de l’absence de norme dans la législation belge en matière d’enquêtes de sécurité, le gouvernement s’est attelé à la tâche et un projet de loi relatif aux habilitations de sécurité est toujours en discussion devant le Parlement.

b) La différence de traitement entre le personnel “civil” et “policier” est le résultat d’une interprétation personnelle de la direction de la Commission “SIRENE” belge.

   Rappelons en effet qu’il appert des investigations que les responsables de la Commission “SIRENE”, dès son origine et actuellement encore, estiment que les policiers sont présumés remplir d’office, de par leur qualité, les conditions prévues à l’article 118-3°.

(3) Rapport d’activités du Comité R 1995, page 112.

5. CONSTATATIONS

Pour mémoire, le Comité R renvoie le lecteur au rapport de l'enquête de contrôle sur la problématique des certificats de sécurité publié dans son rapport annuel de 1995 page 112 et suivantes.

Dans la présente enquête, le Comité R constate que :

1) à propos de l'octroi de certificats de sécurité au personnel de la commission "SIRENE" en général :

- il existe une différence de traduction du texte de l'article 118-3° de la Convention de Schengen dans les trois langues nationales qui permet une interprétation très différente de la norme : dans la terminologie des services de renseignement, les termes français *"contrôle de sécurité"* n'impliquent pas une vérification aussi approfondie que les termes *"veiligheidsonderzoek (enquête de sécurité)"* utilisés dans les textes néerlandais et allemands;

- il existe, et ce sans base légale sur la problématique des enquêtes de sécurité en Belgique, une tradition de collaboration de la Sûreté de l'Etat dans les enquêtes de moralité effectuées pour des candidats à certaines fonctions dans des services de police. Ainsi, la Sûreté de l'Etat a accepté de répondre jusqu'à la fin du mois de septembre 1997 à des demandes d'enquêtes de sécurité émanant du chef de division "Coopération Policière Internationale" ainsi que du SGAP et ce, sur base de l'article 118-3° de la Convention d'application de l'Accord de Schengen. Cette collaboration, à la date d'avril 1998, perdure;

- pour l'octroi d'une habilitation de niveau "SECRET", les services de renseignement se bornent à vérifier leur documentation interne ainsi que le casier judiciaire de l'intéressé; il s'agit d'un contrôle de sécurité et il n'est pas procédé à d'autres vérifications en l'absence d'éléments défavorables;

- seul l'octroi d'une habilitation de niveau "TRES SECRET" exige qu'une véritable enquête de sécurité soit systématiquement menée par les services extérieurs des services de renseignement en collaboration avec la police locale, etc....

- il existe, à l'initiative de la direction de la commission "SIRENE", une différence de traitement entre le personnel civil et le personnel policier : les policiers sont présumés remplir d'office, par leur qualité, les conditions prévues à l'article 118-3°.

2) concernant {X} en particulier :

- dans un premier temps, la commission “SIRENE” n’a pas estimé utile de faire procéder à une enquête ou à un contrôle de sécurité à son sujet;

- la Commission “SIRENE” a adressé une demande de certificat de sécurité à la Sûreté de l’Etat pour 16 civils dont ne faisait pas partie {X}; la Sûreté de l’Etat a répondu qu’il fallait s’adresser à l’A.N.S.. Ensuite la Sûreté des l’Etat a pris l’initiative de n’effectuer qu’un contrôle de niveau “SECRET” alors que l’A.N.S. avait prescrit une enquête de niveau “TRES SECRET”;

- la Commission “SIRENE” s’est ensuite directement adressée à la Sûreté de l’Etat pour qu’elle effectue une enquête de sécurité au sujet de {X}. En ce qui concerne {X}, la Sûreté de l’Etat a directement répondu à la Commission “SIRENE” en lui signalant que l’intéressé n’était pas connu de ses services, sans passer par l’ANS ce qui est la procédure habituelle;

- le contrôle effectué par la Sûreté de l’Etat sur {X} pour répondre à la Commission “SIRENE” est donc conforme à celui qu’elle réalise pour répondre aux demandes d’enquêtes de sécurité de niveau “SECRET” introduites par l’ANS, à savoir la vérification de sa documentation interne et la consultation du casier judiciaire;

- l’Autorité Nationale de Sécurité n’a jamais reçu de demande d’enquête de sécurité et n’a donc jamais fait procéder à une enquête de sécurité au sujet du nommé {X};

- il faut donc relativiser les déclarations de l’administrateur général de la Sûreté de l’Etat suivant lesquelles :

  1) “la Sûreté de l’Etat ne dispose d’aucune base légale pour effectuer des enquêtes de sécurité ou pour délivrer des certificats de sécurité au bénéfice des services de police”.

  Au niveau formel, c’est tout à fait exact, comme il est vrai que les autres missions habituelles de la Sûreté de l’Etat ne sont pas définies par la loi.

2) *"la vérification ponctuelle effectuée par la Sûreté de l'Etat ne peut être considérée comme une enquête de sécurité et encore moins comme un certificat de sécurité".*

Les circonstances de l'affaire et la collaboration que ce service apporte habituellement à l'octroi de certificats de sécurité permettent au directeur a.i. de la Commission"SIRENE" de l'époque de soutenir qu'à son estime, la réponse de la Sûreté de l'Etat concernant {X} équivalait à lui octroyer une habilitation de sécurité du niveau "SECRET".

- par ailleurs {X} n'a jamais été titulaire d'un quelconque certificat de sécurité OTAN délivré lors de ses obligations militaires : l'intéressé est totalement inconnu de la documentation du SGR.

En conclusions, le Comité R estime que malgré le chemin peu orthodoxe pris pour satisfaire aux exigences de l'article 118-3° de la Convention d'Application de l'Accord de Schengen, une enquête de sécurité de niveau "SECRET" a été effectuée au sujet de {X}. Cette enquête a été effectuée en 1993, les faits dont il est suspecté ont été commis dans le courant de l'année 1995 et ils ont été découverts en 1997.

6. RECOMMANDATIONS

1. Est-il encore besoin d'insister sur l'extrême urgence d'une législation en matière d'habilitations de sécurité ?
   Un projet de loi existe, terminé sur le plan de la technique rédactionnelle. Il ne reste qu'à le finaliser dans les meilleurs délais afin de mettre un terme définitif à la diversité et l'incertitude des procédures utilisées en cette matière.

2. L'affaire {X} a démontré l'importance des enquêtes de sécurité et de la nécessité de détecter, à temps, des facteurs de risques.
   Dans ces conditions, l'ensemble du personnel, ayant accès aux données du système d'information Schengen, tant civil que policier, doit être soumis à une enquête de type approfondi, c'est-à-dire en vue de l'obtention d'un certificat de sécurité de niveau "TRÈS SECRET".
   La simple vérification de fichiers n'est pas suffisante pas plus que la dispense d'une catégorie de personnel (policiers) n'est justifiable.

3. Il convient de mettre en concordance, et ce d'urgence, les traductions des textes suivants afin de définir correctement les responsabilités et missions de chacun :

   - l'article 118-3° de la Convention d'Application de l'Accord de Schengen;

   - dans le cadre de l'application 118-3° ci-dessus cité le Comité R recommande que la Sûreté de l'Etat soit consultée via l'ANS à propos de tout le personnel "SIRENE";

4. Le Comité R recommande que toute personne ayant accès aux données du service d'information "SIRENE" soit soumise à une enquête de sécurité préalable à un certificat de sécurité que seule l'ANS pourra délivrer.

CHAPITRE 3 : ENQUÊTE DE CONTRÔLE CONCERNANT MONSIEUR X

1. PROCEDURE

Par lettre du 9 février 1998, un syndicat a fait parvenir à la Présidente du Comité R une plainte contre le SGR à propos du retrait illicite d'un certificat de sécurité et de la violation des droits constitutionnels et légaux d'un militaire.

