COMITE PERMANENT DE CONTROLE

DES SERVICES DE RENSEIGNEMENTS

RAPPORT D'ACTIVITES

2000

COMITE PERMANENT DE CONTROLE

DES SERVICES DE RENSEIGNEMENTS

RAPPORT D'ACTIVITES

2000

Rue de la Loi 52 - 1040 Bruxelles

Tél 02/286.28.11 -- Fax 02/286.29.99

e-mail : comiteri@skynet.be

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,

Bruxelles, le 2 avril 2001

Messieurs les Présidents,
Messieurs les Ministres,

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

Ce rapport couvre la période du 1er janvier 2000 au 31 décembre 2000.

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

JEAN-CLAUDE DELEPIERE
PRESIDENT

GERALD VANDE WALLE
CONSEILLER

JEAN-LOUIS PRIGNON
CONSEILLER

WOUTER DE RIDDER
GREFFIER

TABLE DES MATIERES

TITRE 1 : INTRODUCTION

CHAPITRE 1 : GENERALITES

1. LES ENQUETES DE CONTROLE

1.1. Les compétences générales de contrôle du Comité R

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

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

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

Il faut préciser également que le Comité ministériel du renseignement [2] (présidé par le Premier ministre et composé des ministres des Affaires étrangères, de l'Intérieur, de la Défense nationale, de la Justice et du Secrétaire d'Etat à l'Energie et au Développement) établit la politique générale du renseignement. Il détermine également les priorités de la Sûreté de l'Etat et du Service général du renseignement et de la sécurité des Forces armées. Il coordonne aussi les activités de ces différents services. Le Comité ministériel définit, en outre, la politique en matière de protection des informations sensibles. Il établit pour ce faire des directives

---

1 Article 1er de la loi du 18 juillet 1991 tel qu'il a été modifié par la loi du 1er avril 1999 (M.B. 03/04/1999, p. 11.161).

2 Cf. notamment les articles 4, 7. 1°, 10.1er, 11.§ 4° , 20 § 3, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (M.B. 18 décembre 1998).

Le Comité R attire à ce sujet l'attention sur le fait que l'article 33 précité de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991 n'inclut pas les directives du Comité ministériel du renseignement et de la sécurité, ni celles du Collège du renseignement et de la sécurité[3], dans les documents internes que les services de renseignement doivent transmettre d'initiative au Comité R.

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

En ce qui concerne la manière dont les enquêtes administratives de contrôle peuvent être initiées, il faut distinguer celles suscitées par le parlement, celles ouvertes d'initiative par le Comité R ou par son Service d'enquêtes et celles résultant d'une plainte d'un particulier concerné par les activités d'un service de renseignement ou d'un membre de ces services. En outre, bien que le Comité R soit une émanation du pouvoir législatif, la loi prévoit encore qu'une enquête de contrôle peut être confiée au Comité R à la demande d'un des ministres compétents, à savoir celui de la Justice et celui de la Défense nationale[4].

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

La problématique de ce contrôle pour des matières susceptibles de concerner à la fois les services de police et de renseignement est rencontrée par l'article 53 de la loi du 18 juillet 1991 qui prévoit que *« pour ce qui concerne la répartition des missions et la coordination du fonctionnement entre d'une part les services de police et d'autre part les services de renseignement, les Comités permanent P et R peuvent réaliser des enquêtes communes de contrôle. »* (*voir le rapport d'enquête commune concernant « les mesures de sécurité prises au sein du SGAP en vue d'assurer le succès des enquêtes judiciaires et de manière plus générale sur l'efficacité de ce service » page 173 du présent rapport).*

1.2. La situation des enquêtes

S'il est de tradition dans un rapport annuel d'activités d'aligner des statistiques, il convient de souligner d'emblée que dans la matière spécifique, très particulière[5], et somme toute récente du contrôle parlementaire permanent des activités des services de renseignement[6],

---

3 Créé par l'arrêté royal du 21 juin 1996.

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

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

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

ces données n'ont sans doute qu'une importance secondaire pour appréhender les résultats de la mission de contrôle, telle qu'elle est décrite au point 1.1. ci-dessus.

Au-delà d'ailleurs des enquêtes de contrôle, le Comité R a recours à d'autres démarches pour tenter d'accomplir concrètement sa tâche dans un climat de plus grande transparence de la part des services de renseignement.[7]

C'est en effet dans le domaine d'une meilleure information, tant quantitative que qualitative, de l'organe de contrôle par ces services que des efforts doivent encore être développés et des progrès accomplis.

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

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

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

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

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

---

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

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

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

Il faut signaler enfin qu'à l'occasion de quelques enquêtes de contrôle, la Sûreté de l'Etat a opposé au Comité R, ainsi qu'à son Service d'enquêtes, le secret d'une instruction judiciaire en cours pour justifier de ne communiquer aucune information à l'organe de contrôle. Ce faisant, la Sûreté de l'Etat invoque le § 2 de l'article 48 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement qui indique notamment : *« Les membres des services de renseignements sont tenus de révéler au Comité R les secrets dont ils sont dépositaires, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours. »*

Le Comité R estime néanmoins que si le principe est totalement fondé, son interprétation extensive est de nature à empêcher dans la pratique et pour un temps indéterminé le déroulement d'une enquête de contrôle et est, dans ce sens, incompatible avec la philosophie du système mis en place par la loi organique du contrôle du 18 juillet 1991 précitée. Il convient d'ailleurs de souligner que la connaissance par le Comité R, ainsi que par ses enquêteurs, de faits précis intéressant un dossier judiciaire n'est pas nécessairement indispensable dans le cadre d'un contrôle *« a posteriori »* de l'efficacité des services et de la manière dont la coopération entre ceux-ci s'est coordonnée. Dans cette optique, le Comité R recommande aux services de renseignement d'évaluer aussi précisément que possible le secret de l'instruction et, en cas de doute, de s'en référer au magistrat titulaire. Le Comité R se réserve également la même possibilité.

2. LES ENQUETES JUDICIAIRES

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

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

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

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

Cette procédure prévoit pour le chef d'un service de renseignement la possibilité de faire opposition à la saisie judiciaire de documents classifiés [8].

En l'espèce, les raisons de cette opposition mentionnées dans la notification pour information faite en vertu de la loi au président du Comité R par le chef du service concerné, sont les suivantes : *« l'atteinte qui pourrait être portée aux relations internationales et le danger pour une personne physique[9]. »*

Au-delà du cas d'espèce[10], dont le Comité R ne manquera ni de suivre l'évolution dans le contexte de ses compétences de contrôle ni de faire rapport à ce sujet au Parlement, se pose également de manière plus générale le problème de la circulation des informations, et plus particulièrement de celles qui sont classifiées en application de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

En ce qui concerne leur communication aux autorités judiciaires, le Comité R a constaté à ce sujet dans deux autres enquêtes de contrôle, dont l'une est publiée dans le présent rapport, que malgré les principes de coopération et de communication des données, affirmés par le législateur dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité[11], des obstacles subsistent parfois en pratique dans ce domaine qui relèveraient dans les cas d'espèces de la protection des sources et notamment de l'application par nos services de renseignement de *« la règle du tiers ou du service tiers.[12] »*

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

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

---

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

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

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

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

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

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

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

Il convient de rappeler à ce propos qu'en ce qui concerne plus précisément les autorités judiciaires, la limitation d'accès aux divers éléments classifiés, prévue par l'article 8 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, ne s'applique pas lorsque ces autorités agissent dans le cadre de leurs compétences propres.

3. LES ENTREPRISES DE RENSEIGNEMENT PRIVE (SRP)

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

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

D'une manière générale, le Comité R estime que la dimension actuelle du renseignement privé doit être prise en considération. Les activités de ce secteur, particulièrement au niveau international et dans la sphère économique, industrielle et financière, sont reconnues comme de plus en plus importantes. Bien qu'elles ne soient pas illégales en tant que telles[13], la conscience que l'on peut en avoir au niveau de la société civile et de ses responsables dans les risques et les menaces qu'elles peuvent représenter, n'est pas toujours des plus aiguës.

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

---

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

Ces dispositions prévoient notamment que le ministre de l'Intérieur fait annuellement un rapport écrit devant les Chambres. Des dispositions pénales existent également dans notre droit interne pour répondre aux éventuels dysfonctionnements, abus et infractions de toute nature qui seraient constatés ou dénoncés dans ce domaine. Ne citons qu'à titre exemplatif et représentatif du domaine particulier qui nous occupe, la loi du 28 novembre 2000 relative à la criminalité informatique.

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

D'autres aspects comme celui du recrutement voire du débauchage par des entreprises privées de renseignement de membres des services de renseignement officiels et de la collaboration éventuelle de ces entreprises avec ces mêmes services doivent pour le Comité R faire également partie d'une évaluation et d'une réflexion.[14]

Pour illustrer ces thèmes, il est intéressant de signaler que lors de la conférence *« Intelligence in the 21th Century »* qui s'est tenue en Italie en février dernier, et qui rassemblait des responsables européens et américains du renseignement, le problème de l'intelligence privée a particulièrement retenu l'attention, du moins aux termes du compte rendu qu'en fait le périodique *« Le Monde du Renseignement »* dans sa livraison du 22 février 2001. On peut y lire notamment en ce qui concerne la collaboration entre les services officiels et privés : *« Les décideurs publics reconnaissent que ces collaborations cessent dès lors que les missions portent sur des sujets très sensibles et globaux : ceux sur lesquels seuls les agents tenus par des liens avec leur gouvernement peuvent intervenir. A l'inverse, les sociétés privées qui mènent des investigations à l'échelle de la planète se trouvent à la tête d'une imbrication de réseaux d'enquêteurs locaux, issus le plus souvent des services de renseignement des pays concernés. »* En ce qui concerne d'autre part le renseignement économique, le Comité R retient également la conclusion de l'analyse faite par le chercheur canadien Gregory Treverton qui est citée dans le même article : *« La culture des services secrets se révèle définitivement inadaptée aux événements qui marquent la vie des affaires. Les informations économiques sensibles ne nécessitent pas des débauches de clandestinité, mais plutôt des carnets d'adresse de haut niveau, manipulés par des professionnels qui ont le sens du tempo. Un tel état des lieux conduirait donc à isoler le renseignement économique du renseignement étatique. »* (voir Titre II - chapitre 7 du présent rapport : *« Rapport de l'enquête sur la manière dont la Sûreté de l'Etat s'acquitte de sa nouvelle mission de protection du potentiel scientifique et économique »* p. 109 et le chapitre 2 : *« Rapport de l'enquête sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge »* p. 58).

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

4. LE CONTROLE DE LA GESTION DE L'INFORMATION

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

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

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

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

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

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

« Les missions attribuées par la loi du 30 novembre 1998, organique des services de renseignement et de sécurité (M.B. du 18 décembre 1998) à la Sûreté de l'Etat visent des domaines comme les organisations criminelles, le terrorisme, les organisations sectaires nuisibles, l'extrémisme. Le Service général du renseignement et de la sécurité a également en charge pour sa part, dans le cadre de ses missions légales, des missions qui peuvent intéresser la lutte contre ces différentes formes graves de criminalité. »

« Dans ces secteurs, la coopération avec les services de police et les autorités judiciaires, coopération imposée d'ailleurs par l'article 20 de la loi précitée, implique bien évidemment l'échange d'informations, qui est d'autre part visé par« l'article 44/1 de la loi sur la fonction de police[15] *»*

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

---

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

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

« Bien que marginal, ce contrôle externe revêt toutefois un caractère complémentaire important dans la mesure ou il n'existe pas au niveau des services de renseignement un contrôle interne de la même nature que celui prévu par l'article 44/7 de la loi sur la fonction de police[16] ».

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

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

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

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

16 Art. 44/7 , 1er alinéa : « Il est créé un organe de contrôle sous l'autorité du ministre de l'Intérieur et de la Justice, chargé du contrôle de la gestion de la banque de données nationale générale visée à l'article 44/4, alinéa 1er. Cet organe de contrôle a un accès illimité à toutes les informations et les données conservées dans cette banque de données »
Art . 44/7, 5ème alinéa : « Cet organe est présidé par un magistrat fédéral….. »

CHAPITRE 2 : QUESTIONS POSEES AUX SERVICES DE RENSEIGNEMENT PAR LE COMITE R

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

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

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

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

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

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

1. TOURNOI DE FOOTBALL "EURO 2000" - EVALUATION PAR LA SURETE DE L'ETAT DES MENACES QUE CERTAINS SUPPORTERS EXTREMISTES DE CLUBS DE FOOTBALL PEUVENT FAIRE COURIR LORS DE LEUR SEJOUR EN BELGIQUE

Un article intitulé "*L'ombre d'Arkan plane sur l'Euro 2000*" paru dans la revue «Courrier International » n° 483 du 3 au 9 février 2000 a attiré l'attention du Comité R.

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

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

- le danger évoqué par l'article est-il réel ?
- la Sûreté de l'Etat a-t-elle examiné ce problème ?
- a-t-elle produit des rapports sur la question ?
- à qui les aurait-elle transmis ?
- la Sûreté de l'Etat surveille-t-elle certains clubs belges de supporters ?

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

Résumé :

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

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

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

Au mois de février 2000, la Sûreté de l'Etat examinait cependant l'éventualité que des groupements organisés d'hooligans d'extrême droite ou yougoslaves cherchent à profiter du tournoi Euro 2000 pour mener des actions.

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

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

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

2. LE RÔLE ÉVENTUEL DES SERVICES DE RENSEIGNEMENT DANS L'ÉVALUATION DES SANCTIONS ÉCONOMIQUES APPLIQUÉES A CERTAINS PAYS

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

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

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

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

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

Si oui, à propos de quels pays en particulier ? A qui ces rapports éventuels ont-ils été transmis ?

Estimez-vous que votre service est compétent, ou non, pour recueillir ce type d'information, l'analyser et la transmettre aux décideurs politiques ? ».

Réponse du SGR (lettre du 10 juillet 2000)

Résumé :

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

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

Ce document définit les priorités du SGR. Vu ses missions et ses moyens limités, le SGR n'a cependant pas la possibilité de suivre l'efficacité des sanctions internationales de près. Si les informations dont le service dispose à ce sujet concernent aussi la sécurité des troupes militaires belges, le SGR en fait part aux autorités (Premier ministre, ministre des Affaires étrangères, ministre de la Défense nationale et la Sûreté de l'Etat).

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

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

Résumé :

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

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

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

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

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

3. QUESTIONS POSEES DANS LE CADRE D'UN SUIVI DE L'ENQUETE SUR LA PARTICIPATION DES SERVICES DE RENSEIGNEMENT BELGES A DES PROGRAMMES SATELLITAIRES DE RENSEIGNEMENT

3.1 L'accès du SGR aux images satellitaires

A l'issue de son rapport d'enquête menée en 1998 sur la participation des services de renseignement belges à des programmes satellitaires de renseignement [(2)], le Comité R était d'avis que le SGR devait pouvoir disposer d'un accès direct et autonome à des images satellitaires comme source complémentaire d'informations, surtout pour le soutien à des opérations où la Belgique agit et prend ses décisions seule dans un cadre national.

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

(2) Cf. Rapport d'activités Comité R - 1998, Chapitre 5, p. 130

Cependant, en octobre 1998, le Conseil des ministres restreint a pris la décision de ne pas poursuivre ces démarches vu le coût trop élevé qui en résulterait pour le budget de la Défense nationale. Cette décision était toutefois susceptible d'être revue lors de la finalisation du nouveau plan des investissements de la Défense nationale.

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

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

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

Réponse du SGR (briefing circonstancié du 11 février 2000)

Résumé :

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

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

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

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

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

Commentaires du Comité R :

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

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

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

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

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

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

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

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

***Réponse du SGR (lettre du 21 juin 2000*)**

Résumé :

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

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

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

<u>Commentaires du Comité R</u> :

Le rapport de l'année 2000 rédigé par l'« *Intelligence and security committee* » [(3)] a reconnu la survenance de cette panne informatique de la NSA en soulignant au passage la qualité de la coopération existant entre les services de renseignement britanniques et américains dans le cadre du traité UKUSA.