Le syndicat a été consulté par Monsieur X et agissant en tant qu'organisation syndicale, il a porté plainte, au nom de l'intéressé, contre le SGR, parce que ce service avait retiré à tort à l'intéressé son certificat de sécurité et refusait de lui communiquer les motifs de ce retrait.

Le 22 avril 1997, le certificat de sécurité - niveau 'secret' - de l'intéressé a été retiré et il a été éloigné de sa fonction.

Au cours de sa réunion du 19 février 1998, le Comité R a ouvert une enquête de contrôle sur base de la plainte d'un particulier à propos du refus / retrait d'un certificat de sécurité. A cette date, le Comité R a chargé l'un de ses membres de mener cette enquête et de remettre des rapports réguliers au Comité R sur l'évolution de cette enquête.

Dans une apostille du 20 février 1998, le Comité R a prié le Chef du Service d'enquêtes de convoquer Monsieur X pour qu'il vienne personnellement porter plainte auprès du Comité R.

Monsieur X a été entendu le 2 mars 1998 par le Service d'enquêtes.

Le 4 mars 1998, une apostille a été transmise au Chef du Service d'enquêtes le priant de prendre connaissance du dossier de l'intéressé auprès du SGR et d'examiner en détail, sur base dudit dossier, de quelle manière l'enquête de sécurité a été menée.

Conformément à l'article 46, alinéa 3 du règlement d'ordre intérieur du Comité R, les présidents de la Chambre et du Sénat ont été mis au courant de l'ouverture de l'enquête par lettre du 4 mars 1998.

Conformément à l'article 43, alinéa 1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le Chef du Service d'enquêtes a mis le ministre de la Défense nationale au courant de l'ouverture de l'enquête par lettre du 4 mars 1998.

Un accusé de réception a été envoyé le 4 mars 1998 à Monsieur X. Dans cet accusé de réception, il lui a été confirmé que le Comité R vérifierait le bien-fondé de sa plainte et qu'à l'issue de l'enquête, il serait informé de la décision prise par le Comité R.

Le 14 mai 1998, une apostille subséquente a été transmise au Chef du Service d'enquêtes.

2. DIRECTIVES

Pour exécuter l'enquête de sécurité, le SGR s'est basé sur un document édité par l'OTAN, le C-M 55 (15) Définitif, qui règle la 'Sécurité' au sein de l'Organisation du Traité de l'Atlantique Nord.

Ce document définit certains critères auxquels le candidat doit satisfaire et qui doivent être contrôlés par l'autorité délivrant le certificat de sécurité.

3. DEROULEMENT DE L'ENQUETE

3.1. Audition de Monsieur X le 2 mars 1998

Monsieur X est entré à l'Armée et a été incorporé dans la Force aérienne. Dès le début de sa carrière, il a été confronté à la problématique des certificats de sécurité. Il savait qu'une enquête de sécurité était effectuée lorsqu'on complétait une demande en vue d'obtenir un certificat de sécurité.

Il occupait une fonction pour laquelle il devait disposer d'un certificat de sécurité de niveau 'secret'.

En 1997, il a été privé de son certificat de sécurité et éloigné de sa fonction. Actuellement, il est employé dans une fonction logistique pour laquelle il n'a pas besoin d'un certificat de sécurité. Il n'a jamais pu connaître le motif pour lequel on lui avait retiré son certificat de sécurité.

Comme il a été éloigné d'une fonction classifiée, il s'est senti indûment lésé et trouve que ses collègues de travail le considèrent différemment. Il en subit un préjudice moral.

Il appert que l' intéressé n'a pas subi de perte financière. Il veut seulement savoir pour quel motif on lui a retiré son certificat de sécurité.

3.2. Dossier auprès du SGR/S

Le dossier de Monsieur X auprès du SGR/SM a été examiné par le Service d' enquêtes du Comité R.

La plupart de ces documents portent sur des demandes d'un certificat de sécurité et sur les enquêtes de sécurité qui en résultent.

A la demande du Comité R, le Service d'enquêtes a examiné la manière dont l'enquête de sécurité a été effectuée.

Il ressort du dossier que le plaignant a été condamné à une peine correctionnelle.

3.3. Entretien avec le Chef de Corps et avec l'officier de sécurité de l'unité du plaignant

Le Service d'enquêtes du Comité R a pris connaissance du dossier de sécurité du plaignant et a eu un entretien avec le Chef de Corps et avec l'officier de sécurité de son unité.

La non-reconduction du certificat de sécurité a eu comme conséquence, pour le plaignant, qu'il a été retiré de sa fonction parce que, du fait de la non-reconduction:

- il ne pouvait prendre connaissance d'informations classifiées;

- il ne peut être désigné pour fonctionner ou continuer à fonctionner dans une unité protégée ou dans une fonction classifiée.

Le Service d' enquêtes du Comité R a par ailleurs appris que sur le plan militaire, Monsieur X était apprécié par ses supérieurs directs comme étant un bon militaire, correct et poli, qui exécute son travail correctement. Il n'avait pas encouru de sanctions disciplinaires.
Il était peu souple dans ses relations avec ses égaux et avec ses subordonnés, ce qui a entraîné des frictions tant à l'intérieur qu'à l'extérieur de son cercle de travail.

3.4. "Jurisprudence" du SGR/S en matière de certificats de sécurité

L'officier/lecteur auprès du SGR/SM base sa décision sur l'octroi ou non d'un certificat de sécurité sur les éléments qui ressortent de l'enquête de sécurité et sur la comparaison de ceux-ci avec les critères énoncés dans le document de l'OTAN.

4. CONSTATATIONS

1. Compte tenu du certificat de sécurité de niveau 'secret' qui était nécessaire pour exercer sa fonction dans une zone classifiée, la Sécurité Militaire a appliqué de façon stricte le point 26 du "C-M 55 (15) Définitif".

2. Le plaignant a été condamné à une peine correctionnelle d'emprisonnement.

3. Le retrait du certificat de sécurité de Monsieur X n'a aucun impact sur sa sécurité d'emploi auprès de l'Armée. Il a été muté dans un autre poste qui ne nécessite pas de certificat de sécurité.
   Le motif du retrait de son certificat de sécurité ne lui a pas été communiqué. Monsieur X n'a pas subi de perte financière mais se plaint de ce qu'il se sent lésé moralement du fait de la perte de son certificat de sécurité.

4. Le retrait du certificat de sécurité ne signifie pas non plus que l'intéressé ne puisse plus jamais exercer de fonction classifiée. Il a la possibilité de continuer à postuler étant donné qu'un nouveau certificat de sécurité lui sera éventuellement délivré après enquête.

5. La loi ne prévoit aucune procédure de recours pour l'intéressé en cas de refus ou de retrait d'un certificat de sécurité. Seule une action introduite devant un tribunal compétent aurait pu obliger l'Etat belge à communiquer à l'intéressé le motif précis à la base du retrait de son certificat de sécurité[1].

6. Il ressort de cet examen de contrôle que les pièces du dossier de Monsieur X n'ont été ni numérotées ni inventoriées. Le SGR a l'intention de combler cette lacune lorsque l'informatisation en cours sera terminée.

5. CONCLUSIONS

1. Le Comité R est d'avis que le SGR n'a nullement violé les droits et libertés du plaignant de façon déraisonnable.

2. C'est à bon droit que le syndicat fait remarquer que l'exécution d'enquêtes de sécurité non réglementée par la loi est contraire à l'article 8 de la Convention Européenne des droits de l'Homme et à l'article 22 de la Constitution, et que ces enquêtes constituent dès lors des violations de la vie privée. De plus, il dénonce également le fait que l'intéressé ne dispose d'aucun moyen de recours contre le refus ou le retrait d'un certificat de sécurité.

   Le Comité R est d'avis en l'espèce que le plaignant devrait pouvoir prendre connaissance du motif du retrait de son certificat de sécurité.

   En ce qui concerne l'argumentation développée par le syndicat, le Comité R renvoie à son rapport d'activités de 1995, et notamment à l'examen de contrôle relatif aux certificats de sécurité[2].