(3) L'organe britannique de contrôle des services de renseignement

CHAPITRE 3 : LE CONTENTIEUX DES HABILITATIONS DE SECURITE

1. PRÉAMBULE

Jusqu'il y a peu la Belgique ne disposait pas d'une législation structurée réglant la procédure de délivrance d'une "**habilitation de sécurité**". Plusieurs milliers de "**certificats de sécurité**" étaient cependant annuellement délivrés.

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

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

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

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

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

2. AVERTISSEMENT MÉTHODOLOGIQUE

Dans le but de ne pas alourdir la présente synthèse, il n'entre pas dans les intentions du Comité R de se livrer au commentaire de cette loi qui a été voulue « claire, complète, accessible et précise » (voir « exposé des motifs », Chambre des Représentants de Belgique, 1193/1 96-97 et 1194/1 96/97, p. 5) en réponse aux attentes conjointes de la Convention Européenne, de la Jurisprudence de Strasbourg et des avis répétés du Conseil d'Etat.

Le Comité R en a cependant effectué, qualitate qua, l'analyse à usage interne qui lui était indispensable, s'agissant du droit positif applicable aux cas concrets lui soumis, et se propose de la publier à l'occasion du prochain rapport, affinée à la lumière d'une année complète d'exercice de son rôle d'organe de recours.

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

3. L'ANALYSE ACTUELLE DU COMITÉ R

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

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

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

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

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

Toutefois, à supposer pertinents les motifs de la plainte, ce citoyen ne pouvait attendre du Comité R/organe de contrôle qu'un rapport confidentiel dont le contenu était strictement réservé au ministre de tutelle et à la commission parlementaire de suivi. Le Comité R n'est en outre pas le destinataire naturel de l'information relative aux mesures éventuellement prises et, l'eût-il été, il n'est pas organiquement habilité à la divulguer.

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

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

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

D=autres modalités concrètes illustrent ce caractère formel, qu=il serait superflu de détailler ici. S=il fallait cependant en convaincre encore, il suffirait alors de renvoyer aux commentaires des articles du projet de loi (n° 1194/1), et notamment de l'article 3 '2, qui expriment clairement la volonté de créer de la sorte un organe juridictionnel indépendant du pouvoir législatif auquel le Comité AR@ est normalement soumis sous sa casquette d=organe de contrôle..

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

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

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

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

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

---

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

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

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

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

On le voit, nous sommes ici bien éloignés des principes du droit judiciaire. Sans entrer dans l'analyse individuelle et systématique des dispositions ci-dessus évoquées, on retiendra globalement que la motivation du législateur était, sur ce plan, de ne pas permettre la divulgation d'informations susceptibles de porter atteinte à la protection due aux sources, à la vie privée des tiers et à l'accomplissement des missions des services de renseignement, par le biais d'une procédure par principe uniquement destinée à offrir une voie de recours individuel. A*La solution adoptée par le gouvernement tend à réaliser un équilibre entre les droits de la défense et les exigences de la protection des sources et de la sécurité nationale*@ (1193/1-96/97 et 1194/1 -96/97 art.5 p. 23.)

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

A bon escient semble-t-il, puisqu'à l'heure actuelle, et à un niveau de sécurité contrôlé, l'organe de recours met hebdomadairement, en rigoureuse application de la loi, à la disposition de requérants et/ou leurs conseils, qui ne justifient par hypothèse pas de l'habilitation de sécurité du degré correspondant, un dossier contenant des informations classifiées auquel ils n'auraient jamais accès en d'autres circonstances que le recours.

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

---

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

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

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

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

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

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

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

Pour être tout à fait exact il convient de préciser que la grande majorité des recours réceptionnés à ce jour visent une décision rendue par le SGR en sa qualité d=autorité de sécurité compétente non seulement @pour les personnes qui relèvent du ministre de la Défense nationale@ mais aussi Apour les candidats à un emploi au sein du Ministère de la Défense nationale@ (art. 15 2° de la loi du 11décembre 1998 relative à la classification et aux habilitations de sécurité). C=est de très loin le groupe de détenteurs d=habilitation le plus important.

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

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

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

Une seconde contestation concerne la motivation (indispensable) apportée par l=autorité de sécurité à chaque décision. Il y est abondamment question d=intégrité, de loyauté, d=honorabilité et de fiabilité. Il a rapidement paru au Comité "R" que les critères d=honorabilité, de loyauté et, dans une certaine mesure, d=intégrité n=étaient pas automatiquement adéquats et que leur usage systématique encombrait plutôt la motivation de la décision. Quoi de plus discutable en effet que le concept d=honorabilité, évolutif dans le temps et selon les cultures ? Quid de la Aloyauté@, par exemple dans un contexte militaire intégré international ?

Quelle nécessaire liaison existerait-il automatiquement entre une condamnation pénale antérieure, par exemple, et une intégrité actuellement restaurée ?

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

N'est-ce en définitive pas ce, seul, à quoi tendent ces enquêtes de sécurité : évaluer la capacité d'une personne ayant accès à des informations classifiées à n'en faire usage qu'en exécution stricte des règles de sécurité prévalentes.

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

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

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

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

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

On ne répétera donc jamais assez qu'en vertu de la loi, le corollaire obligé du droit au recours pour un candidat évincé, soit le contrepoids **individuel** qui faisait précédemment défaut, n'est autre que le droit **collectif** à la sécurité pour l'information classifiée, et derrière ce secret, pour la collectivité qu'il protège.

Le Comité "R", quant à lui, s'efforce de faire comprendre qu'en tenant compte, par exemple de condamnations pénales antérieures significatives, en rapport avec la fiabilité générale d'un individu, il ne condamne pas une seconde fois cette personne (« non bis in idem ») en lui refusant l'accès à l'habilitation de sécurité convoitée.
Il fait le plus exactement possible la part des choses entre les droits individuels et le droit de la collectivité à bénéficier de titulaires d'informations classifiées (dont la divulgation serait de nature à causer un préjudice grave à la nation) qui puissent justifier de la fiabilité la plus éprouvée possible.

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

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

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

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

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

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

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

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

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

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

Cette évaluation préliminaire nécessiterait évidemment un investissement supplémentaire de la part du SGR, mais elle éviterait vraisemblablement les frustrations, hautement préjudiciables à la qualité ultérieure du service, régulièrement exposées à l=organe de recours par des requérants navrés de devoir interrompre une activité dans laquelle ils s=étaient investis et qui, dans certains cas, semblait justement de nature à les réintégrer plus rapidement dans un contexte de fiabilité suffisante.

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

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

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

* * *

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

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

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

TITRE II : LES ENQUETES DE CONTROLE

A . ENQUETES A LA REQUETE DU PARLEMENT OU DES MINISTRES

CHAPITRE 1 : RAPPORT DE SYNTHESE SUR LA MANIERE DONT LES SERVICES BELGES DE RENSEIGNEMENT REAGISSENT FACE A L'EVENTUALITE D'UN RESEAU «ECHELON» D'INTERCEPTION DES COMMUNICATIONS EN BELGIQUE

1. INTRODUCTION

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

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

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

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

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

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

« Comment les services belges de renseignements réagissent-ils face à l'éventualité d'un système « Echelon » d'interception des communications téléphoniques et fax en Belgique ? Nos services cherchent-ils à établir l'existence du système Echelon, et le cas échéant, à protéger les entreprises et les citoyens belges contre ces interceptions ? ".

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

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

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

Ces deux experts sont :

- le professeur Yves Poullet, Docteur en Droit, directeur du Centre de Recherche Informatique et Droit des Facultés Universitaires Notre Dame de la Paix à Namur, membre de la Commission de la protection de la vie privée,

ainsi que son collaborateur,

- M. Jean-Marc Dinant, Maître et Doctorant en Informatique, auteur de plusieurs travaux de recherche sur le thème de la vie privée et de la sécurité des données personnelles sur Internet.

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

D'une manière générale, il convient de rappeler que le Comité R s'était déjà penché par le passé sur la protection des systèmes informatiques et de communication.

Dans ce cadre il avait recommandé, dès 1994, qu'un organisme officiel soit chargé de concevoir et d'appliquer une politique globale de sécurité pour l'ensemble des systèmes d'information de la fonction publique.

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

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

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

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

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

2. QUELQUES REACTIONS ET MANIFESTATIONS DE L'INTERET DES INSTANCES EUROPEENNES, DE PARLEMENTS ET DE GOUVERNEMENTS NATIONAUX CONCERNANT L'EXISTENCE D'UN RESEAU « ECHELON »

2.1. Les instances européennes

2.1.1. Le Parlement européen

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

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

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

« Le Parlement européen, (…)

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

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

- *demande que de telles technologies de surveillance fassent l'objet d'un réel débat ouvert, tant au niveau national qu'à celui de l'Union européenne, et soient soumises à des procédures garantissant une responsabilité sur le plan démocratique ;*

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

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

Les 22 et 23 février 2000, la commission des libertés et des droits des citoyens, de la Justice et des affaires intérieures du Parlement européen s'est réunie à Bruxelles sur le thème « l'Union européenne et la protection des données ».

Le but des auditions prévues à cette occasion était de passer en revue les questions sensibles de la stratégie de l'Union européenne, qu'elle agisse dans le cadre de ses compétences communautaires et, en particulier celui de la directive 95/46/CE du 24 octobre 1995 du *Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci, (JO L 281 du 23.11.1995 p. 31)* ou dans celui d'autres politiques et formes de coopération *(IIème pilier : politique étrangère et de sécurité commune, IIIème pilier : coopération policière et judiciaire en matière pénale)*

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

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

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

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

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

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

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

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

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

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

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

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

- émettre des propositions pour des initiatives politiques et législatives.

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

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

La commission « Echelon » du Parlement européen est présidée par le député portugais Carlos Cuelho et son secrétaire est le député allemand Gerhard Schmid. Elle est composée de trente trois députés ; le représentant belge est le député Gérard Deprez.

Les membres de cette commission comptent user de leur influence et de leur pouvoir de persuasion pour obtenir les informations nécessaires à leur mission.

La presse rapporte que le secrétaire de la commission a émis le souhait de questionner M. Michael Hayden, le directeur de la NSA, l'organisme de sécurité américain, sur les actions du système Echelon en Europe.

La commission a également manifesté l'intention de s'intéresser aux discussions menées sur « Echelon » au sein de différents parlements et gouvernements nationaux, notamment en Belgique. Elle s'intéressera aux bases légales, aux missions, aux activités et aux contrôles des services de renseignement des pays membres de l'Union européenne, des Etats-Unis, du Canada, de l'Australie et de la Nouvelle-Zélande.

2.1.2. La position de la Commission de l'Union européenne

Interpellé peu après la réunion du 23 février 2000, le commissaire hollandais Frits Bolkenstein déclara d'abord que le système «Echelon » n'était qu'une rumeur et que lui-même n'intervenait pas sur des rumeurs, mais sur des faits.

Intervenant devant le Parlement européen le jeudi 30 mars 2000, M. Erkki Liikanen, commissaire finlandais chargé des entreprises et de la société de l'information a répondu aux interpellations parlementaires en déclarant que le type d'activités évoquées tombait « au-delà des compétences de la loi communautaire. »

Par contre, le président de la Commission, M. Romano Prodi, s'est quant à lui engagé à ce que celle-ci joue son rôle de gardien des traités ; il a confié la gestion technique du dossier au commissaire Liikanen, mais aussi au commissaire pour la Justice, le portugais Antonio Vittorino, et à celui pour le marché interne, le hollandais Frits Bolkenstein.

Les lignes possibles d'intervention de la Commission européenne concernent en effet différentes compétences : la sauvegarde de la vie privée des citoyens, la protection des données technologiques et celle de la recherche, l'espionnage industriel et la lutte contre la criminalité.

La commission européenne a donc adressé une demande de clarification au département d'Etat américain, ainsi qu'aux autorités britanniques.

Dans sa réponse, le sous-secrétaire d'Etat aux affaires européennes déclare que le gouvernement américain et les services secrets américains n'acceptent aucune demande d'espionnage de la part de firmes privées et ne collectent aucune information financière, technique ou commerciale au bénéfice de firmes privées.

Le représentant permanent du Royaume-Uni auprès de l'Union européenne a pour sa part fait savoir que les services de renseignement britanniques travaillent dans un cadre légal fixé par le parlement britannique. La lettre précise que ces services n'effectuent que des interceptions de communications autorisées, c'est-à-dire celles relatives à la sécurité nationale, la sauvegarde du bien-être économique de la nation et la grande criminalité. Pour le surplus, le gouvernement britannique ne « fait pas de commentaire à propos d'une activité d'interception présumée, quel que soit le caractère non fondé des allégations en question ».

2.2. La France

2.2.1. L'Assemblée Nationale française

Le 1er octobre 1998, Monsieur le sénateur Jacques Legendre a demandé à Monsieur le Premier ministre de lui faire savoir s'il est exact qu'un réseau électronique d'espionnage connu sous le nom "*d'Echelon*" a été mis en place par les Etats-Unis, la Grande-Bretagne et quelques autres pays anglo-saxons et si ce réseau procède à des écoutes motivées par l'espionnage industriel. Il lui a demandé quelles mesures le Gouvernement comptait prendre pour exiger de nos alliés qu'il soit mis un terme à une action aussi intolérable.

Selon le compte-rendu n° 27 de la Commission de la Défense nationale et des Forces Armées du mardi 29 février 2000[1], son Président Paul Quilès, après avoir fait référence au débat engagé dans plusieurs Parlements étrangers et au Parlement européen, ainsi que dans le public, sur le réseau dit « Echelon », a souligné qu'il appartenait à la Commission de la Défense de mener une enquête sur un système d'interception des communications dans le monde qui, en raison de son caractère d'organisation en réseau très étendu, de sa reconversion partielle vers l'espionnage industriel et de la participation d'un Etat membre de l'Union européenne, n'était pas sans poser de questions pour la sécurité du pays et la politique de défense, en particulier au moment où une politique européenne commune de sécurité et de défense était instituée.

La commission de la Défense nationale a dés lors nommé M. Arthur Paecht rapporteur de la mission d'information sur « les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale ».

Le 6 mars 2000, le député Yves Nicolin a déposé une proposition de résolution « tendant à la création d'une commission d'enquête sur la mise en cause des intérêts français par le réseau d'interception des communications dit « système Echelon », ainsi que les moyens déployés pour préserver la confidentialité des télécommunications ».

Cette dernière proposition a été rejetée le 22 mars 2000 considérant que la poursuite de la mission d'information de M. Paecht au sein de la Commission de la Défense nationale était préférable à la création d'une commission d'enquête.

(1) http://www.assemblee-nationale.fr

M. Paecht a déposé son rapport à l'Assemblée nationale en octobre 2000 dont les conclusions générales sont les suivantes :

« Oui, il existe bien un vaste système d'interception et de traitement des informations nommé Echelon. Il est organisé en réseau. Il s'agit d'ailleurs du seul système multinational connu.
Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. (…)

Oui, le système Echelon a divergé par rapport à ses objectifs initiaux, qui étaient fondamentalement liés au contexte de la guerre froide et par rapport même aux conditions du pacte initial UKUSA entre les cinq partenaires. Il n'est pas impossible que des informations recueillies soient utilisées à des fins économiques, voire à l'encontre de certains membres de l'alliance atlantique. (…)

Oui, des liens bilatéraux ont été organisés entre les Etats-Unis, l'UKUSA et d'autres services de renseignement pour des raisons de sécurité liées à des besoins militaires ou à la nécessité de lutter contre le terrorisme ou le grand banditisme.
Oui, Echelon peut constituer un danger pour les libertés publiques et individuelles. »

2.2.2. La position du gouvernement français

Répondant au sénateur Legendre, le Premier ministre français a notamment déclaré :

"(...) Il n'existe pas d'autorité qui puisse empêcher techniquement, l'interception de communications radioélectriques lorsque celles-ci sont véhiculées dans un espace mondial qui ne connaît pas de frontière physique. Par ailleurs, (...) les enjeux économiques de ces activités sont considérables, compte tenu de l'interconnexion des réseaux de communication avec les systèmes internes des entreprises. Il convient de répondre à ces développements inéluctables au plan des technologies par une politique volontariste dans au moins deux directions. D'une part, le Gouvernement français encourage le développement des moyens permettant de répondre aux besoins de confidentialité et d'intégrité des systèmes d'information sensibles. (...)

L'analyse des risques, le développement des moyens de protection, l'évaluation de la sécurité des systèmes d'information constituent des tâches prioritaires confiées notamment au service central de la sécurité des systèmes d'information du secrétariat général de la défense nationale. (...)

D'autre part, il est également clair que les investissements consentis pour l'interception des systèmes de communication répondent à des besoins de sécurité et de défense importants. Ceux-ci sont liés, par exemple à la surveillance des activités criminelles ou terroristes, à la prévention et au suivi des crises militaires ou encore à la lutte contre les programmes clandestins de prolifération des armes de destruction massive. Ces sujets présentent un caractère transnational et les Etats recherchent nécessairement, dans ces domaines, des formes nouvelles de partenariat.

Le développement de moyens de protection d'un côté, la mise en place d'investissements nécessaires pour faire face à l'essor accéléré des technologies de l'autre, enfin l'établissement de cadres juridiques et de coopération crédibles constituent donc les principales orientations de la politique du Gouvernement dans ces domaines." (Sénat français 3 décembre 1998 - Réseau d'espionnage industriel).

En évoquant officiellement la menace du réseau Echelon ou d'autres attaques informatiques, le Premier ministre français Lionel Jospin a donc redéfini sa politique en matière de sécurité des systèmes d'information.

En conseil des ministres du 15 mars 2000, le gouvernement a nommé Monsieur Henri SERRES, ingénieur général des télécommunications, comme directeur chargé de la sécurité des systèmes d'information.

Cette mesure intervient dans le cadre de la politique de sécurité qu'entend promouvoir le Gouvernement français, parallèlement au développement accéléré des outils de la société de l'information dans l'administration et les services publics.

Cette politique, au service du citoyen et de l'entreprise, doit aussi permettre de protéger la confidentialité des échanges et la vie privée.

Il reviendra au nouveau directeur de transformer le « Service central de la sécurité des systèmes d'information », intégré au « Secrétariat général de la défense nationale » depuis le 1er janvier 1999, en Direction de plein exercice du SGDN, chargée de la sécurité des systèmes d'information au niveau interministériel.

Cette décision marque à la fois un changement d'échelle dans les moyens dont le Gouvernement souhaite se doter dans ce domaine et la volonté d'assurer une meilleure coordination des efforts de l'État.

Le communiqué du gouvernement français précise :

« *Début 2000, l'attaque par des pirates informatiques non identifiés - et l'immobilisation pendant quelques heures - des sites Internet de sociétés américaines majeures du commerce électronique, ainsi que l'existence du réseau mondial d'écoute électronique Echelon, ou la mise en cause de certains produits "grand public", ont mis au premier plan de l'actualité les préoccupations liées aux nouvelles menaces et la nécessité d'assurer la protection de nos réseaux.*

Dans ce domaine, le Gouvernement et l'administration, ainsi que les services publics, devront donner l'exemple. Pour cet ensemble de raisons, le Gouvernement a décidé de la création, en 2000, à partir des moyens du SCSSI, d'une nouvelle direction centrale de la sécurité des systèmes d'informations (DCSSI) au Secrétariat général de la défense nationale.»

Le ministre de la Justice, Elisabeth Guigou, a rappelé devant l'assemblée nationale le 23 février 2000 les conseils de prudence aux entreprises pour se préserver de l'espionnage et assurer la sécurité des renseignements qui transitent par les nouvelles technologies : *« Le contenu de ces renseignements ne doit jamais comporter d'information vitale, surtout lorsque la liaison est relayée par un satellite de rediffusion, principalement dans les connexions internationales »* .

2.2.3. Le rapport d'activité 1999 de la « Commission nationale de contrôle des interceptions de sécurité » (CNCIS).

La loi française du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit les motifs qui justifient la conduite d'interceptions administratives de communications, à savoir, le terrorisme, la criminalité organisée, la sécurité nationale, mais aussi la sauvegarde du potentiel économique et scientifique.

Le 8ème rapport d'activités 1999 de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) indique qu'au cours de l'année 1999, 4.577 interceptions de sécurité ont été autorisées en France dont 186 à des fins de sauvegarde du potentiel économique et scientifique, soit 4 %.

2.2.4. Réactions du pouvoir judiciaire

Le journal français 'Le Figaro' du mardi 4 juillet 2000 annonce que le procureur de la République de Paris a chargé la Direction de la surveillance du territoire (DST) d'effectuer une enquête préliminaire sur le réseau de renseignement « Echelon ».

Selon le parquet de Paris, les écoutes illégales qui seraient pratiquées par ce système d'interception pourraient être visées par les articles 411-6 et 226-15 du code pénal et qualifiées ainsi d'« *atteinte aux intérêts fondamentaux de la nation »* et d' « *atteinte au secret des correspondances émises par voie de télécommunications».*

Cette enquête a été déclenchée le 24 mai 2000 suite à une plainte déposée le 2 mai par le député européen Thierry Jean-Pierre qui s'inquiète de pratiques *« de nature à porter un préjudice considérable à l'ensemble de nos concitoyens, de nos intérêts économiques et nationaux ».*

La DST est un service de police et de renseignement qui a pour compétence de rechercher et de prévenir, sur le territoire de la République française, les activités inspirées, engagées ou soutenues par des puissances étrangères et qui sont de nature à menacer la sécurité du pays, et, plus généralement, de lutter contre ces activités. A ce titre, la direction de la surveillance du territoire exerce une mission se rapportant à la défense [(2)].

2.3. La République fédérale d'Allemagne

2.3.1. Les discussions au Parlement (Deutscher Bundestag)

Des parlementaires du parti FDP (Freie Democraten) ont posé des questions au gouvernement fédéral le 11 avril 2000 concernant le système d'écoutes par satellites « Echelon » mis en œuvre par les Etats-Unis et quatre autres Etats *(références 14/2964*).

Ce groupe parlementaire a exhorté le gouvernement à porter son attention sur le rapport STOA discuté au Parlement européen.

---

(2) Décret n° 82-1100 du 22 décembre 1982 fixant les attributions de la direction de la surveillance du territoire.

Dans sa réponse, le gouvernement fédéral constate qu'il n'existe aucune constatation selon laquelle la vie privée des citoyens ou les capacités commerciales de l'économie allemande seraient mises en péril par un système d'écoutes généralisé.

Le gouvernement allemand confirme cependant que plusieurs pays anglo-saxons ont collaboré au temps de la guerre froide à un système de surveillance électronique des communications appelé « Echelon ».

Selon le gouvernement allemand, des experts ont établi que le rapport STOA avait fortement exagéré les capacités techniques du système « Echelon ».

Les contacts pris avec les autorités étrangères compétentes au sujet de faits supposés d'espionnage économique n'ont fourni aucun élément concret.

2.4. Les Pays-Bas

2.4.1 L'intérêt des autorités néerlandaises

Le 20 janvier 2001, suite aux remous causés par Echelon, et après examen de diverses sources ouvertes, parmi lesquelles les rapports du Comité R, le ministre néerlandais de la Défense nationale a présenté une note circonstanciée intitulée «*l'écoute à grande échelle des systèmes de télécommunication* » [(3)].

Le gouvernement déclare qu'il ne dispose pas d'information propre, confirmée par les gouvernements cités dans l'affaire « Echelon », sur l'existence de ce réseau. Mais sur base de l'information disponible par enquêtes et sources ouvertes, il estime l'existence du réseau Echelon plausible.

Non seulement les autorités, mais aussi les citoyens, les entreprises et les organisations criminelles sont en mesure de pratiquer de telles activités. Le gouvernement néerlandais estime que l'écoute à grande échelle des systèmes de télécommunication est une activité pratiquée par les services d'enquêtes, de sécurité et de renseignement de *« beaucoup de pays de couleurs politiques différentes* ».

Les sources ouvertes citent les Etats-Unis, le Royaume-Uni, la Russie, la Chine, la France, l'Allemagne, la Suisse, le Danemark. Les Pays Bas sont aussi cités mais la note du gouvernement s'abstient de le confirmer ou de le démentir.

Il existe au Pays-Bas un cadre légal pour l'interception et le repérage des communications aussi bien par câbles que sans fil.

L'interception et le repérage des communications sans fil au profit des services de renseignement militaire (MID) et civil (*Binnenlandse inlichtingen-dienst* - BVD) est effectuée par la section COMINT du *Militaire inlichtingendienst* (MID).
Les services de police et le BVD peuvent procéder à l'interception de communication par câbles dans les limites que la loi leur impose.

(3) disponible sur www.nrc.nl/W2/Lab/Echelon/doc010120.html

Selon le gouvernement néerlandais, la législation de ce pays offre des garanties suffisantes contre les atteintes intempestives à la vie privée des citoyens.

Les compétences du BVD et du MID en la matière sont actuellement discutées à l'occasion d'une proposition de loi qui fixe en même temps un certain nombre de limites (entre autres, un mandat préalable et une appréciation de la mesure sur base du principe de la proportionnalité et de la subsidiarité).

L'interception à grande échelle du trafic international des télécommunications pose la question de l'application du droit national à l'encontre du droit international.

Pour répondre à cette question, les Pays Bas privilégient l'idée que le droit international ne peut poser de limite à l'exercice d'une juridiction sur des actes posés sur son propre territoire ou à un endroit où les autres pays n'ont aucune juridiction, par exemples, sur un navire de haute mer ou sur un satellite dans l'espace.

A cet égard, il n'existe aucune législation aux Pays Bas qui donne la possibilité de s'opposer à l'interception des télécommunications. Une telle législation serait par ailleurs impossible à faire appliquer.

La protection du secret des télécommunications des citoyens devrait être recherchée dans la conclusion d'accords internationaux destinés à donner la possibilité aux citoyens de se défendre contre les écoutes et interceptions illégales.

Les conséquences juridiques des prises de position précitées doivent encore être discutées de façon plus approfondie. Le gouvernement néerlandais s'emploie à préciser sa position.

Le ministre néerlandais de la Défense nationale dément cependant qu'il puisse exister un lien entre les interceptions du gouvernement américain et celles des services européens de police et de renseignement.

Il indique que les réunions du *« International Law Enforcement Telecommunications Seminar (ILETS) »* et celles du groupe de travail *« Coopération policière »* organisées dans le cadre du troisième pilier de l'Union européenne ne sont pas destinées à faire ce lien.

Il dément également que cette relation devrait conduire à un système d'écoutes paneuropéen sur lequel le gouvernement américain exercerait une grande influence par le biais du FBI.

Suivant le ministre, ILETS est une conférence informelle rassemblant des représentants de services européens de police et de sécurité ainsi que des représentants de ces mêmes services de l'Australie, du Canada, de la Nouvelle Zélande, de la Norvège et des Etats-Unis. Elle est destinée à échanger de l'information sur les méthodes et techniques d'interception légale de systèmes de télécommunications à l'intérieur des frontières de ces Etats.

Le groupe de travail *« Coopération policière »* tente d'harmoniser au niveau européen la politique des interceptions légales des systèmes de télécommunications.

Le 22 janvier 2001 s'est tenue une réunion publique de la commission permanente de la Justice du parlement néerlandais. Celle-ci a examiné en quoi les Pays Bas seraient impliqués dans le réseau international d'espionnage Echelon.

Parmi les intervenants à cette table ronde, notre compatriote Jean-Marc Dinant (un des experts choisis par le Comité R pour rédiger son rapport au Sénat), le journaliste britannique Duncan Campbell, le journaliste néerlandais Cees Wiebes (co-auteur du livre « *Villa Maarheeze »* consacré au défunt IDB, *Inlichtingendienst Buitenland,* le service de renseignement extérieur des Pays Bas) et M. Maurice Wesseling (de l'organisation *« Bits of Freedom »* qui lutte pour le droit des citoyens sur les autoroutes de l'information).

Selon ce dernier, il devrait y avoir plus de contrôle parlementaire sur les systèmes d'écoute.

2.5. Les Etats-Unis

2.5.1 L'intérêt du Congrès américain : le rapport de la NSA

Suite à une disposition introduite dans *« The Intelligence Authorisation Act for Fiscal Year 2000 »* à la demande du député américain Bob Barr (Républicain, Géorgie), le 'Director of Central Intelligence', le 'Director of the National Security' et l'Attorney General' des Etats Unis ont présenté en février 2000 un rapport au Congrès américain *« describing the legal standards employed by elements of the intelligence community in conducting signals intelligence activities, including electronic surveillance»*.

Le Comité R a pris connaissance de ce volumineux rapport en mai 2000 [(4)].

La demande du Congrès américain traduisait ses craintes que les droits constitutionnels de citoyens américains soient atteints par le réseau Echelon.

L'angle d'approche du député Barr est effectivement concentré sur la protection de la vie privée des citoyens américains seulement, en partant de la constatation qu'une bonne partie de l'arsenal législatif relatif au domaine de la vie privée d'une part et des activités de renseignements de l'Etat, d'autre part, date des années 70 et ne recouvre plus adéquatement les nouveaux instruments d'échange d'informations.

Le rapport présenté par l'administration américaine réaffirme donc de manière circonstanciée que la NSA et le FBI respectent scrupuleusement le «Foreign Intelligence Surveillance Act (FISA) - the Executive Order N° 12333 » ainsi que le quatrième amendement de la Constitution américaine qui garantit à chaque citoyen de ce pays *« the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures »*.

La surveillance électronique est menée par des agents de la communauté américaine du renseignement à des fins de renseignement extérieur et de contre-espionnage.

Etant donné son caractère intrusif et ses implications pour la vie privée, ce mode de surveillance est soumis à une réglementation stricte ainsi qu'à un contrôle approfondi qui traduit une mise en balance des intérêts du gouvernement et des droits des « United States persons ».

(4) "*Legal Standards for the Intelligence Community in Conducting Electronic Surveillance"* disponible sur : http://www.fas.org/irp/nsa/standards.html , http://cryptome.org/dod5240-l-r.htm , http://cryptome.org/nsa-ussid18.htm et http://cryptome.org/fbi-fic-fci.htm .

Le rapport définit comme “U.S. person” tout citoyen des Etats-Unis, tout étranger légalement admis à y résider de manière permanente, toute société dont un nombre substantiel de membres sont citoyens américains ou étrangers légalement admis à résider aux Etats-Unis ou encore toute société implantée dans ce pays à condition qu’elle ne compte aucun représentant d’une puissance étrangère parmi ses membres.

Ainsi, pour pouvoir mener une opération de surveillance électronique sur un citoyen américain situé aux Etats-Unis, il est nécessaire d’obtenir une ordonnance de la “Foreign Intelligence Surveillance Court”.

Si cette personne se trouve à l’étranger, l’Attorney General (le ministre de la Justice), doit approuver la surveillance. La surveillance sera autorisée si la personne cible est, par exemple, suspectée d’être un agent d’une puissance étrangère.

L’autorisation n’est accordée que si l’information recherchée ne peut être recueillie par aucun autre moyen technique moins intrusif.

En toute circonstance, la surveillance électronique doit être menée de manière telle qu’elle réduise au minimum la collecte, la détention et la diffusion d’informations au sujet de citoyens américains non consentant.

Les règles américaines de protection à l’égard de la surveillance électronique à des fins de renseignement et de contre-espionnage ne s’appliquent pas à d’autres personnes que les citoyens américains.

Selon le journal « Le Monde » du 10 mars 2000, Georges Tenet, directeur actuel de la CIA, aurait déclaré devant le Congrès américain que les Etats-Unis n’utilisaient pas leurs services de renseignement pour promouvoir leurs activités économiques.