   Le Comité R a recommandé de promulguer d'urgence une loi sur cette matière et de prévoir en même temps une procédure de recours en cas de refus ou de retrait d'un certificat de sécurité.

3. Le Comité R a donné son avis sur les deux projets de loi relatifs à cette matière et espère que le législateur apportera une réponse appropriée dans les plus brefs délais.

---

(1) Rapport d'activités Comité R - 1995, Titre II, Chapitre 2, p. 133 - *"Tribunal de première instance".*

(2) Rapport d'activités Comité R -1995, Titre II, Chapitre 2, pp. 112-137 - *"Certificats de sécurité"*

TITRE III : CONTACTS DU COMITE

CHAPITRE 1 : RENCONTRE AVEC LA COMMISSION NATIONALE DE CONTRÔLE DES INTERCEPTIONS DE SÉCURITÉ (CNCIS)

1. INTRODUCTION

La Belgique est un des rares pays à ne permettre aucune interception administrative des communications téléphoniques. Ainsi, notre législateur a voulu consacrer, de façon presque absolue, l'interdiction de ce type d'interception.

En effet, seuls les juges d'instruction ont la possibilité d'obtenir, en vertu de l'article 88 bis, 90 ter à 90 deciès du Code d'instruction criminelle, le repérage et l'écoute de communications téléphoniques.

La révision de cet article fait actuellement l'objet de débats au Parlement : un projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées a été déposé à la Chambre des Représentants.

Pour cette raison, le Comité R a recommandé dans son rapport annuel d'activités 1997[(1)] *"de revoir la législation pour permettre le recours aux écoutes de sécurité, mais avec de solides garanties de contrôle et de recours pour le citoyen."*

Le Comité R n'ignore pas que le gouvernement prépare un avant-projet de loi qui autorise les écoutes de sécurité. Il s'en réjouit.

Il a estimé que, conformément à ses missions légales, ses préoccupations devaient porter sur l'aide qu'il devait apporter au Parlement pour qu'une loi s'inspirant sur ce qui est prévu dans les autres pays européens soit votée le plus rapidement possible et que cette loi soit motivée en faisant la balance entre les intérêts de l'Etat et ceux du citoyen.

A cette fin, un membre du Comité R s'est rendu en France le 28 novembre 1997 où il a rencontré le président de la Commission nationale des interceptions de sécurité et ses collaborateurs.

---

(1) Rapport d'activités du Comité R - 1997- "*Bilan de quatre années de contrôle et de recommandations"*
p. 265.

2. LA LOI N° 91- 646 DU 10 JUILLET 1991

2.1. Aperçu historique

La problématique des écoutes téléphoniques administratives a fait l'objet de débats et de rapports pendant environ 12 ans en France.

Les Arrêts Kruslin et Huvig de la Cour européenne des droits de l'homme ont amené l'Etat français à adopter une législation spécifique permettant de protéger la vie privée des citoyens des atteintes irrégulières pouvant être commises au moyen d'interceptions de communications téléphoniques.

C'est dans ce contexte que le gouvernement français a déposé devant l'Assemblée nationale le projet de loi n° 2068 relatif au secret des correspondances émises par la voie des télécommunications qui devait aboutir à la loi n° 91-646 du 10 juillet 1991.

2.2. La loi relative au secret des correspondances émises par la voie des télécommunications

Seul le titre II de la loi est consacré aux interceptions de sécurité. Le Comité R estime qu'il est d'intérêt mineur de livrer le texte concernant les interceptions ordonnées par l'autorité judiciaire au lecteur d'un rapport établi par un Comité qui contrôle les services de renseignement. Le texte de cette loi relative aux interceptions ordonnées par l'autorité judiciaire se trouve à la disposition de toute personne qui souhaite en prendre connaissance au greffe du Comité R.

2.2.1. Champ d'application de la loi

La loi (article 3) autorise à titre exceptionnel les interceptions de sécurité dans le but de *"rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées."*

2.2.2. Pouvoir décisionnel

Le Premier ministre, sur proposition des ministres de l'Intérieur, de la Défense et du ministre chargé des Douanes a seul le pouvoir d'autoriser ce type d'interceptions. Sa décision doit être écrite et motivée (article 4).

2.2.3. Contingent

Le Premier ministre fixe le nombre d'interceptions susceptibles d'être pratiquées et sa répartition entre les différents ministres faisant les propositions d'interceptions de sécurité (article 5).

Les services sont ainsi disciplinés à ne pas procéder à des écoutes sans fin et parfois sans justification légale.

2.2.4. Durée

Les autorisations d'interceptions de sécurité ne peuvent être données que pour une période maximum renouvelable de quatre mois (article 6).

2.2.5. Procédure d'application

Seuls les renseignements en relation avec l'objectif fixé à l'article 3 de la loi peuvent faire l'objet d'une transcription (article 8). Le relevé des opérations mentionne la date et l'heure des interceptions. Les enregistrements sont détruits (articles 9 et 12).

La loi désigne le personnel travaillant sous la tutelle du ministre des télécommunications comme seules habilitées à exécuter les interceptions et sur ordre de ce ministre (article 11).
Les personnes appelées à intervenir dans la réalisation d'une interception ne sont pas directement placées sous sa tutelle.

Dans les faits, le ministère n'entretient de relations directes qu'avec des entreprises et leurs responsables. Les agents qui exécutent les opérations matérielles ne sont liés qu'à leur employeur.

Il faut cependant noter qu'ils s'exposeraient, en application des règles protégeant le secret professionnel, à des sanctions pénales en cas de révélation de l'existence d'une interception (article 26 de la loi).

L'énumération de l'article 11 rappelle que tout organisme, toute entreprise qui intervient dans le domaine des télécommunications peut être requis, sur ordre du ministre chargé des télécommunications, de prêter son concours à la réalisation d'interceptions de sécurité.

Il est également précisé que, parmi les agents ou employés de ces organismes et de ses entreprises, seuls ceux qui sont "qualifiés" peuvent réaliser matériellement les opérations nécessaires à la mise en oeuvre de l'interception.

2.2.6. Dispositions communes

Les personnes physiques ou morales exploitant des réseaux de télécommunications ou fournisseurs de services de télécommunication sont tenus sous peines de peine de prison et d'amende de fournir les informations et documents qui sont nécessaires aux interceptions de sécurité.

L'article 22 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications ne semble pas avoir écarté dans sa totalité la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Parmi les dispositions de la loi du 6 janvier 1978, est seul évoqué l'article 44, dont la substance a été reprise, depuis le 1er mars 1994, dans l'article 226-21 du nouveau code pénal.

L'article 22 exempte seulement de toute responsabilité pénale l'exploitant de réseau ou le fournisseur de services de télécommunications qui est amené, pour répondre aux demandes de renseignements que lui adressent les autorités compétentes en matière d'interceptions de sécurité, à communiquer à celles-ci les données personnelles enregistrées dans ses fichiers de gestion, alors que telle n'est pas la finalité de ces informations.

2.2.7. Les écoutes sauvages

La loi instaure une réglementation et soumet à l'autorisation du Premier ministre la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente des appareils permettant les interceptions de sécurité (article 24).

Cette loi modifie aussi le code pénal (article 226-3) en y insérant des peines d'un an d'emprisonnement et 300.000 FF d'amende pour toutes les personnes physiques ou morales qui enfreindrait cette législation.

Il convient d'ajouter que l'article 226-3 du code pénal, qui a succédé le 1er mars 1994 à l'article 371 de l'ancien code pénal, ne concerne pas seulement les appareils permettant les interceptions de sécurité.

Ainsi qu'il est précisé au paragraphe suivant du compte rendu, le champ d'application de cette disposition s'étend en effet à l'ensemble des appareils qui permettent de capter, d'enregistrer ou de transmettre des paroles prononcées à titre privé ou confidentiel.

Une liste des appareils est établie et arrêtée par le Premier ministre (article R 226-1 du code pénal, partie réglementaire et non pas, directement, des dispositions législatives de ce code).

Le code pénal vise également les captations, enregistrements et transmissions des paroles prononcées à titre privé ou confidentiel, sans le consentement de leur auteur.

Cette disposition est conforme au respect de la vie privée et ne concerne pas les autorisations données par le Premier ministre dans le cadre de la loi du 10 juillet 1991.

L'action publique ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droits.

3. LE CONTRÔLE

La loi relative au secret des correspondances émises par la voie des télécommunications inclut la création d'un organe de contrôle (article 13 de la loi mentionnée ci-dessus), composé d'un collège restreint en vue de préserver la confidentialité de ses travaux. Ce contrôle vise à éviter des comportements contestables de la part du gouvernement.

La Commission nationale de contrôle des interceptions de sécurité constitue une autorité administrative indépendante. Elle bénéficie d'une dotation prise sur le budget du Premier ministre.

Le président de la Commission est nommé par le président de la République pour une durée de six ans. Le choix du chef de l'Etat s'exerce parmi les quatre noms que lui proposent conjointement le Premier Président de la Cour de Cassation et le Vice-président du Conseil d'Etat.

Les deux autres membres de la commission, un député de l'opposition et un sénateur de la majorité sont désignés respectivement par le président de l'Assemblée et le président du Sénat.

Les mandats ne se recoupent pas afin d'assurer la continuité du service. Il n'existe pas de commissaire du gouvernement désigné par le Premier ministre auprès de la Commission, comme il en existe un auprès de la Commission nationale de l'informatique et des libertés.

De fait, la Commission nationale des interceptions de sécurité se compose d'un délégué général (magistrat), d'un chargé de mission (magistrat), de deux secrétaires, d'un ingénieur en télécommunications suite à une décision administrative de 1991 qui a été rapportée en 1998 et d'un chauffeur.

Dans la mesure où de telles compétences (ingénieur en télécommunications) seraient nécessaires à la réalisation de ses missions, la Commission nationale des interceptions de sécurité recourait à des experts.

La Commission a pour mission de veiller au respect des dispositions légales concernant l'autorisation et la réalisation des mesures d'interceptions. Cinq motifs légaux sont prévus à l'article 3 de la loi, permettant d'autoriser des interceptions de sécurité.

Deux procédures distinctes sont prévues :

* Le président de la Commission est informé, dans les 48 heures suivant la décision, de toutes les autorisations d'interceptions décidées par le Premier ministre (article 14).

Si la mesure semble soulever un problème de légalité, le président de la Commission en informe la Commission qui le cas échéant adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Le Premier ministre doit informer la Commission des suites données à sa recommandation. Il peut passer outre l'avis de la Commission qui fera état du désaccord dans son rapport annuel.

A l'heure actuelle, environ cinq désaccords francs par an ont été portés à la connaissance du public selon les dires du président de la Commission nationale de contrôle des interceptions de sécurité. La plupart de ces cas sont jugés des "cas limites" par la Commission.

Page 22 de son troisième rapport d'activités, la Commission nationale des interceptions de sécurité précise qu'il s'agit de cas *"dont on peut dire qu'ils sont étrangers aux prévisions de la loi et pour lesquels la responsabilité particulière du pouvoir exécutif peut expliquer une appréciation différente de celle de la commission"*.

Il est ajouté que *" la commission, si elle partage le souci de ne pas priver l'Etat de moyens d'information prévus par la loi, estime que son rôle propre doit, dans les cas-limites, la conduire à s'en tenir à un avis négatif, au nom du caractère exceptionnel des interceptions, lorsqu'il n'y a pas d'élément impératif de décision contraire".*

* La Commission peut d'initiative ou sur plainte d'un particulier (article 15) y ayant un intérêt direct et personnel, vérifier la légalité de toute interception en cours. Une recommandation peut être prise immédiatement tendant à faire cesser l'interception litigieuse. Le particulier est avisé *"qu'il a été procédé aux vérifications nécessaires".*

Enfin chaque année, la Commission remet au Premier ministre un rapport d'activités qui est rendu public. Ce rapport contient des recommandations. La Commission ne dispose pas, tout comme le Comité R, de pouvoir de sanction.

Les recommandations faites par la Commission ont un effet de dissuasion sur le Premier ministre qui n'entend pas être trop critiqué par ladite Commission. C'est ainsi que le nombre de désaccords francs est limité, comme indiqué ci-dessus.

4. EVOLUTION DU CONTRÔLE

4.1. Compétence étendue du président de la Commission

La loi prévoit un contrôle a posteriori des autorisations d'interceptions de communications téléphoniques.

Toutefois, ces dernières années cette compétence s'est muée en un contrôle a priori et ce avant la lettre : le président de la Commission est consulté par le Premier ministre avant de prendre la décision de mettre un particulier sous écoutes téléphoniques.

4.2. Ecoutes individuelles

Le contrôle de l'application de la loi se fait non seulement sur le temps de gardiennage des enregistrements mais également sur les transcriptions des écoutes de sécurité.

Depuis 1996, la Commission nationale de contrôle des interceptions de sécurité s'est engagée, sur demande du Premier ministre dans le contrôle du matériel dont il a été question ci-dessus.

Le décret du 10 juillet 1997 modifiant les articles R.226-1 et suivants du code pénal a officialisé cette mission de la CNCIS.

Un projet de loi visant à réformer la procédure de "secret défense" sur proposition d'Alain Richard, ministre de la défense, a été approuvé par le conseil des ministres le 17 décembre 1997 et déposé à l'Assemblée nationale.

Ce texte tend à donner au président de la CNCIS une nouvelle compétence concernant le contrôle de l'application du concept, non encore défini de "secret défense".

A propos de cette problématique le Comité R renvoie le lecteur au chapitre concernant "le secret".

CHAPITRE 2 : COLLOQUE SUR LES NOUVELLES PRATIQUES DE LA COMPÉTITIVITÉ INTELLIGENCE

1. INTRODUCTION

Dans le cadre de son enquête sur la nouvelle mission de la Sûreté de l'Etat, le Comité R a décidé d'envoyer un de ses membres assister au colloque organisé par la société 'Development Institute International' les 25 et 26 février 1998 à Paris.

Ce colloque était surtout destiné à des employés de firmes qui pratiquent l'intelligence économique concurrentielle (IEC).

2. LES EXPOSÉS

Divers orateurs ont pris la parole sur les thèmes suivants :

- *"Introduction aux structures d'IEC"*
  par Daniel Rouach, professeur à l'école européenne des affaires, chambre de commerce et d'industrie de Paris ;

Ce premier orateur, auteur d'ouvrages traitant de ce secteur des entreprises tel que *"la veille technologique et l'intelligence économique"* paru dans la collection *"Que sais-je ?"* aux presses universitaires de France en 1996, a décrit comment une veille technologique et concurrentielle efficace peut contribuer à l'amélioration des capacités innovatrices de l'entreprise, et renforcer ainsi l'impact du transfert de technologie sur ses performances.

Cet éminent professeur a donné de la veille technologique la définition suivante :

"Art de repérer, collecter, traiter, stocker des informations et des signaux pertinents (faibles, forts) qui vont irriguer l'entreprise et permettre d'orienter le futur. Elle permet de protéger le présent et l'avenir face aux attaques de la concurrence. Se pratique dans la légalité et le respect des règles de déontologie."

Il a ensuite détaillé sa conception de la problématique en décrivant la pyramide de la veille (ce que le Comité R fait sous le vocable le cycle du renseignement économique dans l'enquête qu'il a mené sur la protection du potentiel scientifique ou économique) pour enfin énumérer et définir le rôle des acteurs de la veille.

‘ *“Passez de la veille concurrentielle à la cellule de stratégie opérationnelle en créant et pilotant votre nouvel outil IEC”*,
par Benoît Gougeon manager of Competitive marketing , IBM Europe.