La CIA interviendrait néanmoins lorsqu’elle observe qu’une entreprise américaine est grugée dans ses intérêts par un concurrent qui agit malhonnêtement envers un client.

Le dossier serait alors soumis aux membres du Congrès, au Ministre des Affaires Etrangères ou au Secrétariat au Commerce pour qu’ils en tirent les conclusions nécessaires. Il s’agirait donc d’une démarche purement défensive.

2.5.2. Réaction de M. James Rubin, porte - parole du Département d’Etat (CBS News - février 2000 : «US Accused of Industrial spionage, » document repris du site : http://cbsnews.cbs.com/now/story/o,1597)

"*In Washington, State Department spokesman James P. Rubin denied any involvement in commercial spionage by the National Security Agency. 'The National Security Agency is not authorized to provide intelligence information to private firms. That agency acts in strict accordance with American law," Rubin said. "U.S. intelligence agencies are not tasked to engage in industrial spionage or obtain trade secrets for the benefit of any U.S. company or companies*".

2.5.3. Autres réactions et commentaires aux Etats-Unis

A l'occasion de la présentation du rapport de M. Campbell sur le système Echelon au Parlement européen, la presse américaine s'est fait l'écho des alarmes européennes et des dénégations des autorités américaines et britanniques.

Déjà le 24 février 1999, le New York Times avait publié un article décrivant en termes généraux le système Echelon comme une coopération entre l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les Etats-Unis visant à « écouter » l'ensemble des échanges téléphoniques et électroniques dans le monde.

L'article note cependant que les moyens d'écoutes de ce système ne sont pas à la hauteur de l'immensité des échanges existants du fait en particulier de la prolifération d'informations sur l'Internet et souligne que ce système a acquis ces dernières années un « statut mythologique ».

Dans le même sens, on trouve un article paru dans le magazine français « Le Figaro » du 28 mars 2000 relatant les confidences d'un « expert » des services de renseignement américains :

«Pour l'adversaire, il est chaque jour plus aisé de cacher son jeu dans le brouhaha. Et pour nous, il devient chaque jour plus difficile de déchiffrer les partitions qui nous intéressent. C'est un vrai problème pour la NSA, et sûrement aussi pour les Anglais du GCHQ et les Français de la DGSE .»

Réaction de M. Zbigniew Brzezinski, ancien conseiller pour la Sécurité Nationale du Président Carter

Le périodique français *"Le Nouvel Observateur"* du 10/16 décembre 1998, publie une interview de M. Brzezinski sous le titre provocateur :

" Un ancien de la Maison Blanche brise le tabou. Nous avons fait le choix de tout savoir. Zbigniew Brzezinski, qui fut conseiller pour la sécurité nationale du Président Carter et reste un spécialiste très écouté en matière internationale, est catégorique : oui, l'Amérique espionne le monde entier. Ses amis comme ses ennemis. Et il ne voit rien là d'immoral".

Selon M. Brzezinski :

"(…) L'Amérique a des responsabilités et des intérêts globaux mondiaux. Toute nouvelle tendance, tout mouvement imprévu sur la planète peuvent avoir un impact sur son bien-être et sa sécurité. Elle doit donc avoir la capacité d'être renseignée partout, non seulement sur ses ennemis mais aussi sur ses amis.

Le renseignement ne veut pas forcément dire espionnage, au sens classique du terme : le recrutement d'agents. Cette forme de renseignement est risquée, et peut conduire à des scandales très dommageables pour les relations avec le pays ami en question. Mais les écoutes ou l'imagerie spatiale sont, pour ainsi dire, ouvertes, libres et relativement peu risquées. Ces moyens techniques permettent un recueil systématique - et non compromettant - de renseignements. Ils sont plus ou moins à la portée de tout le monde. Chaque pays, selon ses moyens et ses objectifs, décide ou non de les mettre en oeuvre. L'Amérique a fait ce choix.

Je pense que le débat éthique sur le renseignement ne se pose vraiment que dans le cas de l'espionnage classique. On peut en effet se demander : le recrutement d'agents est-il une forme appropriée de renseignement à Bonn ou à Paris ? Mais, en matière d'écoutes ou de photos, quelle est la question éthique ? Est-ce immoral de photographier le monde ?"

Réaction de M. Thomas D. Grant, avocat américain et professeur à l'institut de droit international « Max Planck » à Heidelberg (RFA) – (article paru le 2 mars 2000 dans le 'Wall Street Journal'- Europe : « Spy Games : Don't let Echelon spook you »).

Selon M. Grant, les allégations de Duncan Campbell devant le Parlement européen ne sont pas plausibles. Elles pourraient avoir des conséquences fâcheuses sur deux domaines de la coopération entre le monde anglo-saxon et le continent européen : la politique industrielle européenne et la coopération militaire Nord-Atlantique : *« A breakdown of relations in these areas could, in turn, lead to the weakening of the West as the unique bastion of democratic rights and values ».*

Tout d'abord, ces allégations renforcent la position de ceux qui, en Europe, refusent les nécessaires réformes politiques et économiques à entreprendre pour rendre les marchés (marchés du travail, marché des capitaux) plus flexibles et plus compétitifs. *« The current accusation against the United States is widely challenged and little corroborated. It would foolishly imperil the economic recovery if Europe fixed on the idea that American wins in the game of economic competition were the result of legerdemain".*

En second lieu, ces accusations réveillent les vieilles antipathies Gaullistes à l'égard des Etats-Unis et de la Grande Bretagne : elles pourraient porter préjudice à l'Alliance Atlantique et avoir des conséquences néfastes pour la sécurité du monde en ce début du 21ème siècle.

Réactions de M. James Woolsey, avocat à Washington et ancien directeur de la 'Central Intelligence Agency' (CIA).

L'espionnage américain sur des firmes européennes a été confirmé par M. James Woolsey, ancien directeur de la CIA, lors d'une conférence de presse le 7 mars 2000, ainsi que dans un article paru dans le 'Wall Street Journal'- Europe, mercredi 22 mars 2000.

Dans cet article au titre très provocateur *« Why America Spies on its Allies – because they bribe»,* M. Woolsey reconnaît sans détour : *« Yes, my Continental European friends, we have spied on you. And it's true that we use computers to sort through data by using key-words. Have you stopped to ask yourselves what we're looking for ?"*

En ce qui concerne l'espionnage technologique, M. Woolsey estime que la technologie européenne n'en vaut pas la peine car, à quelques exceptions près, elle serait très inférieure à la technologie américaine.

Pourquoi alors les Etats-Unis espionneraient-t-ils les Européens ?

Pour M. Woolsey, la réponse à cette question se trouve dans le rapport même de M. Campbell. Dans les deux cas d'espionnage allégués par ce rapport, (un marché brésilien de Thomson-CSF et la vente d'avions à l'Arabie Saoudite par Airbus), il y est fait mention d'actes de corruption de la part de ces entreprises européennes pour obtenir les marchés convoités.

Ceci justifierait l'espionnage américain. M. Woolsey se défend pourtant d'avoir averti les entreprises américaines en compétition dans les marchés précités ; seuls les gouvernements faisant l'objet de manœuvres de corruption auraient été avertis que les Américains ne le prenaient pas à la légère.

Et M. Woolsey de critiquer l'interventionnisme des gouvernements européens qui soutiennent, souvent de manière déloyale, leurs entreprises plus coûteuses et moins performantes que les entreprises américaines : « *It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith* » note-t-il.

M. Woolsey admet que la CIA pratique le renseignement économique mais il affirme que 95% des informations collectées proviennent de sources ouvertes. Il affirme également que la CIA n'est pas engagée dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines.

Si la CIA surveille de près le commerce des super-ordinateurs et celui des produits chimiques, c'est parce que ces produits peuvent aussi être utilisés à produire des armes de destruction massive. La surveillance économique peut aussi concerner des pays soumis à des sanctions économiques tels que la Serbie et l'Iraq.

M. Woolsey défie également les Français d'affirmer qu'ils ne pratiquent pas l'espionnage économique. Si M. Woolsey reconnaît pour sa part la réalité de l'espionnage américain sur l'Europe, en le justifiant, il n'indique pas quels moyens ont été employés pour le pratiquer. Il ne confirme en rien l'existence du réseau Echelon ni ses objectifs tels que décrits dans le rapport de M. Campbell.

Dans une interview accordée au périodique français « Le Figaro » (mardi 28 mars 2000), M. Woolsey se contente de préciser que les Etats-Unis ont trois méthodes de renseignement clandestin : les espions, le satellite de reconnaissance et les écoutes. Il n'en dit pas plus.

Confirmant les propos qu'il a tenu dans le Wall Street Journal, M. Woolsey réaffirme que le but de l'espionnage américain en matière économique est de faire reculer la corruption, pas de faire attribuer le contrat au concurrent américain.

Interrogé sur le fait de savoir si la CIA était alors susceptible de provoquer des scandales politico-économiques (l'affaire Elf en Allemagne, par exemple), M. Woolsey répond :
« *Normalement, non (…) ce n'est pas la politique des Etats-Unis. Mais vous le savez, il y a beaucoup de choses que l'on ignore. Les rancunes personnelles, par exemple … ».*

Il est aussi intéressant de noter l'appréciation que M. Woolsey porte sur le rapport présenté par M. Campbell : *« Certains points du document (…) sont intellectuellement honnêtes. D'autres cherchent à faire vibrer la corde antiaméricaine ».*

Et M. Woolsey de lancer un appel aux gouvernements européens pour qu'ils réforment leurs économies étatiques, ce qui les conduira à plus d'efficacité et à plus d'innovation, et leur évitera ainsi de devoir recourir à la corruption pour gagner des marchés. *« And then we won't need to spy on you »* conclut-il..

Commentaires de M. James Bamford, auteur du livre consacré à la NSA « The Puzzle Palace ».

Dans un article paru le 14 novembre 1999 dans le "*Washington Post*" intitulé « *Loud an Clear – the most secret of secret agencies operates under outdated laws* ", James Bamford commenta les allégations et les craintes concernant le réseau Echelon.
Il écrit notamment :

« *As one of the few outsiders who have followed the agency for years, I think the concerns are overblown-so far. Based on everything I know about the agency, and countless conversations with current and former NSA personnel, I am certain that the NSA is not overstepping its mandate. But that doesn't mean it won't.*

My real concern is that the technologies it is developing behind closed doors, and the methods that have given rise to such fears, have given the agency the ability to extend its eavesdropping network almost without limits.

And as the NSA speeds ahead in its development of satellites and computers powerful enough to sift through mountains of intercepted data, the federal laws (now a quarter-century old) that regulate the agency are still at the starting gate. (...) It is highly unlikely that Echelon is monitoring everyone everywhere, as critics claim.

It would be impossible for the NSA to capture all communications. It has had personnel cutbacks in the past five years as its national security targets have increased in number. North Korean missile development, nuclear testing in India and Pakistan, the movement of suspected terrorists and so on.

Listening in on European business to help American corporations would be a very low priority, and passing secret intercepts to companies would quickly be discovered".

En mars 2000, James Bamford persiste à affirmer que les allégations du rapport Campbell sont du « non-sens ». Les renseignements collectés par la NSA ne sont pas transmis aux entreprises privées américaines. *« The NSA is a very, very secretive place. Even if you are in the government, even if you're in another intelligence agency, it's hard to get information from the NSA*".

Et M. Bamford de réaffirmer que les priorités actuelles de la NSA sont le terrorisme et la prolifération des armes nucléaires (propos cités par Kevin Poulsen dans *« Security Focus News » le 23 mars 2000 (http://www.securityfocus.com).*

Réaction de David Ignatius, journaliste au « Washington Post ».

Dans un article intitulé *« Despite What Europe Thinks, It Benefits From U.S. Spying »* paru le 18 avril 2000, ce journaliste américain commente l'affaire « Echelon » plutôt dans le même sens que James Bamford.

David Ignatius déclare notamment : *« Rather than the omnipotent agency its critics imagine, it seems these days to be struggling to keep its head above water. (…) And according to NSA officials, its systems aren't capable of processing the vastly increased flow of signals in a "broadband" world where voice and data travel as "packets" along a global tangle of fiber optic cables. (…)".*

Le journaliste rapporte alors des propos qu'aurait tenu le lieutenant général Michael Hayden, directeur de la NSA : *« The notion that the agency can scoop up every signal and electronic emanation in the world was never true – and is really not true now ».*

David Ignatius fait toutefois remarquer : *"Now, the whole world essentially shares the same communications system. The "enemy" potentially is everywhere, and America's "friends" inevitably are targets of American surveillance. Europeans who worry about a global NSA surveillance program known as Echelon are probably right, in that sense. (…) That doesn't mean the agency wants to steal foreign industrial secrets or violate people's privacy gratuitously as the Europeans fear, but without a global collection and processing capability, the NSA won't be able to monitor biological terrorists or other 21st century bad guys".*

Et Ignatius de lancer un appel aux européens : *« Trust us » is the NSA's implicit message. Trust us to distinguish between the good guys and the bad guys and to use our powerful surveillance tools for the good of humankind* ».

Conscient toutefois que ce message ne pourra être compris par tout le monde, Ignatius ajoute *: "But it is unrealistic to expect the rest of the world to be enthusiastic ».*

2.6. Royaume-Uni

2.6.1. L'intérêt du Parlement britannique

Le Comité R a pris connaissance de deux rapports annuels de l'«*Intelligence and security committee* »[(5)] déposé par le Premier ministre devant le Parlement britannique, le premier le 25 novembre 1999, le second en novembre 2000.

Ces rapports indiquent les quatre priorités actuelles des services de renseignement du Royaume-Uni, à savoir :

- le renseignement comme appui aux missions de maintien de la paix des forces armées,
- la prolifération des armes de destruction massive,
- les attaques terroristes et la croissance du crime organisé.
- le rapport souligne également…la menace croissante de l'espionnage économique.

Le « Committee » se penche aussi sur le fonctionnement du GCHQ (General Communication Headquarter), qui serait, d'après le rapport Campbell, le service opérationnel britannique participant au réseau « Echelon ».

Il est signalé que le GCHQ cible la Russie d'un point de vue stratégique, politique et militaire.

Il joue aussi un rôle significatif dans la lutte contre le crime organisé et le terrorisme. Il fournit des renseignements en appui des missions de maintien de la paix des forces armées dans les Balkans.Ces renseignements sont adressés au gouvernement, à des commandements militaires alliés et à celui de l'OTAN.

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

Le rapport 2000 du « Committee » souligne la qualité de la coopération dans le cadre du traité UKUSA [6] en en donnant pour preuve que le GCHQ a fourni des renseignements à la NSA américaine et à d'autres services pendant trois jours durant lesquels une panne du système américain privait ses clients habituels d'informations.

Le « Committee » appelle enfin le GCHQ à une plus grande rigueur budgétaire dans la réalisation de nouvelles infrastructures.

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

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

2.6.2. Autres réactions et commentaires en Grande Bretagne

La presse britannique aussi a publié de nombreux commentaires sur l'affaire « Echelon » dont les suivants méritent d'être cités.

Le député conservateur Daniel Hannan déclare dans le « Daily Telegraph » du 28 février 2000 *: « I'm proud we're spying on Europe ».*

Développant le thème de l'espionnage justifié par les pratiques de corruption des firmes françaises et celui de la solidarité anglo-saxonne, M. Hannan ajoute : *« When truly vital matters are at stake, the blood of the English-speaking peoples is thicker than the water of the Channel. We don't mind sharing our military secrets with Her Majesty's Canadian subjects, but how many of us could honestly claim to feel the same about the Belgians ?" (sic).*

Les commentaires de M. Jonathan Eyal, Director of Studies au « Royal United Services Institute for Defence Studies » à Londres [7]

Selon Jonathan Eyal, *« c'est le Renseignement qui freine la construction d'une structure européenne de la Défense. A de nombreux égards, le débat actuel sur le système « Echelon » se fourvoie et est complètement dépassé. D'une part, parce que les gouvernements anglo-saxons ne sont pas les seuls à pratiquer la surveillance électronique des communications : la France aussi dispose de «grandes oreilles » tournées vers les Etats-Unis (la DGSE).*

D'autre part, parce que le problème actuel des services de renseignement n'est plus de savoir comment collecter l'information, mais bien comment maîtriser l'immense quantité de données disponibles. L'idée que tous les courriers électroniques européens sont interceptés est absurde car aucun service de renseignement n'est en état de les traiter en totalité.