Cet orateur a expliqué le travail qu’il effectuait dans ce secteur au sein de la société IBM en abordant les questions suivantes :

* comment vendre à votre Direction Générale votre projet de cellule IEC ;

* évaluer les différentes catégories d’intelligences nécessaires à votre entreprise ;

* assurer la circulation transversale de l’information entre les groupes de travail ;

* contrôler les retours et les demandes d’information des différents services de l’entreprise ;

* établir un budget pour les investissements et charges.

‘ *“Identifiez et exploitez les nouvelles sources publiques de collecte d’information”*
par Gilbert Croze, directeur du Bureau régional d’information scientifique et technique à Paris;

Monsieur Croze a exposé l’utilité des sources ouvertes pour limiter le budget de la firme en obtenant un résultat efficace.

Les organismes cités comme spécialisés dans ce domaine sont les suivants : Arist, Adit, Anvar, Critt, CTI, les administrations centrales et locales, les chambres de commerce et d’industrie, et les Euro Info centres.

‘ *“Pourquoi et comment externaliser vos services d’intelligence économique”*
par Yves-Michel Peyrache, JITEX - International Technology & Strategy Experts;

Monsieur Peyrache a attiré l’attention des participants au séminaire sur l’importance qu’il y avait à tirer parti des réseaux d’informations extérieurs à l’entreprise et à généraliser les méthodes pratiquées au Japon, pays pionnier en la matière.

‘ *“Sécurisez un routage rapide et exhaustif des informations confidentielles ou gérez les réseaux internes pour une diffusion optimale”*
par Robert Guillaumont, Président Directeur Général, INFORMA;

Au cours de cet exposé l’accent a été mis sur la problématique de la sécurité du système informatique de l’entreprise, sur la formation du personnel à des réflexes de sécurité et sur l’obligation qu’il y avait de faciliter la prévention en instaurant un système de contrôle au préalable.

‘ *“Sensibilisez vos employés à la recherche spontanée d’informations grise”*

C’est-à-dire non accessible à tout un chacun en essayant de vaincre les réticences au concept même d’intelligence économique, en enseignant à tout le personnel les réflexes de l’IEC et en traduisant les informations collectées, constitue l’essentiel du discours tenu par Olivier Juif, chef Produits visuels de la société SHARP.

‘ *“Traitement d’informations: enrichissez vos données en leur apportant une valeur ajoutée”*

Des méthodes de travail telles que la maîtrise de nouveaux instruments, ont été évoquées. Les nouveaux instruments cités furent les logiciels, la bibliométrie, les matrices et études d’opinion au système décisionnel et surtout l’exploitation du centre de documentation comme un centre de développement.

Cet exposé a été donné par Joachim Fernandez responsable des études marketing de la banque cantonale de Genève, qui n’a pas hésité à considérer la banque où il travaille de PME étant donné qu’elle emploie 900 personnes.

‘ Jean-Claude Salomon, chargé de mission relations internationales à l’Institut des Hautes Etudes de la Sécurité Intérieure, a traité de quatre sujets à l’occasion de l’utilisation d’Internet :

* le secret par rapport à la transparence ;

* la rapidité et la sécurité de la transmission d’informations ;

* la désinformation : bon exemple de problématique que tous ceux qui font de l’intelligence économique doivent avoir à l’esprit;

* la fiabilité et de la crédibilité du personnel de l’entreprise pour une bonne administration de l’intelligence économique.

3. CONCLUSION

Cet intéressant colloque a permis au Comité R d'approfondir ses connaissances dans le domaine du renseignement économique tel que les français le conçoivent.

CHAPITRE 3 : RENCONTRE AVEC LES AUTORITÉS LUXEMBOURGEOISES EN CHARGE DU RENSEIGNEMENT

1. INTRODUCTION

En vue de donner au Parlement le plus de points de comparaison possible avec les pays qui ont déjà légiféré à propos des interceptions de sécurité, le Comité R a rencontré le 7 janvier 1998, les autorités luxembourgeoises qui ont en charge ce type de récolte d'informations.

Le Comité R a été fort aimablement reçu par le président de la Cour supérieure de Justice, le président de la Chambre des Comptes, le président de la Cour administrative et par le chef du service de renseignement luxembourgeois.

2. LÉGISLATION SPÉCIFIQUE AUX ÉCOUTES TÉLÉPHONIQUES

Le Grand-duché de Luxembourg a réglementé cette problématique en introduisant les articles 88-3 et 88-4 dans son code d'instruction criminelle par une loi du 26 novembre 1982.

Cette disposition déroge à la loi du 11 août 1982 relative à la protection de la vie privée qui interdit les écoutes et les observations. Des sanctions pénales sont prévues en cas de violation de cette loi.

Les tribunaux sont compétents pour juger toute personne ayant contrevenu à la loi du 11 août 1982 concernant la protection de la vie privée.

Les articles 88-1 et 88-2 de la loi du 26 novembre 1982 définissent la procédure que doit suivre le juge d'instruction pour ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication.

2.1. Autorités habilitées à autoriser l'écoute

Le président du Gouvernement donne avec l'assentiment d'une commission composée du président de la Cour supérieure de Justice, du président de la Chambre des comptes et du président de la Cour administrative, l'autorisation de procéder à des interceptions concernant les télécommunications.

La commission et le président du gouvernement se réunissent environ tous les trois mois. A l'issue de la réunion de la commission un procès-verbal, documentant son assentiment, est dressé.

En foi de quoi, le président du gouvernement qui, lui, n'assiste pas à la réunion de la commission (en vertu du principe de l'indépendance de la commission par rapport à l'exécutif) autorise le service de renseignement à procéder à la mesure de surveillance.

La commission ne constitue pas un organe de contrôle mais intervient dans le processus décisionnel précédent l'interception de télécommunication.

Une procédure d'urgence est prévue dans le cas où la commission ne pourrait pas se réunir dans un délai très bref : l'assentiment est donné postérieurement par la commission. Les cas d'application de cette procédure sont très rares. Nos interlocuteurs nous ont parlé de deux ou trois cas en dix ans.

2.2. Champ d'application et nature de la demande

La requête longuement motivée par la lutte contre la criminalité organisée ou par la recherche des infractions contre la sécurité extérieure de l'Etat, est présentée par le chef du service de renseignement au président du gouvernement et à la commission (principe de légalité).

La requête comporte deux ou trois pages. Les faits allégués sont précis et le chef du service de renseignement expose qu'il n'a pas d'autres moyens de recueillir l'information (principe de subsidiarité).

Sur base de cette requête, le président du gouvernement, après assentiment de la commission, émet alors une ordonnance ou une décision qui sera notifiée, pour exécution, au service de renseignement et à l'entreprise des Postes et Télécommunications.

Il n'y a pas de quota prévu par la loi par opposition à la loi française.

L'ordonnance peut porter sur plusieurs personnes. Une dizaine d'ordonnances, prolongations comprises, sont délivrées par an. Ces ordonnances sont valables pour une durée de trois mois renouvelables de trois mois en trois mois, sans limitation.

Une discussion informelle entre le chef du service de renseignement, le président du gouvernement et la commission, portant sur le résultat des écoutes a lieu à l'occasion d'une demande de renouvellement de l'ordonnance. Elle influence la décision de renouvellement.

2.3. Exécution du mandat

L'ordonnance est exécutée par une section du service de renseignement qui s'occupe de l'objectif suivi et techniquement par un employé de la poste. L'ordonnance est présentée au directeur, ou son délégué, de l'entreprise des Postes et Télécommunications pour exécution.

L'agent chargé de l'interception ne transcrit que ce qui intéresse le service de renseignement. Les transcriptions pourraient être utilisées par les autorités judiciaires dans le cadre de procédure. Toutefois, les hôtes du Comité R ont précisé que cette hypothèse ne s'est jamais réalisée.