---

(6) A la connaissance du Comité R, c'est la première fois que l'existence du traité UKUSA est reconnue officiellement dans un document parlementaire britannique.

(7) Article paru le 30 mai 2000 dans le journal néerlandais « NRC Handelsblad ».

Par ailleurs, si l'espionnage est le plus souvent associé à la conduite de la guerre, les systèmes modernes de surveillance électronique sont en réalité les meilleures garanties possibles pour la paix. Ainsi, la surveillance électronique est le seul moyen disponible dont disposent les pays occidentaux pour lutter contre la prolifération des armes chimiques, bactériologiques et autres.

Le problème le plus délicat survient lorsque des communications entre entreprises privées sont interceptées. Une telle pratique est assurément blâmable et probablement illégale. Mais les choses ne sont pourtant pas si simples.

Dans les marchés internationaux, on trouve souvent plusieurs entreprises américaines en concurrence l'une avec l'autre ; en pareille situation, il est absurde de croire que Washington aiderait l'une au détriment de l'autre, car cela finirait bien par se savoir. De plus, la plupart des accusations d'espionnage commercial concernent des contrats d'armement qui sont les transactions les moins représentatives du commerce international. En effet, les fabricants d'armes ont toujours des liens étroits avec leurs gouvernements et ils ne peuvent opérer sur un marché libre.

Il n'y a d'ailleurs que dans les pays ou la vie économique est pour une bonne part dans les mains de l'Etat que des liens étroits peuvent se nouer entre les entreprises et les services de renseignement. Ceci n'est pas le cas des Etats-Unis, mais bien de la France.
Mais le temps des entreprises purement nationales est bien révolu, et par-là même, celui des liens avec les services de renseignement. Beaucoup de firmes de défense ne sont plus purement américaines ni purement européennes ; elles développent ensemble des projets de part et d'autre de l'Océan Atlantique. Certaines sont cotées en bourse.(…)

Enfin, dans la plupart des crises qui se sont produites dans le monde, les Européens et les Américains sont des alliés qui partagent leurs renseignements.

Londres a pris récemment l'initiative d'un plan de système de défense européen. Mais par sa relation avec les Etats-Unis, la Grande-Bretagne conserve cette position unique d'avoir accès au potentiel de renseignement d'une super puissance.

Ainsi que les conflits dans les Balkans l'ont montré, l'Union européenne est donc dépendante des Etats-Unis pour le renseignement et la Grande-Bretagne conserve sa position ambivalente en Europe. Les débats au Parlement européen et à la Commission n'y changeront probablement rien.

Le frein le plus important à la construction d'une structure européenne de défense reste donc les services de renseignement », selon M. Eyal.

2.7. Canada

2.7.1. Les rapports annuels du commissaire du Centre de la sécurité des télécommunications

Le Canada est, d'après le rapport de M. Campbell, l'un des Etats qui participe au réseau « Echelon ».

Ce pays dispose en effet d'un organisme équivalent à la NSA américaine ou au GCHQ britannique. Il s'agit du Centre de la sécurité des télécommunications (CST), organisme du ministère de la Défense nationale, dont la mission est de fournir au gouvernement du Canada des renseignements électromagnétiques (SIGINT) sur des pays étrangers.

Le CST obtient ces renseignements en interceptant et en analysant les transmissions par radio, par radar et par d'autres moyens électroniques très perfectionnés non précisés. Dans le cadre de son programme de sécurité des technologies, le CST donne aussi des conseils sur la sécurité des technologies de l'information du gouvernement.

Le CST est contrôlé par un Commissaire, nommé par le ministre de la Défense nationale, dont la tâche est de s'assurer que cet organisme agit conformément aux principes fondamentaux de la légalité canadienne et de la protection de la vie privée.

Le CST n'est pas autorisé à cibler les communications des citoyens canadiens ni celles des résidents permanents au Canada.

Le commissaire doit présenter un rapport annuel au ministre de la Défense nationale. Ce rapport est également déposé au Parlement.

Les rapports du Commissaire du CST sont publiés et le Comité R a pris connaissance des rapports des exercices 1998/1999 et 1999/2000. Il y a recherché d'éventuelles indications relatives à l'existence du réseau « Echelon ».

L'existence du réseau «Echelon » n'est évoquée en aucune manière dans les rapports. Cependant, sans la nommer de manière explicite, le commissaire canadien du SCT reconnaît officiellement l'existence de l'entente « UKUSA » :

« Le SCT reçoit des renseignements électromagnétiques recueillis par d'autres gouvernements. Il fournit également à ceux-ci des renseignements qu'il a lui-même recueillis. Ces accords de partenariat avec les Etats-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande ont été établis au cours de la Deuxième Guerre mondiale et maintenus pendant toute la durée de la guerre froide.».

Le commissaire relève à ce propos que les gouvernements des pays qui participent à cet échange de renseignements ont des politiques destinées à protéger la vie privée de leurs citoyens. Chaque gouvernement a convenu de ne pas effectuer, pour le compte de l'autre, de travail de collecte qui serait illégal dans un des pays partie prenante à l'entente.

Les renseignements recueillis par le CST sont, selon le commissaire, diffusés aux ministères chargés de protéger les intérêts du Canada sur les plans de la sécurité, du renseignement, de l'économie et de la défense.

Les rapports ne font pas état d'une quelconque diffusion à des sociétés privées. Les rapports du commissaire canadien traduisent son obsession que le CST n'enfreigne pas la vie privée des citoyens canadiens.

A ce sujet, on relève notamment les constatations suivantes :

« Des communications canadiennes peuvent se retrouver dans les fonds de renseignements du CST, car il est techniquement impossible, à l'heure actuelle, de les exclure totalement; le CST utilise les moyens techniques à sa disposition pour réduire l'interception involontaire de communications canadiennes ; le CST possède des politiques et des pratiques destinées à assurer la protection et le traitement approprié des communications canadiennes recueillies involontairement, conformément aux lois du Canada (…) ».

2.7.2. Autres réactions et commentaires au Canada

La presse internationale a relayé les déclarations contenues dans un livre du canadien Mike Frost. Celui-ci se présente comme étant un ancien membre du Centre de la Sécurité des Télécommunications (CST).

Il y affirme que le CST a autrefois intercepté les communications de deux ministres du gouvernement de Mme. Thatcher, sur demande expresse de ce premier ministre britannique.

Il s'agirait d'un cas d'espionnage politique. La législation britannique ne permettant pas l'écoute de ses propres citoyens, la pratique aurait été de s'adresser à un service ami étranger pour le faire.
Dans un article paru le 4 avril 2000 et intitulé *« A Vast Conspiracy ?* », le journal anglophone canadien « National Post » commente les réactions du gouvernement français sur les allégations concernant le système « Echelon » :

«What such comments seek to insinuate is that lacklustre performance of the French and other European economies is the result not of over-regulation and excessive taxation, but of the perfidious ways of English-speaking countries. French firms did not lose contracts because they were overpriced and inefficient, but because les « Anglo-saxons » cheated.

And in all this indignation, no one mentions the existence of the EU's K4 Committee, which is busy establishing its own Euro-Echelon to spy on electronic telecommunication traffic. But Europe's economic stagnation is not caused by Echelon and it will not be cured by a Euro-imitation of it".

3. L'ATTITUDE DES SERVICES DE RENSEIGNEMENT BELGES A L'EGARD DE LA PROBLEMATIQUE « ECHELON ».

Il ressort des constatations faites par le Comité R que les services de renseignement belges sont globalement restés passifs sur le sujet en invoquant principalement le fait qu'ils ne disposaient pas des possibilités légales techniques et humaines qui leur permettraient de constater eux-mêmes l'existence du système « Echelon ». La protection du potentiel scientifique et économique du pays est une mission de la Sûreté de l'Etat et non du SGR. Les seules informations dont ils disposaient sur le sujet provenaient de la consultation des sources ouvertes.

3.1. La Sûreté de l'Etat

Questionnée par le Comité R, l'administration générale de la Sûreté de l'Etat a déclaré que ce service :

« (…) n'avait aucune compétence technique ou légale pour s'occuper de problèmes de sécurité des communications ;

manquait de moyens, tant en personnel qu'en matériel, pour pouvoir vérifier la réalité de l'existence du système « Echelon »;

ne procédait pas au recueil de renseignements par satellites et qu'il n'avait aucun accès à ce type de source d'information;

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

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

qu'à part la communication en février 1999 d'informations tirées de sources ouvertes au ministre de la Justice en vue de lui permettre de répondre à des interpellations parlementaires, la Sûreté de l'Etat n'a jamais produit aucun rapport ni aucune note sur le système « Echelon ».

En ce qui concerne les objectifs économiques que viserait le système « Echelon », la loi organique du 30 novembre 1998 des services de renseignements, en son article 7, assigne une nouvelle mission spécifique à la Sûreté de l'Etat qui est la protection du *« potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel.* »

L'administrateur général a précisé que son service n'avait pas encore reçu d'instructions du Comité ministériel du Renseignement en matière de protection du potentiel scientifique et économique.

Une vérification effectuée par le Service d'enquêtes du Comité R a permis de constater qu'au moment même où celui-ci était chargé de la présente enquête par le Parlement, un agent de la Sûreté de l'Etat avait entrepris d'initiative une recherche de renseignements sur le réseau « Echelon » en consultant des sources ouvertes, notamment l'Internet.

Le produit de ces recherches a été transmis à la direction de la Sûreté de l'Etat qui n'y a cependant donné aucune suite.

3.2. Le Service Général du Renseignement et de la Sécurité (SGR)

Le SGR n'a pas connaissance de l'existence de réseaux étrangers d'interceptions des communications autrement que par les sources ouvertes, dans lesquelles on trouve de l'information mais aussi de la désinformation.

Le SGR considère néanmoins la menace venant des grands pays comme plausible et il applique donc le principe de précaution. Le service ne « suit » donc pas le système « Echelon » en particulier mais ce service considère que les interceptions de communications existent réellement, et que, quel que soit le pays qui les pratique, il faut s'en prémunir.

Le SGR considère également que n'importe quel système de chiffrement informatique est susceptible d'être cassé.

Le SGR ne dispose pas de moyens légaux techniques et humains nécessaires pour déceler l'existence du réseau « Echelon ». Le SGR n'effectue pas de recherche active sur ce réseau, se fondant, d'une part, sur le fait que la défense du potentiel scientifique et économique n'est pas une des compétences qui lui est attribuée par la nouvelle loi organique du 30 novembre 1998 sur les services de renseignements et, d'autre part, sur les restrictions légales qui lui sont imposées en matière de captage des radiocommunications.

S'agirait-il même d'un système d'espionnage militaire, qui lui relève de la compétence du SGR, ce service n'a pas pour priorité de suivre l'espionnage émanant des alliés de la Belgique. En cette matière, d'autres pays poursuivent des activités bien plus menaçantes pour les intérêts militaires belges.

Etant chargé de la sécurité des communications des forces armées, le SGR a élaboré différentes règles destinées à assurer la confidentialité des données classifiées transmises par télécommunication ou traitées par des réseaux informatiques. Une extension d'une telle mission à des intérêts autres que militaires n'est pas mentionnée explicitement dans la loi.

Toutefois, le SGR se propose de contribuer aussi bien à la conception des structures fédérales qu'à l'établissement d'une politique générale en matière de sécurisation des réseaux informatiques.

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

Par conséquent, le SGR suit de très près le développement de la législation en matière de cryptographie en Belgique. Le problème de la cryptographie est cependant très complexe vu qu'il se situe au croisement de plusieurs intérêts divergents : les intérêts économiques et commerciaux, la sécurité, la protection de la vie privée.

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

4. LE DEBAT SUR LA NSA_KEY DE MICROSOFT

Selon le périodique français « le Monde du Renseignement » n° 376 du 17 février 2000, le ministère français de la Défense nationale serait en possession d'un rapport de la Délégation aux affaires stratégiques (DAS) intitulé *« Sécurité des systèmes d'information : dépendance et vulnérabilité ».*

Ce rapport pointerait les défauts de fiabilité des logiciels Microsoft, mais surtout les manques de transparence et les risques de collusion avec les services de renseignement américains que ceux-ci impliquent.

Cette complicité de Microsoft permettrait d'offrir des facilités techniques à l'agence de renseignement américaine pour réaliser des intrusions et des interceptions de communications électroniques.

Le rapport de Messieurs Yves Poullet et Jean Marc Dinant, experts à qui le Comité R a confié la mission d'examiner, analyser et commenter tous les documents disponibles issus de sources ouvertes traitant de l'existence du réseau Echelon, mentionne ce qui suit à propos de ce problème :

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

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

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

3. *On imagine encore plus mal que le nom de cette clé soit « NSA_KEY ».*

Cette fausse alerte ne doit cependant pas faire croire que les fonctions de chiffrement fournies par Microsoft soient sûres. Les signataires de ce rapport partagent avec de nombreux experts l'opinion selon laquelle toute exportation d'outils de chiffrement hors des USA n'est autorisée que lorsque les services américains possèdent la capacité technique de casser le chiffrement. De toutes façons, il est actuellement généralement admis dans le monde de la cryptographie qu'un logiciel de chiffrement n'est fiable que lorsque l'on dispose de son code source. »

Dans son numéro 383 du 1er juin 2000, le périodique français « Le Monde du Renseignement » revient sur ce problème de l'éventualité de « backdoors » installés par la NSA dans le programme informatique sur lequel est bâti le système «Windows ». Pour Microsoft, la NSA_Key ne représente qu'une clé de sauvegarde.

Le journaliste Duncan Campbell, qui enquête sur la question, a demandé à un haut responsable de Microsoft de lui transmettre le détail du programme litigieux. Ce dernier a refusé au motif que cette diffusion violerait la propriété intellectuelle de Microsoft.

Un chercheur en cryptographie de l'Ecole polytechnique de Lausanne croit que les arguments avancés par Microsoft sont tout à fait vraisemblables, mais il n'exclut cependant pas l'éventualité d'une clé en possession de la NSA.

Le Comité R a redemandé l'avis de Monsieur Dinant [(8)] sur cette controverse et si, après lecture des informations précitées, il maintenait son point de vue selon lequel la NSA_Key n'est pas une clé secrète permettant à la NSA de décrypter des messages.
La réponse de Monsieur Dinant est la suivante (lettre du 14 juin 2000) :

« Après lecture de l'article paru dans le « monde du renseignement » et consultation de plusieurs sources ouvertes postérieures au rapport de février 2000 sur le réseau Echelon, je maintiens tout à fait et réaffirme avec force mon point de vue exposé à la section 4.2. du dit rapport.

(8) Monsieur Jean-Marc Dinant est doctorant en informatique et chercheur au Centre de recherches informatique et droit des facultés universitaires Notre-Dame de la Paix à Namur.

J'y ajoute que, depuis lors, Microsoft a répondu, selon moi, de manière transparente et honnête aux douze premières questions qui lui furent posées par écrit par Duncan Campbell. Par la suite ce dernier a reformulé de manière vexatoire et agressive certaines des questions auxquelles il avait déjà été répondu et en a rajouté d'autres. C'est à ce moment que Microsoft a décidé d'interrompre des « échanges non constructifs ».

Il est techniquement possible mais peu vraisemblable que cette deuxième clé (la NSA KEY) soit issue de la NSA. Même si cela était le cas, cela permettrait tout juste à cette dernière de falsifier la signature de contrôle de programmes cryptographiques.