Le service de renseignement estime que la dénonciation des crimes et délits aux autorités judiciaires en l'application des articles 88-3 et 88-4 du Code d'instruction criminelle, constitue un sujet délicat : il désire protéger ses sources.

Cette position est à l'inverse de celle de la Sûreté de l'Etat qui collabore de manière systématique avec les autorités judiciaires en transmettant à celles-ci les informations dont elle dispose en dehors du contexte de l'application de l'article 29 du Code d'instruction criminelle(1).

Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes de tenter de commettre ou d'avoir commis ou tenté de commettre l'infraction comme auteurs et complices, ne peuvent être utilisées. Leur enregistrement et leur transcription sont immédiatement détruits par le chef du service de renseignement.

Les copies, enregistrements et toutes autres données et renseignements obtenus sont détruits soit parce qu'ils ne sont pas utiles au service de renseignement soit au plus tard au moment de la prescription de l'action publique.

Aucun recours sur l'autorisation de procéder à des écoutes n'est prévu par la loi. Le droit administratif luxembourgeois pourrait suppléer à la carence de cette loi (voir à ce sujet la décision de la Commission européenne des Droits de l'Homme relative au recours intenté contre la loi du 26 novembre 1982).

Le président du gouvernement et la commission arrivent toujours à un concessus avant la délivrance de l'ordonnance.

La loi ne prévoit pas de notifier les décisions d'écoutes aux particuliers. Des recours contre la loi du 26 novembre 1982 ont été intentés auprès de la Commission européenne des Droits de l'Homme(2), qui les a déclarés irrecevables.

2.4. Contrôle

La loi ne prévoit pas de rapport annuel d'activités au Parlement. Certains parlementaires y songent. Deux questions parlementaires(3) ont été posées au président du Gouvernement à la chambre depuis l'application de la loi du 26 novembre 1982 ; la question a porté sur le nombre de mandats délivrés.

---

(1) Note de la Sûreté de l'Etat du 24 septembre 1997 : *"La collaboration entre la Sûreté de l'Etat et les autorités judiciaires"* - p. 1.

(2) Décision de la Commission européenne des Droits de l'Homme relative au recours introduit contre la loi du 26 novembre 1982 (articles 88-1 à 88-4 du Code d'instruction criminelle).

(3) Question parlementaire du député J. Schummer - Question parlementaire du député R. Mehlen.

3. LOI DU 30 JUILLET 1960 CONCERNANT LA PROTECTION DES SECRETS INTÉRESSANT LA SÉCURITÉ EXTÉRIEURE DE L'ETAT

Le Grand-Duché de Luxembourg a organisé le service de renseignement en insérant dans le code pénal la loi du 30 juillet 1960 concernant la protection des secrets intéressant la sécurité extérieure de l'Etat.

Cette loi comporte 6 articles. La mise à jour de cette loi est en cours d'élaboration.

3.1. Mission

L'article 2 institue un service de renseignement et lui assigne une mission très large :

"(...)assurer la protection des secrets visés à l'article premier et de rechercher les informations que requiert la sauvegarde de la sécurité extérieure du Grand-Duché de Luxembourg et des Etats avec lesquels il est uni par un accord régional en vue d'une défense commune."

Les concepts de 'sécurité extérieure' et 'intérieure' de l'Etat ne sont pas définis. Toutefois, le code pénal énumère, de façon exhaustive, les infractions en matière de sécurité (espionnage, subversion, défense nationale).

Le chef du service de renseignement conçoit que la sécurité extérieure puisse être menacée par des activités menées à l'intérieur du pays.

C'est la raison pour laquelle le terrorisme, l'espionnage et la prolifération des armes non conventionnelles et le potentiel scientifique ou économique sont notamment considérées comme étant des missions du service de renseignement.

Ce même article vise la collaboration du service luxembourgeois avec les services de renseignement étrangers dans la mesure où le service luxembourgeois a pour mission de rechercher les informations que requiert la sauvegarde de la sécurité extérieure (...) des Etats avec lesquels il est uni par un accord régional en vue d'une défense commune.

Le secret d'Etat n'est pas défini dans la loi. Toutefois, le chef du service de renseignement estime que les directives de l'OTAN et de l'UEO sont d'application en vertu du principe de la prééminence non seulement des traités internationaux ratifiés par le Grand-Duché de Luxembourg sur le silence de la loi nationale, mais aussi de l'article 2 ci-dessus mentionné.

Le chef du service de renseignement n'élabore pas de liste des sujets traités par son service.

3.2. Autorité responsable

L'article 2 de la loi place le service de renseignement sous la responsabilité du président du Gouvernement.

3.3. Statut des agents du service de renseignement

Les articles 3 et 4 de la loi concernent le statut des agents du service de renseignement.

Le chef du service de renseignement est désigné par le Conseil du Gouvernement sur proposition du Premier ministre. Son mandat est illimité.

Le chef du service de renseignement porte, en vertu de la loi, le titre de directeur du SREL. Le directeur du SREL est le seul membre du SREL à ne pas être détaché d'autres services publics (art. 3 al. 1). Il est donc le seul à faire partie du cadre du SREL. L'actuel directeur du service a fait carrière dans l'armée.

Le service se compose de vingt-sept agents qui ont été recrutés dans la fonction publique par détachement sur arrêté du Ministre d'Etat, selon les besoins du service.

Ces fonctionnaires sont approchés par le chef du service après enquête de sécurité officieuse. Cette enquête porte principalement sur la consultation du casier judiciaire des intéressés.

Les fonctionnaires détachés gardent leurs droits et avantages dans leur cadre d'origine où ils peuvent être renvoyés à tout moment, sur proposition du chef du service de renseignement. Une mobilité des agents du service existe en principe.

3.4. Budget

L'article 5 de la loi est relatif au budget du service de renseignement. Ce budget est géré par le chef du service et contrôlé par la Chambre des comptes. Le secret des opérations du service est garanti par la loi.

3.5. Secret professionnel

L'article 6 de la loi concerne le secret professionnel des personnes ayant à connaître dans le cadre de leur fonction des renseignements recueillis par le service ou relatif au fonctionnement du service de renseignement.

3.6. Habilitations de sécurité

Aucune loi luxembourgeoise ne sanctionne la problématique des habilitations de sécurité.

Le chef du service de renseignement propose que le Parlement ratifie le texte de la CM55/15, classifiée diffusion restreinte, qui vient d'être revue par les autorités compétentes de l'OTAN.

CHAPITRE 4 : JOURNÉE D'ETUDE CONSACRÉE AU DÉFI À RELEVER CONTRE LE CRIME ORGANISÉ

Le 20 mars 1998, une journée d'étude se déroula à Louvain au sujet du défi à relever à l'encontre des activités du crime organisé. L'Administrateur Général de la Sûreté de l'Etat y a fait un exposé intitulé *"Pour une gestion de l'information globale"*.

Cet exposé peut être résumé comme suit.

Une banque de données doit tenir compte des diverses normes de droit qui protègent la vie privée sur la sécurité de la banque de données.

La gestion des informations doit être organisée de façon efficace, ce qui, du point de vue démocratique, serait un véritable enrichissement.

A l'heure actuelle, des dizaines d'autorités et services s'occupent du crime organisé mais la circulation de l'information doit être revue.

Pour une meilleure compréhension de l'exposé, l'orateur a repris les définitions classiques des concepts suivants :

- prévention et répression ;

- autorités et services ;

- autorités judiciaires et administratives ;

- information sensible (à propos de ce concept, l'orateur a renvoyé notamment au projet de loi sur les habilitations de sécurité et l'avant -projet modifiant la loi sur la fonction de police. D'après l'orateur, la Belgique est largement en retard en matière de codification concernant la protection de l'information administrative sensible).

L'Administrateur général de la Sûreté a plaidé pour la création d'une seule banque nationale de données sensibles. Il s'agit cependant d'une responsabilité conjointe des autorités administratives et judiciaires.

Une procédure spécifique édictée par une loi doit être prévue en vue de régler les conflits d'intérêt qui pourraient survenir entre les différentes autorités.