Encore faudrait-il pouvoir télécharger sur la machine à espionner un programme cryptographique doté d'un cheval de Troie sans que l'utilisateur s'en aperçoive. En outre cette technique laisserait probablement pas mal de traces sur la machine espionnée elle-même. Il ne s'agirait donc pas d'une écoute applicable à tous et qui ne laisserait aucune trace.

Il est plus vraisemblable que cette NSA-KEY soit une clé de rechange de Microsoft, utilisable si la première clé originale venait à être détruite ou compromise. Dans ce cadre, le principal reproche fait à Microsoft est que l'utilisateur ne sait pas si c'est la clé originale ou la clé de rechange qui est utilisée pour valider les programmes cryptographiques installés sur sa machine. Un tel avertissement rendrait cette NSA KEY peu utilisable dans la pratique.

De l'avis de nombreux experts, la cryptographie « Made in Microsoft » présente bien d'autres lacunes et failles bien plus faciles à exploiter et le brouhaha médiatique autour de cette affaire ne doit pas distraire notre attention de ces failles et lacunes.

En conclusion, il est possible que la NSA_KEY ait été forgée par la NSA et il est actuellement impossible de prouver le contraire (probatio diabolica). Même si cette clé est l'œuvre de cette dernière, le danger directement créé par la connaissance de cette clé pour la sécurité des informations est minime dans l'absolu et relativement aux autres failles structurelles et ponctuelles de la cryptographie made in Microsoft ».

signé : Jean-Marc Dinant

5. CONCLUSIONS DU COMITE PERMANENT R

Le Comité R conclut ce qui suit :

1) en ce qui concerne l'existence « d'Echelon » et ses activités :

- ni l'existence, ni les capacités, ni les pratiques du réseau d'interception de communications, telles que décrites par le rapport STOA de M. Campbell n'ont jamais été reconnues officiellement par les gouvernements mis en cause (Etats-Unis, Grande Bretagne, Canada, Australie, Nouvelle-Zélande) ;

- quel que soit le nom de code donné à leurs systèmes (le code « Echelon » n'apparaît jamais dans les documents officiels récents), il est évident que les Etats-Unis, la Grande Bretagne, le Canada et l'Australie notamment, disposent de services officiels (la NSA, le GCHQ, le CST, le DSD) chargés d'intercepter des télécommunications à des fins de sécurité, mais aussi « *in the interest of the national well-beeing* » (dans l' intérêt du bien-être national) des pays concernés ;

- l'existence du traité UKUSA et celle d'une collaboration technique entre les organismes d'interception de ces cinq pays anglo-saxons sont à présent reconnues officiellement ;

- les capacités techniques et en personnel de ces services sont énormes : « Echelon » serait capable de capter la totalité des communications passant par satellites (environ un pour-cent des communications téléphoniques internationales) ;

- toutefois, la technologie ne permettrait pas encore une surveillance exploratoire et généralisée sur base d'un système de recherche automatique de mots clés dans des conversations téléphoniques; seuls existent actuellement des systèmes de reconnaissance d'empreintes vocales qui permettent de repérer la voix d'un individu spécifique lorsque celui-ci passe une communication internationale ;

- un tel système d'interception se heurte aussi à la maîtrise de l'immense quantité de données récoltées ;

- il existe des indices sérieux, mais aucune preuve certaine, que ces capacités d'écoutes peuvent être utilisées à des fins d'espionnage économique contre des entreprises de pays de l'Union européenne ;

- une telle pratique constituerait assurément une atteinte à la vie privée des citoyens et violerait les principes généraux du Conseil de l'Europe qui limitent strictement les interceptions de télécommunications ;

- les déclarations ambiguës des autorités américaines et britanniques à ce sujet ne permettent pas de lever le doute ;

- les garanties pour le respect de la vie privée et les recours offerts par les législations américaine, britannique et canadienne ne s'adressent d'ailleurs qu'aux citoyens et résidents de ces pays et non aux ressortissants des autres Etats ;

- M. James Woolsey, ancien directeur de la CIA, admet que la CIA pratique le renseignement économique mais il affirme que 95 % des informations collectées proviennent de sources ouvertes. Il affirme également que la CIA n'est pas engagée dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines.Pour M. Woolsey, il s'agit de mesures de protection justifiées par les manœuvres de corruption pratiquées par certaines entreprises européennes ; M. Woolsey n'indique pas les autres moyens mis en œuvre pour recueillir le renseignement ;

2) en ce qui concerne l'attitude des services de renseignement belges :

- les responsables de la Sûreté de l'Etat et du SGR déclarent que leurs services ne suivent pas le système « Echelon » étant donné qu'ils ne disposent pas des moyens humains, techniques et légaux nécessaires pour le faire ;

- le SGR déclare que l'espionnage militaire éventuel émanant de pays alliés de la Belgique ne constitue pas pour lui une priorité dans ses missions ;

- la Sûreté de l'Etat n'a pas encore reçu d'instructions du Comité ministériel du Renseignement et de la sécurité en matière de protection du potentiel économique et scientifique ; elle n'a pas encore affecté de moyens importants à cette nouvelle mission ;

- tant la Sûreté de l'Etat que le SGR regrettent de ne pas pouvoir procéder à des interceptions de sécurité dans un cadre légal ;

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

- étant chargé de la sécurité des communications des forces armées, le SGR a élaboré différentes règles destinées à assurer la confidentialité des données classifiées transmises par télécommunication ou traitées par des réseaux informatiques ;

- le SGR suit de très près le développement de la législation en matière de cryptographie; il préconise qu'un organisme officiel soit chargé d'assurer la politique de sécurité de l'information en Belgique.

6. RECOMMANDATIONS

- Constatant que les services de renseignement belges (Sûreté de l'Etat et SGR) n'ont entrepris aucun travail de recueil et d'analyse d'information à propos de l'existence éventuelle d'un réseau d'interception des communications européennes, appelé « Echelon », et piloté notamment par les Etats-Unis et la Grande Bretagne ;

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

- Considérant de manière plus générale que les possibilités technologiques actuelles permettent tant aux Etats qu'aux organisations criminelles d'intercepter des communications à grande échelle ;

- Considérant qu'une telle pratique est un moyen susceptible de procurer à une puissance étrangère, ou à une organisation criminelle, des informations confidentielles sur la sécurité, le potentiel scientifique et économique du pays ;

- S'associant aux conclusions et recommandations de MMS Poullet et Dinant ;

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

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

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

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

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

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

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

LES DOCUMENTS « SOURCES »

Les documents sur base desquels le présent rapport a été rédigé sont les suivants :

Les documents du Parlement européen :

- *"Development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control)"*;

  part 1/4 : "The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception" (mai 1999);

  part 2/4 : "The legality of the interception of electronic communications : a concise survey of the principal legal issues and instruments under international, European and national law" (avril 1999);

  part 3/4 : "Encryption and cryptosystems in electronic surveillance : a survey of the technology assessment issues" (avril 1999);

  part 4/4 : "The state of the art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition" (avril 1999);

  volume 1/5 : « 1) présentation des quatre études; 2) protection des données et Droit de l'Homme dans l'Union européenne et rôle du Parlement européen » (octobre 1999) ;

  volume 2/5 : "The state of the art in communications intelligence (COMINT) of auto mated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition" (octobre 1999) - Duncan Campbell;

  volume 3/5 : « Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie » (octobre 1999) - professeur Frank Leprévot;

  volume 4/5 : "The legality of the interception of electronic communications : a concise survey of the principal legal issues and instruments under international, European and national law" (octobre 1999) - professor Chris Elliot;

  volume 5/5 : "The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception" (octobre 1999)

- LEXICON –

Définition ' Source Ouverte' : Dans son rapport d'activités 1996, le Comité R a définit les sources ouvertes comme suit :
"les sources qui, d'un point de vue éthique ou légal, sont accessibles au public moyennant paiement ou non". (Rapport d'activités 1996 - Titre III - Chapitre 3 - p. 208).

BND : Bundesnachrichtendienst (Allemagne - Duitsland)

CIA : Central Intelligence Agency (USA)

CSE : Canadian Communications Security Establishment - provides the Government of Canada with foreign Sigint Intelligence

DGSE : Direction Générale de la Sécurité Extérieure (France - Frankrijk)

DSD : Defense Signals Directorate (Australia)

FBI : Federal Bureau of Investigation, the National Law Enforcement and Counter-intelligence agency of the USA

GCHQ : Government Communications Headquarters - the Sigint- agency of the UK

GCSB : Government Communications Security Bureau (New Zealand)

INTELSAT : International Telecommunications Satellite

JIC : Joint Intelligence Committee (UK)

LMR: Le Monde du Renseigement , périodique bimensuel édité en français et en anglais par le groupe INDIGO PUBLICATIONS, Paris, France

MI6 : Secret Intelligence Service (UK)

NSA : National Security Agency USA, the Sigint Agency of the USA

STOA : Science and Technology Options Assessment of the European Parliament

UKUSA agreement: Accord associant les Etats-Unis, la Grande Bretagne (UK-USA), le Canada, l'Australie et la Nouvelle Zélande.

La NSA et le GCHQ ont conclu en 1948 un accord secret, les unissant avec le CSE Canadien.

Le DSD australien , puis le GCSB néo-zélandais ont rejoint le consortium, qui travaille sur le renseignement politique et militaire, sur le trafic de drogue, le terrorisme et sur le monde économique .

CHAPITRE 2 : RAPPORT DE L'ENQUETE SUR LA MANIERE DONT LES SERVICES DE RENSEIGNEMENT (SURETE DE L'ETAT ET SGR) ONT REAGI A PROPOS D'EVENTUELS FAITS D'ESPIONNAGE OU DE TENTATIVES D'INTRUSION DANS LE SYSTEME INFORMATIQUE D'UN CENTRE DE RECHERCHE BELGE

1. INTRODUCTION

Le 19 juillet 2000, des parlementaires, membres des Commissions du Sénat et de la Chambre des Représentants chargées respectivement de l'accompagnement des Comités permanents R et P, ont demandé au Comité R de s'intéresser à d'éventuelles tentatives d'intrusion dans le système informatique d'un centre de recherche universitaire dont ils avaient eu connaissance.

Cette demande s'inscrivait dans le cadre de l'examen par lesdites commissions du rapport d'enquête sur la manière dont les services belges de renseignement réagissaient face à l'éventualité d'un système américain « *Echelon* » d'interception des communications téléphoniques et fax en Belgique.

Faisant suite à cette demande, une délégation du Comité R a rencontré le directeur et le responsable de la sécurité informatique de ce centre le mardi 25 juillet 2000. De cet entretien préliminaire, le Comité R a retenu les éléments qui suivent :

- alors qu'il venait de conclure en 1999 un contrat important de fourniture d'un certain matériel d'expérimentation avec un pays étranger, le centre a été la cible de tentatives d'intrusions dans son système informatique dont la direction situe la provenance en Allemagne et aux Etats-Unis (Washington) ;

- ce contrat avait été obtenu après que le gouvernement des Etats-Unis eût interdit à une firme américaine d'exporter ce même type de matériel pour des raisons de non prolifération ;

- ces tentatives d'intrusions électroniques furent suivies d'une effraction dans les bâtiments du centre au cours de laquelle les ordinateurs ont été manipulés et des composants informatiques volés (un clavier d'ordinateur) ;

- une enquête a été menée par la police sur ce vol avec effraction et c'est à cette occasion que les responsables du centre ont reçu la visite d'un inspecteur de la Sûreté de l'Etat. Le directeur du centre a également mis au courant certains parlementaires des faits précités ;

- selon le directeur, ce ne seraient pas tant les données technologiques du centre qui auraient été la cible de ces intrusions, car celles-ci sont disponibles dans la littérature scientifique et il n'est donc pas nécessaire de recourir à l'espionnage pour se les procurer. Selon lui, son centre ne détient aucune information sensible de haute technologie. Ce seraient plutôt les données commerciales du marché conclu avec le pays étranger qui auraient été visées.

Néanmoins, le Comité R a estimé que le centre en question pouvait être une cible intéressante non seulement pour l'espionnage économique et/ou technologique, mais également pour l'espionnage militaire puisqu'il est apparu au cours de l'entretien que ce centre devait prochainement tester du matériel militaire.

D'ailleurs, le directeur du centre a déclaré avoir rempli une demande d'habilitation de sécurité pour lui et son personnel et avoir reçu des consignes de sécurité très strictes pour l'entreposage de ce matériel dans ses locaux.

2. PROCEDURE

Le 11 août 2000, le Comité R s'est adressé au parquet du Procureur du Roi afin d'obtenir des informations concernant le vol avec effraction au centre de recherche en 1999. Ces informations ont été obtenues le 23 août 2000.

Le Comité R a décidé le 23 août 2000 d'ouvrir une enquête «*sur la manière dont les services de renseignement (Sûreté de l'Etat et SGR) ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge ».*

Une apostille a été adressée au chef du Service d'enquêtes le 28 août 2000.

Par courrier du 31 août 2000, conformément à l'article 32 de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le président du Comité R a informé le président du Sénat de l'ouverture de la présente enquête.

Par courrier du 31 août 2000, le chef du Service d'enquêtes, conformément à l'article 43-1° de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, a informé les ministres de la Justice et de la Défense nationale de l'ouverture de la présente enquête.

Le Service denquêtes du Comité R a procédé à divers devoirs d'enquêtes au cours du quatrième trimestre de l'année 2000. Il a rentré son rapport le 11 janvier 2001.

Après avoir examiné ce rapport, ainsi que le dossier de l'enquête, le Comité R a approuvé, à la date du 13 mars 2001, un rapport classifié « secret » en vertu de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

A la même date, le Comité R a également approuvé la version confidentielle du présent rapport au sens de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements destinée aux membres des commissions du Sénat et de la Chambre des Représentants chargées respectivement de l'accompagnement des Comités permanents R et P.

Cette version confidentielle est destinée à être publiée dans le rapport d'activités du Comité R.

3. CONSTATATIONS

3.1. Les constatations à la Sûreté de l'Etat

Un agent des services extérieurs de la Sûreté de l'Etat a bien suivi l'affaire du vol de matériel informatique au centre de recherche ainsi que les tentatives d'intrusion dans son système informatique.

Cette enquête trouve bien son fondement dans deux des missions légales attribuées à la Sûreté de l'Etat, à savoir rechercher, analyser et traiter le renseignement relatif à des menaces telles que la prolifération et l'espionnage économique et scientifique (articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).

Cette enquête a donné lieu à un échange interne de rapports classifiés entre les différents services de la Sûreté de l'Etat en charge des matières précitées.

Des observations particulièrement pertinentes y ont été consignées, notamment en ce qui concerne l'attitude du milieu scientifique universitaire à l'égard du problème de la sécurité des systèmes d'information, les risques liés à l'emploi de certains logiciels, les failles des systèmes de protections, l'exportation de certains matériels à usage dual, etc… .

Des propositions intéressantes d'ouverture et de collaboration avec les milieux scientifiques ont été émises. Un rapport indique même que le centre aurait sollicité l'expertise de la Sûreté de l'Etat.

Aucune suite ne semble avoir été donnée à ces remarques et propositions. La Sûreté de l'Etat ne dispose pas des compétences nécessaires pour assurer la sécurisation des systèmes informatiques des centres de recherche, elle n'a donc pas pu pourvoir à cette tâche.

Aucune application de l'article 19 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité n'a été constatée, à savoir qu'aucune information relative à cette affaire ne paraît avoir été communiquée à une quelconque autorité judiciaire, politique ou administrative compétente dans les matières traitées.

Le Comité R estime pourtant que certaines informations et recommandations contenues dans les rapports qu'il a examinés pouvaient être déclassifiées et utilement communiquées à certaines autorités.

3.2. Les constatations au SGR

Le SGR connaît le centre de recherche dans le cadre de l'habilitation de sécurité accordée pour lui permettre de travailler occasionnellement pour la Défense nationale. Cet intérêt trouve son fondement dans les missions attribuées au SGR par l'article 11 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le SGR déclare ne pas avoir été mis au courant des incidents de sécurité du centre, autrement que par le déclenchement de la présente enquête.

Le SGR justifie son absence d'intervention dans cette affaire en acceptant pour argent comptant les explications du responsable de la sécurité du centre qui déclare que les incidents n'ont pas affecté l'activité «Défense nationale» du centre. Le SGR n'a mené aucune enquête subséquente pour vérifier le bien fondé de cette allégation.

Le SGR justifie également son absence d'intervention par le manque de moyens humains qualifiés dont il dispose.

Pourtant, le fait que le centre soit actuellement investi d'une mission dans le cadre d'un projet international de développement militaire auquel le gouvernement belge veut s'associer ne semble pas avoir attiré spécialement l'attention du SGR.

3.3. Les constatations en ce qui concerne la collaboration entre la Sûreté de l'Etat et le SGR

Cette collaboration fut inexistante alors que ces deux services avaient chacun leurs intérêts légitimes pour s'occuper du centre. En ce sens, le SGR et la Sûreté de l'Etat n'ont pas fait application de leur devoir de collaboration prescrit par l'article 20 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

3.4. Les constatations en ce qui concerne la collaboration avec les services de police et le ministère public

Le Comité R constate que la Sûreté de l'Etat a recueilli auprès de la police une information concernant le vol avec effraction commis au centre de recherche, ce qui lui a permis de démarrer son enquête. Cette information a été recueillie de manière informelle.

Au niveau policier, ce vol a été traité sous le registre principal de « vol à l'aide d'effraction et escalade » et encodé comme tel. Si ce traitement correspond bien à la qualification pénale des faits constatés, il ne rend pas compte de l'intention sous-jacente éventuelle d'espionnage ; il ne permet pas non plus une exploitation statistique, analytique et criminalistique spécifique de ce phénomène au niveau national, voire international.

A la connaissance du Comité R, il n'existe pas au sein du ministère public de notice permettant de relier les procès-verbaux dressés à l'occasion des faits précités au thème de l'espionnage économique ou scientifique.

4. CONCLUSIONS GÉNÉRALES

La présente affaire est exemplative car elle démontre qu'il existe en Belgique des centres de recherches susceptibles d'être une cible intéressante non seulement pour l'espionnage économique et /ou technologique, mais également pour l'espionnage militaire.

La protection du potentiel scientifique et économique du pays est l'une des nouvelles missions de la Sûreté de l'Etat. Le maintien de la sécurité militaire, celle des installations, des systèmes informatiques et de télécommunications qui intéressent la Défense nationale, est une des missions du SGR.

Or, les tentatives d'intrusion et de vol au centre de recherche ne sont parvenus aux oreilles de la Sûreté de l'Etat que de manière fortuite. Le SGR n'en a été informé qu'à la suite de la présente enquête.

Si la Sûreté de l'Etat s'est activement investie à recueillir des informations sur cette affaire, le Comité R regrette la passivité du SGR en la matière. Les deux services n'ont pas collaboré.

Le Comité R regrette également qu'aucune suite n'ait été donnée aux demandes d'aide et propositions de collaboration entre le milieu scientifique et la Sûreté de l'Etat. Aucun service ne dispose en effet des compétences nécessaires pour assurer la sécurisation des systèmes informatiques des centres de recherche.

Le Comité R regrette enfin que l'intéressant travail de recueil de renseignements par la Sûreté de l'Etat n'ait trouvé aucun débouché vers une quelconque autorité judiciaire, politique ou administrative compétente dans les matières traitées.

Dans cette affaire, il n'a été fait aucune application des articles 19 et 20 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité, réglant la communication des informations d'une part, et la collaboration entre services d'autre part.

5. RECOMMANDATIONS

La conclusion d'un accord spécifique entre les autorités judiciaires et les services de renseignement, dans le cadre de l'article 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, devrait notamment viser à faciliter les échanges d'informations sur l'espionnage militaire, économique et scientifique entre ces autorités.

Dans un tel cadre, le Comité R se demande s'il ne faudrait pas réfléchir également à l'élaboration d'une notice spécifique relative à l'espionnage économique, scientifique et industriel. Celle-ci s'ajouterait aux notices classiques du droit pénal commun.

Par ailleurs, le Comité R ne peut que réitérer les recommandations qu'il a formulées à l'issue de son enquête menée « sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau « *Echelon* » d'interception des communications » et dont les constatations matérielles qui précèdent illustrent parfaitement la pertinence.

Pour mémoire, le Comité R a recommandé :

- de considérer l'éventualité de systèmes d'interceptions de communications mis en œuvre par des pays étrangers à des fins contraires aux intérêts légitimes de la Belgique (notamment la protection du potentiel scientifique et économique) comme hautement vraisemblable, à défaut d'être prouvée ;

- de donner par conséquent comme mission aux services de renseignement belges de collaborer en vue de recueillir toute information disponible (de source ouverte et autres) sur la question ;

- de donner aux services de renseignement les moyens techniques et humains nécessaires pour accomplir cette mission (en leur permettant notamment de faire appel à des experts externes comme des informaticiens, des ingénieurs en télécommunications, des spécialistes en cryptographie, des analystes, etc. …) ;

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

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

6. PROLONGEMENTS

Le présent rapport, approuvé le 13 mars 2001, a été adressé aux ministres compétents (ministre de la Justice et ministre de la Défense nationale) le 16 mars 2001 afin de recueillir leurs avis préalables en vue de sa publication, ceci conformément à l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le ministre de la Justice a communiqué son avis au Comité permanent R par lettre du 11 avril 2001. Celui-ci déclare se rallier au point de vue exprimé par l'administrateur général de la Sûreté de l'Etat dans une note du 5 avril 2001. Dans cette note, l'administrateur général confirme que la Sûreté de l'Etat n'a pas encore reçu de directive de la part du Comité ministériel du renseignement et de la sécurité concernant la manière d'exécuter sa mission de protection du potentiel scientifique et économique. Le projet de définition de cette notion que la Sûreté de l'Etat a élaboré après concertation avec le cabinet du ministre des Affaires économiques et celui du ministre des télécommunications, fait encore l'objet de discussions au sein du Collège du renseignement et de la sécurité.

Dans une lettre adressée le 28 mars 2001 au chef du Service d'enquêtes du Comité R, la Sûreté de l'Etat a fait savoir qu'elle avait «*réagi par une démarche de prospection le 26 septembre 2000, à l'invitation de l'Université de (x), en vue d'une sensibilisation à (sa) nouvelle mission ».* A la suite de cette rencontre, les mesures nécessaires auraient été prises au niveau du centre de recherche cité dans la présente enquête, notamment en constituant un groupe de travail chargé d'examiner les mesures de sécurité à prendre. Sur base de son expérience spécifique, la Sûreté de l'Etat se déclare disposée à collaborer avec les responsables pour attirer leur attention sur des problèmes ponctuels de sécurité en ne pouvant toutefois pas se porter garante de l'exécution des mesures prises par ceux-ci, tant sur le plan des systèmes d'information que de l'infrastructure et du personnel.

La Sûreté de l'Etat considère également que sa mission légale est de recueillir, de traiter et d'analyser le renseignement de sécurité, mais non d'assurer elle-même la sécurité des systèmes d'informations. Elle ne peut donc s'engager à acquérir elle-même les compétences humaines et techniques nécessaires à remplir une telle mission qui relève plutôt des compétences du gouvernement fédéral. Ce service déclare d'ailleurs qu'il offre son expertise extérieure au projet FEDICT qui tend à la mise sur pied d'un organe chargé de la sécurité des systèmes d'information.

Pour la Sûreté de l'Etat, il est donc clair qu'en cette matière, les tâches de prospection et celles en rapport avec ses missions traditionnelles mises à part, elle ne peut encore s'engager dans la voie du recueil de renseignements qu'avec prudence, et ce, aussi longtemps qu'elle n'aura pas reçu les directives nécessaires du Comité ministériel du renseignement et de la sécurité.

Par courrier du 25 avril 2001, le ministre de la Défense nationale a fait part au Comité R de ses observations. Il a insisté pour qu'une confusion ne soit pas faite entre deux missions distinctes du SGR.

D'un côté, la mission légale reprise dans la loi organique des services de renseignements, en particulier la protection du secret des systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense gère et de l'autre côté le contrôle dans les firmes agréées travaillant au profit de la Défense dans lesquelles des informations classifiées sont détenues ou traitées, mission issue de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité. En ce qui concerne le Centre de recherche concerné c'est surtout dans le cadre de la seconde mission que le SGR est intervenu, la protection du potentiel scientifique ou économique étant une mission légale de la Sûreté de l'Etat prévue dans la loi organique.

Le Comité R reste persuadé que les conclusions et prolongements qui précèdent suscitent toujours des interrogations sur la manière dont la Sûreté de l'Etat et le SGR ont traité le problème ici abordé ; il maintient par conséquent sa décision de poursuivre son enquête sur le sujet.

B. ENQUETES A L'INITIATIVE DU COMITE R

CHAPITRE 1 : RAPPORT RELATIF A L'ENQUETE SUR LE FONCTIONNEMENT DE LA SECTION « LEGISLATION » EN MATIERES D'ARMES DE LA SURETE DE L'ETAT

1. INTRODUCTION

En 1998, le Comité R a mené une enquête relative aux compétences du service « législation en matière d'armes » de la Sûreté de l'Etat afin d'apprécier si cette matière devait bien relever de ce service de renseignement [1]. Pour rappel, la Sûreté de l'Etat est compétente pour délivrer les permis suivants aux étrangers sans résidence en Belgique, ainsi qu'aux belges résidant à l'étranger :

- les autorisations de détention d'une arme à feu de défense ou de guerre;
- les permis de port d'arme de défense;
- les autorisations temporaires de détention d'une arme de défense ou de guerre;
- les permis temporaires de port d'arme de défense (cartes européennes d'armes à feu).

Outre ses compétences décisionnelles précitées en matière d'armes, la Sûreté de l'Etat rend des avis à l'intention d'autres instances chargées de l'application de la législation sur les armes, à savoir, les gouverneurs de province, les polices communales et l'Office des Etrangers.

Ces avis concernent essentiellement :

- les permis de port d'arme pour les membres du personnel des représentations diplomatiques qui ne bénéficient pas de l'exonération d'inscription dans les registres communaux;
- les agréments d'armuriers (article 27 de la loi du 3 janvier 1933 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions);
- les permis de port d'arme pour les membres des services de gardiennage;
- les belges naturalisés dont les activités concernent la Sûreté de l'Etat;
- les demandes introduites par des étrangers résidant en Belgique.

[1] Comité R, rapport d'activités 1998, p. 103

Dans les conclusions de son rapport, le Comité R avait recommandé :

- 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'arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

En 1999, le Comité R a décidé de poursuivre sa réflexion sur le sujet :

- en examinant de plus près le fonctionnement du service « législation en matière d'armes » de la Sûreté de l'Etat d'une part;

- en évaluant l'importance quantitative de l'exercice de cette mission d'autre part.

2. PROCEDURE

Par apostille du 13 juillet 1999, le président du Comité R a dès lors chargé le Service d'enquêtes de procéder à certaines vérifications qui couvrent l'année 1998 et les six premiers mois de l'année 1999.

Par courrier du 27 juillet 1999, conformément à l'article 43, 1° de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements, le ministre de la Justice, a été averti de l'ouverture et de l'objet de l'enquête par les soins du chef du Service d'enquêtes.

Le Service d'enquêtes a remis son rapport au Comité R le 16 novembre 1999.

Le Comité R a adressé une nouvelle apostille au Service d'enquêtes le 1er septembre 2000 lui demandant de procéder à quelques vérifications complémentaires.

Le Service d'enquêtes a remis son rapport complémentaire au Comité R le 24 octobre 2000.

Le Comité R a demandé un complément d'information à la Sûreté de l'Etat le 29 décembre 2000.

La Sûreté de l'Etat a communiqué sa réponse le 6 février 2001.

Le présent rapport a été approuvé le 15 février 2001.

Par courrier du 6 avril 2001, le ministre de la Justice a fait valoir ses observations. Celles-ci contenues dans une note classifiée « Confidentiel – loi du 11 décembre 1998 » ont pu être transmises aux Commissions de suivi P et R après avoir fait l'objet d'une déclassification de la part de la Sûreté de l'Etat . Ce document porte cependant la mention « Diffusion restreinte » [2] et ne peut être reproduit « in extenso » dans le présent rapport

3. CONSTATATIONS

3.1. L'analyse et la diffusion de l'information par la Sûreté de l'Etat

3.1.1. Le service d'étude « législation armes »

Il existe au sein des services administratifs de la Sûreté de l'Etat, un service d'étude chargé de l'application de la législation en matière d'armes.

Depuis 1997, le service « législation armes » est également chargé d'examiner toutes les formes de prolifération qui peuvent contribuer à l'application ou au développement de systèmes d'armement non conventionnels ou très avancés; cette compétence s'étend aux formes et structures du crime organisé qui se rapportent intrinsèquement à la prolifération.

L'introduction de ces nouvelles compétences résulte des articles 7 et 8 *d)* et *f)* de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Le service prolifération et armes est tenu de transmettre toutes les informations utiles aux services compétents pour les autres matières traitées par la Sûreté de l'Etat. La transmission inverse d'informations utiles doit également être assurée.

Le service « législation armes » est placé sous la direction d'un conseiller adjoint statutaire (troisième grade du niveau 1) .

Au 1er décembre 2000, ce service comptait sept personnes. Le responsable du service « législation armes » représente la Sûreté de l'Etat aux réunions du Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes

[2] Eu égard à certaines informations, cette mention limite la diffusion aux personnes qualifiées pour en connaître sans attacher à cette limitation les effets juridiques prévus par la loi (art. 20 de l'A.R. du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité).

3.1.2 Le Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes (CITI)

Ce comité a été créé par un arrêté royal du 9 février 1999. Il a pour mission *d'optimaliser la coordination et l'échange d'informations en matière de lutte contre les transferts illégaux d'armements, afin de permettre à tous les services concernés par le commerce des armes de mieux exercer les compétences qui leur ont été attribuées* [3].

Le CITI réunit le Magistrat national et des représentants des ministères des Affaires étrangères, du Commerce extérieur et de la Coopération au Développement, de la Justice, des Affaires économiques, de l'Intérieur, des Finances, de la Défense nationale (le SGR), de la Gendarmerie et du Banc d'épreuves des armes à feu.
La Sûreté de l'Etat a été chargée, en collaboration avec le SGR et la Gendarmerie d'élaborer un questionnaire destiné à connaître les compétences respectives de chacun des membres du CITI en matière d'armes, et d'identifier leurs besoins en informations. Selon les réponses apportées à ce questionnaire, le CITI élaborera un projet de protocole d'accord sur l'échange d'informations entre les membres.

Les membres du CITI distinguent parmi eux les "*autorités »* d'une part, les "*services »* d'autre part.

- Par "*autorités*" il faut entendre les membres du CITI qui, sur base de l'information dont ils disposent ou qui leur est fournie, doivent prendre des décisions, les faire appliquer et contrôler et qui doivent mener une politique administrative ou judiciaire.

- Par "*services* ", on entend les fournisseurs d'information (e.a. les services de police) et les exécutants (e.a. les services de contrôle) qui ont pour mission de préparer et d'exécuter de manière adéquate les décisions prises par les "autorités". De par sa compétence, la Sûreté de l'Etat est considérée comme un "service".

En attendant la conclusion d'un protocole d'accord sur l'échange d'information, le CITI peut déjà jouer un rôle important de coordination. Dans la pratique, la collaboration entre la Sûreté de l'Etat et les autres services se construit en fonction de cas concrets.

3.1.3. Les réunions interdépartementales sur la prolifération

Depuis 1999, la Sûreté de l'Etat participe également à des réunions interdépartementales (Affaires étrangères, Finances, Affaires économiques, Justice, Défense nationale, Forces armées et Ecole Royale militaire) chargées de veiller à ce que les exportations de matériels et d'équipements ne contribuent pas à la dissémination d'armes chimiques ou biologiques.