L'orateur a mentionné à cet égard la fonction d'arbitrage prévue dans l'amendement déposé par le sénateur Vanden Berghe au projet de loi sur les services de renseignement et de sécurité.

La banque de données doit donc être créée conformément aux règles de droit et être efficace.

Cela implique que :

- une seule banque de données subsiste et un accès à d'autres banques de données pour que leurs informations soient complètes;

- les informations relatives à la criminalité organisée doivent être transmises au ministère public;

- un contrôle externe soit envisagé et assuré, par exemple, par un collège de magistrats;

- des règles de sécurité efficaces soient établies et prises;

- chaque consultation ou manipulation de la part des autorités et des services, laisse une trace et soit justifiée par des motifs légitimes ;

- le service chargé de la gestion de cette banque de données soit placé sous la direction du ministère public et composé de représentants des services de police et d'autorités administratives;

- la banque de données soit intégrée au ministère public ou à la future police nationale.

Enfin, l'Administrateur général souhaite une discussion rationnelle à ce sujet.

CHAPITRE 5 : VOYAGE D'UN MEMBRE DU COMITÉ ET DU CHEF DU SERVICE D'ENQUÊTES À MADRID

Un membre du Comité R ainsi que le chef de son Service d'enquêtes se sont rendus à Madrid les 12, 13 et 14 mai 1998. Ce voyage s'inscrivait dans le cadre de l'enquête sur les satellites et celui de l'étude sur les législations de certains pays sur les secrets officiels.

Ayant pu prendre connaissance de la loi espagnole du 5 avril 1968 (9/68) réglementant les secrets officiels ainsi que de la loi 11/95 du 11 mai 1995 réglementant l'emploi et le contrôle des dépenses "réservées", le Comité R avait souhaité rencontrer des représentants des autorités de ce pays concernées par leur application, à savoir, un membre du conseil des ministres et un membre de l'Etat-major, de même que des parlementaires membres de la commission de contrôle des fonds secrets. Cette rencontre n'a pu avoir lieu étant donné que l'agenda politique et parlementaire était très chargé à ces dates en Espagne. Par contre, la délégation du Comité R a pu rencontrer et s'entretenir avec Monsieur Madrigal, secrétaire général de l'unique service de renseignement espagnol, le "Centro Superior de Información de la Defensa" (Centre supérieur d'information de la défense - CESID). Cet entretien a porté sur le cadre légal dans lequel fonctionne le CESID. Il en ressort que si l'Espagne est dotée de lois réglementant les secrets officiels, le contrôle des dépenses "réservées" et les écoutes téléphoniques du CESID, il lui manque par contre, tout comme en Belgique encore à ce jour, une loi organique pour son service de renseignement. Celui-ci est néanmoins organisé par une dizaine d'arrêtés royaux.

La journée du 14 mai a été consacrée à la visite du centre satellitaire de l'UEO à Torrejoñ, situé à une quarantaine de kilomètres de Madrid. La délégation du Comité R y a été reçue par le colonel Molard, directeur du centre et par les responsables de ses différentes sections; elle a pu assister à des démonstrations d'interprétation d'images satellitaires assistée par ordinateur.

Le Comité R tient à remercier tout particulièrement :

- M. Gautier, conseiller conseiller général f.f. au ministère des Affaires étrangères, du Commerce extérieur et de la Coopération au développement,

- M. Xavier Demoulin, ambassadeur de Belgique à Madrid,

- le colonel aviateur BEM Pierre Billen, attaché de défense près l'ambassade de Belgique à Madrid,

- M. François Bontemps, premier secrétaire de l'ambassade de Belgique à Madrid, sans qui il n'aurait pu nouer ces fructueux contacts.

CHAPITRE 6 : INTERNATIONAL APPLIED OPEN SOURCE COLLOQUIUM

Les 11 et 12 juin 1998, un membre du Comité R a pu participer à un Applied Open Source Colloquium international organisé à l'université de Mercyhurst à Erie (PA-USA).

Ce colloque réunissait à la fois des représentants d'organisations internationales comme Interpol et Europol ainsi que des personnes du monde des affaires, des services de renseignement et de sécurité, des services de police et du monde universitaire.

Dans un premier temps, les personnes présentes ont été réparties en différents groupes : par exemple : sécurité nationale (services de renseignements et de sécurité), services de police, industrie, universitaires et chaque groupe a discuté des problèmes inhérents à l'utilisation des sources ouvertes.

Dans un deuxième temps, les participants ont été répartis en groupes interdisciplinaires pour terminer par un échange d'expériences lors d'une séance plénière.

Généralement, les conférences "Open Sources" ne sont pas suffisamment variés. Leur approche est très théorique, les projets abordés sont généralement extrêmement coûteux et par conséquent, ne sont pas accessibles pour de nombreux services et organisations.

Au cours des années 1997 et 1998, les critiques à l'égard de cette approche se sont multipliées. Nombreux sont ceux qui ont demandé davantage de séminaires et de conférences afin d'aborder le sujet de manière plus pratique.

Le colloque en question est donc un bon exemple de cette nouvelle tendance : une approche à petite échelle qui met l'accent sur des applications pratiques.

L'objectif de ce congrès consistait donc à proposer aux personnes qui jouent un rôle dans la politique d'information de leur organisation, qu'il s'agisse d'un service de police, d'un service de renseignement ou d'une entreprise privée, un forum afin de discuter des évolutions dans le domaine de "l'Open Sources Intelligence", et si possible, de parvenir à une meilleure compréhension du phénomène.

Il est vrai que le concept de “l’Open Sources Intelligence” fait l’objet d’une attention accrue dans le monde du renseignement. Divers services ont déjà développé une structure appropriée pour l’exploitation des sources ouvertes (par exemple : le Canada et les Pays-Bas).

Au cours du colloque, les participants ont exprimé les difficultés qu’ils rencontrent en travaillant avec des sources ouvertes. On s’est ainsi rendu compte que le coût constitue le principal obstacle, même si l’on a déjà suffisamment démontré que l’utilisation efficace des sources ouvertes est très coûteuses, mais plus efficace que les “Intelligence sources” traditionnelles (informateurs, mise sur écoute de télécommunications, surveillance, etc ...).

Néanmoins, certains problèmes techniques restent insolubles à ce jour. Les bons “moteurs de recherche” restent rares et les logiciels de traduction ne sont certainement pas encore au point.

De plus, un débat important portait sur le transfert des connaissances. En d’autres termes, comment peut-on apprendre à travailler le plus efficacement possible avec des sources ouvertes : dans un cadre universitaire par des formations professionnelles ou par un usage fréquent ?

Voici quelques-unes des nombreuses questions qui n’ont encore reçu aucune réponse définitive.

Trois questions importantes relatives à l’utilisation des sources ouvertes ont été abordées.

D’une part, comment peut-on intégrer au mieux une unité de sources ouvertes dans un service public ou une organisation privée ?

D’autre part, comment peut-on s’assurer que les informations arrivent aux bonnes personnes ce qui est d’une importance capitale pour améliorer l’efficacité d’un service.

Malgré la longueur des débats sur ce sujet, la conclusion finale est que chaque organisation doit répondre individuellement à cette question.

Enfin, il est important de signaler que dans l’avenir, il faudra sérieusement réfléchir à une coopération et à un échange des sources ouvertes, surtout entre les petites organisations (services). La principale raison en est évidemment le coût. Dans certains pays, les différents services de police et de renseignement, par exemple sont abonnés conjointement aux grands fournisseurs d’informations, comme Reuters et Lexis-Nexis.

Au XXI^{ème} siècle, les divers acteurs qui travaillent avec des sources ouvertes devront encore relever de nombreux défis.

Dans l’utilisation des sources ouvertes, se pose aussi le problème de la désinformation, qui peut être volontaire ou involontaire. Tout l’art consistera à évaluer à leur juste valeur les informations contenues dans une offre surabondante de sources ouvertes et de contrer la désinformations. Il s’agit d’une difficulté qu’il ne faut pas sous-estimer.

CHAPITRE 7 : JOURNEE D'ETUDE SUR LES COMMISSIONS D'ENQUÊTES PARLEMENTAIRES

Le 16 janvier dernier, Louvain a été le cadre d'une journée d'étude intitulée *"Commissions d'enquêtes parlementaires, possibilités, limites et risques"* (1), sous la direction des professeurs Cyrille Fijnaut, Luc Huyse et Raf Verstraeten.

Le thème, qui est d'une actualité brûlante puisque pas moins de cinq commissions d'enquêtes parlementaires ont fonctionné en même temps, a été abordé en premier lieu par le politologue Kris Deschouwer.

Celui-ci a mis l'accent sur le fait que les commissions d'enquêtes sont des instruments politiques qui opèrent aussi bien dans un cadre politique que dans un cadre juridique, ce qui suscite des tensions et des attentes parfois contradictoires.

Monsieur Deschouwer s'oppose à l'utilisation de ces commissions au sens d'une revalorisation du Parlement parce que ceci repose sur une interprétation dépassée de la séparation des pouvoirs. Il pense en revanche qu'elles prennent tout leur sens dans le contexte du Parlement en tant que représentation populaire.

Le Professeur Raf Verstraeten - également expert en commission - a clarifié les aspects procéduraux des commissions d'enquêtes. Pour lui, c'est surtout la convergence entre une commission d'enquête et une instruction judiciaire qui constitue un exercice d'équilibre délicat et non sans risques.

Ici aussi, il est essentiel de bien comprendre la finalité de l'enquête parlementaire car en définitive, cette enquête a pour dernier objectif de transmettre au parquet des éléments concernant d'éventuelles infractions.

Lors de la discussion sur les pouvoirs des commissions d'enquêtes parlementaires, il a été rappelé que les commissions sont habilitées à confier des devoirs aux Comités permanents P et R (ce qui n'a pas encore été le cas en ce qui concerne le Comité R).

(1) Les exposés et panels de cette journée d'étude ont été retranscrits dans le livre *"Parlementaire onderzoekscommissies: Mogelijkheden, grenzen en risico's"*, C. Fijnaut, L. Huyse & R. Verstraeten (réd.) - Louvain, 1998.

Le journaliste Walter De Bock a relaté les rapports délicats et parfois pénibles entre les commissions d'enquêtes et les médias. Il incombe à la commission d'enquête de faire comprendre à tout un chacun qu'elle est là pour garantir le fonctionnement correct des institutions et non pas pour servir les intérêts de partis politiques.

Au cours des débats qui ont suivi, plusieurs experts de diverses commissions ont accepté de dévoiler partiellement le fonctionnement des commissions d'enquêtes.

La journée d'étude s'est clôturée par la conclusion que les commissions d'enquêtes parlementaires ont toujours un avenir et un sens pour autant qu'elles respectent certaines conditions. La principale d'entre elles est de manier avec un soin tout particulier cet instrument ultime du Parlement.

TITRE IV : EVOLUTION DU COMITE

1. LA COMPOSITION DU COMITE R

Comme l'année dernière, le Comité R est resté composé, en tant qu'organe collégial, de quatre membres en 1998, alors que la loi (article 28 de la loi du 18 juillet 1991) en prévoit 5. Un mandat n'a donc pas été pourvu.

Un autre mandat expiré le 1er juin 1998, a été poursuivi en application de l'article 30 de la loi du 18 juillet 1991, conformément aux instructions des Commissions spéciales d'accompagnement du Parlement, et dans l'attente de la révision de la loi sur les Comités Permanents P et R.

L'article 30 stipule qu'au terme de leur mandat, les membres continuent à exercer leurs fonctions jusqu'à la nomination de leur successeur.

La composition du personnel administratif du Comité R est également restée inchangée, elle se présente actuellement comme suit :

- un comptable en service statutaire ;
- une secrétaire en service statutaire ;
- un employé en service statutaire ;
- un employé engagé comme contractuel (précédemment détaché) ;
- un chauffeur-technicien mis à disposition par l'Armée ;
- un militaire employé en dehors de l'Armée chargé de la réception ;
- un employé contractuel pour la documentation (fin de contrat septembre 1998).

Le Service d'enquêtes a été renforcé le 5 janvier 1998 par l'entrée en service de Monsieur Paul vander Straeten en qualité de Chef du Service d'enquêtes. Avec l'approbation du ministre de la Justice, Monsieur vander Straeten, premier substitut du parquet de Bruxelles, a été délégué au Comité R.

A l'automne 1998, le Comité R procédera également à l'engagement d'un membre supplémentaire du Service d'enquêtes, de sorte que le cadre sera entièrement pourvu pour la première fois et comptera alors (chef du service compris) cinq membres.

2. ACTIVITES DU COMITE R

Du 1er août 1997 au 31 juillet 1998, 42 réunions plénières du Comité R se sont tenues, en fait chaque semaine – hormis les périodes de vacances.

D'autre part, dans le cadre des enquêtes et études du Comité R, de nombreuses réunions internes ont été organisées avec des membres du Comité R et des membres des services d'enquêtes.

En outre, plusieurs réunions ont été organisées, entre autres, avec les chefs des services de renseignements belges.

Durant la même période, 13 nouvelles enquêtes de contrôle ont été ouvertes.

Celles-ci peuvent être ventilées comme suit :

- deux à la demande du Parlement ;
- deux à la suite d'une plainte ;
- deux sur dénonciation ;
- deux sur l'initiative du Service d'enquêtes ;
- quatre sur l'initiative du Comité R lui-même ; et
- une enquête commune avec le Comité P, sur proposition du Comité R et avec l'accord du Comité P.

Durant cette période, aucune enquête n'a été ouverte sur l'initiative des autorités administratives ou judiciaires compétentes.

Les enquêtes complètement clôturées se trouvent sous la partie 2 du Titre II du présent rapport annuel. Ce rapport reprend également trois études clôturées.

Ce rapport n'a pas repris plusieurs plaintes qui ont été immédiatement classées sans suite, conformément à l'article 34 de la loi du 18 juillet 1991. Il s'agissait de plaintes manifestement non fondées, comme en témoignait l'absence d'éléments contrôlables ou crédibles.

3. LES MOYENS FINANCIERS

Les ressources financières du Comité R proviennent d'une dotation allouée chaque année par le Parlement. L'exécution du budget est placée sous le contrôle de la Cour des Comptes, qui établit chaque année un rapport à l'attention de la Chambre des Représentants.

Pour 1997, un budget de 70.715.000 BEF était disponible. Dans le courant de l'exercice 1997, deux adaptations internes ont été effectuées (à savoir des glissements d'un poste budgétaire vers un autre). De cette manière des dépassements budgétaires non autorisés ont été évités.

Sous réserve d'approbation par le Parlement, un excédent de 18.062.019 BEF a été constaté à la clôture de l'exercice. En comptant les ristournes et diverses recettes, l'exercice présente un solde bénéficiaire de 19.253.843 BEF.

Une grande partie de l'excédent s'explique par le nombre incomplet de membres et de membres du personnel du Comité R.

Pour 1998, le Comité R avait demandé un budget de 72.448.000 BEF.

Après amendement de la Commission Comptabilité de la Chambre, un crédit de 71.552.543 BEF a été alloué.

4. ACTIVITES COMMUNES AVEC LE COMITE PERMANENT P

Comme c'est déjà indiqué dans le précédent rapport annuel, cette collaboration intervient à deux niveaux : les enquêtes et la logistique.

En février 1998, une enquête de grande ampleur a été entreprise par les deux Comités conjointement. Cette enquête exige une collaboration intense au niveau des services d'enquêtes, ainsi qu'une concertation et des décisions au niveau des Comités mêmes.

En ce qui concerne la logistique, il existe une collaboration permanente entre les unités administratives des deux Comités.