Dans ce cadre, la Sûreté de l'Etat a produit des informations relatives à l'intérêt porté par des groupes terroristes à la confection d'armes non-conventionnelles.

---

[3] Article 3 de l'arrêté royal du 9 février 1999 instituant le Comité de coordination interdépartemental pour la lutte contre les transferts illégaux d'armes.

3.2. L'octroi des autorisations de détention et de port d'arme (armes de défense ou armes de guerre)

Pendant la période du 1er janvier 1998 au 31 décembre 2000, 5.003 autorisations ont été délivrées par le service "législation armes" à des étrangers et à quelques citoyens belges sans résidence en Belgique.

Ce chiffre se répartit comme suit :

	AUTORISATIONS DE DETENTION ET PERMIS DE PORT D'ARME	***AUTORISATIONS TEMPORAIRES (CARTES EUROPEENNES D'ARMES A FEU)***	***TOTAUX***
1998	1.175	210	1.385
1999	1.625	256	1.881
2000	1.481	256	1.737
Totaux	***4.281***	***722***	***5.003***

Les étrangers bénéficiaires sont principalement des gendarmes et des agents de protection qui accompagnent des personnalités étrangères en Belgique, mais aussi des citoyens ordinaires, des militaires employés au SHAPE, des diplomates d'ambassades étrangères en poste en Belgique, des policiers en transit en Belgique, des tireurs sportifs participant à des compétitions de tir organisées par des associations de tireurs belges reconnues.

C'est dans ce cadre que la Sûreté de l'Etat traite et régularise les cartes européennes d'armes à feu.

Les motifs invoqués lors de la requête relèvent de l'auto-défense, du sport et de la chasse. Dans des cas exceptionnels, des autorisations temporaires ont été refusées à des agents de protection qui accompagnaient des personnalités étrangères ainsi qu'à des tireurs sportifs. Les raisons étaient que ces demandes étaient incomplètes ou avaient été introduites tardivement.

Il n'y pas eu de demande adressée à la Sûreté de l'Etat émanant de citoyens belges résidant à l'étranger en vue d'exporter des armes vers des pays soumis à un embargo.

Une note de service du 16 mars 1992 indique le modus operandi applicable aux demandes introduites par des étrangers pour obtenir une autorisation de détention (d'armes de défense ou d'armes de guerre) ou un permis de port d'arme.

Outre les motifs des demandes, la Sûreté de l'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 procède alors à une enquête plus approfondie.

Par note du 14 mai 1986 adressée à l'administrateur directeur général de l'époque, le chef de cabinet du ministre de la Justice avait toutefois estimé que "*le seul fait de savoir si la personne est connue ou non de vos services* (n'offrait) *pas les garanties suffisantes*"; il prescrivait par conséquent qu'il soit désormais procédé à une enquête à l'étranger.

En ce qui concerne les particuliers qui viennent pratiquer le tir sportif ou la chasse occasionnellement en Belgique, la Sûreté de l'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. Cependant, c'est au demandeur lui-même qu'il est demandé de produire la preuve de la réalité du motif qu'il invoque à l'appui de sa demande, par exemple en produisant sa carte d'affiliation à un club sportif reconnu, une invitation reçue d'un club belge reconnu, etc… .

La Sûreté de l'Etat ne procède pas à une enquête particulière pour chaque cas. Elle consulte sa documentation permanente sur les clubs sportifs de tirs (statuts parus au Moniteur belge, etc…). En cas de doute elle peut consulter des services correspondants étrangers mais il n'existe pas de procédure internationale de consultation réciproque entre services de renseignement et de sécurité. Aucune demande de renseignement n'a été adressée à un service étranger.

Jusqu'à présent il n'y a pas eu d'échange spécifique et systématique de données entre la Sûreté de l'Etat et le S.G.R. concernant l'application de la législation belge sur les armes à feu telle qu'elle est appliquée par le service « législation armes ».

L'autorisation de détention et/ou de port d'arme est signée par des fonctionnaires de la Sûreté de l'Etat, tous de niveau 1 et désignés par arrêté ministériel.

Le permis de port d'arme doit accompagner l'arme autorisée et doit être présenté à toute réquisition des autorités. Son titulaire doit informer l'administration de la Sûreté de l'Etat en cas de perte ou de vol de l'arme durant son séjour en Belgique.

La note de service du 16 mars 1992 n'indique pas quel est le modus operandi applicable aux retraits ou aux suspensions d'autorisation de détention et de port d'arme.

Pendant la période du 1er janvier 1998 au 31 décembre 2000, aucune autorisation de détention, ni aucun permis de port d'arme n'a été suspendu ou retiré.

Les procédures de suspension et de retrait des autorisations ne peuvent bien sûr s'appliquer que pendant les séjours en Belgique des titulaires desdits documents. En cas de court séjour, l'application de ces procédures semble quelque peu aléatoire.

La Sûreté de l'Etat déclare que si elle avait connaissance d'activités violentes de la part d'un titulaire d'un port d'arme, elle en avertirait en premier lieu les autorités judiciaires dont la décision constituerait alors la base du retrait de l'autorisation.

3.3. Les demandes d'avis

Pour la période du 1er janvier 1998 au 31 décembre 2000, le service armes n'a reçu que 164 demandes d'avis écrits (48 en 1998, 75 en 1999, 41 en 2000) de la part des gouverneurs de provinces, de l'Office des Etrangers ou des communes.

La Sûreté de l'Etat a également été consultée quelquefois en vue de la délivrance des permis de port d'arme pour les membres des services de gardiennage, des organisations internationales ou des représentations diplomatiques en Belgique, ainsi que l'a recommandé l'Administration des affaires criminelles et pénales en 1994.

Sachant qu'au cours de la même période, on a délivré en Belgique près de 48.000 autorisations de détention d'arme à feu et permis de port d'arme [4], on constate que la Sûreté de l'Etat n'a été consultée que dans moins d'un pour cent des cas où elle-même n'est pas compétente pour délivrer ces autorisations de détention ou de port d'arme.

Lorsqu'elle est consultée, la Sûreté de l'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.

Pour les avis à l'égard des étrangers non domiciliés en Belgique, la Sûreté de l'Etat consulte son correspondant étranger. En ce qui concerne les diplomates, les modalités d'octroi sont déterminées cas par cas.

En ce qui concerne les armuriers, la Sûreté de l'Etat procède à une enquête rapide sur les activités des intéressés. Elle consulte sa documentation générale relative aux trafics d'armes. Cette enquête n'est pas aussi approfondie qu'une enquête de sécurité. La police judiciaire procède aussi à une enquête. Ces deux enquêtes font parfois double emploi.

3.4. L'information de la Sûreté de l'Etat par les gouverneurs de province et par les polices communales

Au cours de la période visée, la Sûreté de l'Etat n'a pas été avisée par les gouverneurs de province de leurs décisions relatives aux demandes de permis de port d'arme pour le personnel des missions diplomatiques ou équivalent alors qu'ils sont requis de le faire par la circulaire coordonnée du 30 octobre 1995 relative à l'application des dispositions légales et réglementaires dans le domaine des armes.[5]

---

[4] Selon les statistiques fournies au Comité R par la direction de la banque de données nationale – registre central des armes

[5] Moniteur belge des 28 novembre 1995 et 29 février 1996.

De même, les polices communales doivent transmettre à la Sûreté de l'Etat, dans les huit jours, une copie de l'autorisation de détention d'une arme de défense délivrée à un membre d'une représentation diplomatique non exonéré d'inscription dans le registre communal ou à un belge naturalisé dont les activités concernent la Sûreté de l'Etat.

Au cours de la période visée, la Sûreté de l'Etat n'a été avertie qu'une seule fois par une police communale de la délivrance d'une autorisation à un membre d'une mission diplomatique non exempté d'inscription au registre communal.

Par ailleurs, le Comité R constate que si l'arrêté royal du 21 septembre 1991 oblige la Sûreté de l'Etat à alimenter le Registre central des armes en informations, celui-ci par contre ne reste accessible qu'à un nombre strictement limité d'autorités judiciaires, administratives et de police au nombre desquelles ne figurent pas les services de renseignement.

La Sûreté de l'Etat ne peut donc, en principe, avoir une vue globale sur l'ensemble des autorisations de ports d'arme délivrés en Belgique.

Il faut cependant savoir que si la Sûreté de l'Etat ne dispose pas d'un accès par voie électronique au Registre central des armes, elle a toujours eu une réponse à ses demandes de renseignements par fax.

3.5. Le suivi des dossiers

Le Comité R a demandé à la Sûreté de l'Etat quel était le suivi éventuel du dossier une fois l'autorisation accordée ou l'avis donné (par exemple en cas de découverte d'éléments nouveaux susceptibles de modifier la décision ou l'avis), ou après l'expiration du délai d'autorisation.

L'administration de la Sûreté de l'Etat déclare qu'une fois l'autorisation délivrée et l'avis donné, la demande est conservée par le service « législation armes ».

Si des informations défavorables lui parvenaient concernant la personne à laquelle une autorisation a été délivrée ou une personne au sujet de laquelle un avis a été demandé, ce service y donnerait une suite appropriée sur base de la législation en vigueur.

Le Comité R n'a pas été en mesure de vérifier un cas d'application de cette résolution vu que la Sûreté de l'Etat déclare n'avoir reçu depuis 1998 aucun renseignement défavorable concernant une personne à qui une autorisation a été délivrée.

4. LA POSITION DE LA SURETE DE L'ETAT

Le 2 février 2000, l'administrateur général de la Sûreté de l'Etat a fait parvenir une note au ministre de la Justice dans laquelle il se déclare d'accord avec la recommandation du Comité R de retirer à son service toutes les compétences décisionnelles qu'il détient en matière d'exécution de la législation sur les armes à feu.

L'administrateur général plaide aussi pour que soit attribuée à son service une compétence d'avis générale et préalable à la délivrance ou au retrait de toute autorisation de détention d'une arme à feu de défense et de guerre ainsi que de tout permis de port d'arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l'étranger).

Mais contrairement au Comité R, l'administrateur n'estime pas que l'octroi 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 relative à la fabrication, au commerce et au port des armes, et au commerce des munitions. Selon lui, une circulaire ministérielle suffirait.

5. CONCLUSIONS ET RECOMMANDATIONS

La section d'étude « législation armes » de la Sûreté de l'Etat exerce les deux compétences que ce service détient en matière d'exécution de la législation sur les armes à feu : une compétence décisionnelle et une compétence d'avis à l'égard des étrangers et des citoyens belges sans résidence en Belgique.

Pendant la période du 1er janvier 1998 au 31 décembre 2000, 5.003 autorisations de détention et ports d'armes ont été délivrées par le service "législation arme "à des étrangers et à quelques citoyens belges sans résidence en Belgique, alors que pour la même période, ce service n'a reçu que 164 demandes d'avis écrits de la part des gouverneurs de provinces, de l'Office des Etrangers du Ministère de l'Intérieur ou des communes.

Sachant qu'au cours de ces trois années, on a délivré en Belgique près de 48.000 autorisations et permis de port d'arme, on constate que la Sûreté de l'Etat n'a été consultée que dans moins d'un pour cent des cas où elle-même n'est pas compétente pour délivrer ces autorisations de détention ou port d'arme.

Le Comité R reste pourtant d'avis que les compétences décisionnelles de la Sûreté de l'Etat n'ont aucun lien avec les activités naturelles d'un service de renseignement qui consistent à informer les autorités des menaces tant internes qu'externes pouvant peser sur la Belgique. La compétence d'avis de ce service est par contre celle qui entre le mieux dans le cadre de la mission d'information précitée.

Le Comité R constate par ailleurs que dans la pratique, la Sûreté de l'Etat n'a pas une vue globale sur les autorisations de détention et port d'arme délivrées en Belgique.

Le Comité R recommande qu'il soit remédié à cette lacune, notamment en permettant l'accès de la Sûreté de l'Etat au registre central des armes.

Le Comité R réitère par ailleurs les recommandations qu'il a formulées en 1998 et qui restent d'actualité, à savoir :

- retirer à la Sûreté de l'Etat toutes les compétences décisionnelles qu'elle détient en matière d'exécution de la législation sur les armes à feu ;

- attribuer par contre à ce service une compétence d’avis générale et préalable à la délivrance ou au retrait de toute autorisation de détention d’une arme à feu de défense et de guerre ainsi que de tout permis de port d’arme de défense, et ceci quel que soit le lieu de résidence du demandeur (en Belgique ou à l’étranger).

CHAPITRE 2 : LA MANIERE DONT LES SERVICES DE RENSEIGNEMENT ONT TRAITE LES ACTIVITES DE L'ANCIEN KGB EN BELGIQUE

1. INTRODUCTION

1.1. Procédure

Suite aux nombreux articles de presse reprenant les révélations contenues dans le livre intitulé «*The Mitrokhin Archive The KGB in Europe and the West* »[1] de l'historien Christopher Andrew, et la découverte dans notre pays de trois dépôts clandestins du KGB contenant du matériel de transmission, le Comité R a décidé le 6 octobre 1999 d'ouvrir une enquête de contrôle intitulée : *«La manière dont les services de la Sûreté de l'Etat et du SGR ont traité les informations relatives aux activités de l'ancien KGB en Belgique»*.

En application de l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le président du Sénat a été informé de l'ouverture de cette enquête par courrier du 13 octobre 1999.

Le président du Comité R a adressé le 12 octobre 1999 une apostille circonstanciée en la matière au Chef du Service d'enquêtes.

Conformément à l'article 43.1 de la loi organique précitée, les ministres de la Défense nationale et de la Justice ont pour leur part été avertis, par lettre du 3 novembre 1999, du début de l'enquête de contrôle.

Le 8 novembre 1999, le président du Comité R a demandé à Monsieur le Procureur Général près la Cour d'Appel de Bruxelles, l'autorisation pour le Chef du Service d'enquêtes du Comité R de prendre connaissance et copies des pièces du dossier judiciaire relatif à la découverte du matériel de transmission enterré dans diverses caches.

Cette autorisation a été accordée le 21 décembre 1999.[2]

Le rapport du Service d'enquêtes a été communiqué au Comité R le 24 mars 2000.

Une version du rapport classifiée «confidentielle» aux termes de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité a été approuvée par le Comité R le 16 mars 2001.

La présente version adressée au Sénat, ainsi qu'aux ministres de la Justice et de la Défense nationale qui est également la version destinée au rapport public, a été approuvée par le Comité R le 16 mars 2001.

---

1 Publié par ALLEN LANE - THE PENGUIN PRESS.

2 L'affaire a été classée sans suite par les autorités judiciaires après la transmission des informations à celles-ci par le SGR et la découverte des caches et du matériel s'y trouvant.

Par courrier du 11 avril 2001, monsieur le Ministre de la Justice a fait valoir ses observations dans une note classifiée « Confidentiel – loi du 11 décembre 1998 ».

A la demande du Comité R, cette note a été déclassifiée pour être transmise aux Commissions de suivi P et R avec la mention « Diffusion restreinte »[3].

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas de remarque à formuler quant à la publication de ce rapport.

1.2. Les questions posées aux services de renseignement

1. Quelles sont, de manière générale, les possibilités d'accès de la Sûreté de l'Etat et du SGR aux «archives Mitrokhin» ?

2. Quand et comment nos services ont-il été informés de l'existence de ces archives ?

3. Dans quelle mesure nos propres services de renseignements (section contre-espionnage) ont-ils recueilli des informations concernant les activités mentionnées dans ces archives ?

4. Les données ainsi recueillies concernent-elles uniquement les caches de matériel ou bien existe-t-il également des informations relatives à des personnes ou à des personnalités qui auraient travaillé en Belgique pour le compte du KGB ou du GRU[4] ?

5. Comment les informations reçues ont-elles été exploitées ? Ont-elles été transmises, en tout ou en partie, à des tiers ? Le cas échéant, à qui et à quel moment ?

6. Y-a-t-il encore des informations qui n'ont pas été exploitées et/ou transmises ou qui sont actuellement traitées ?

7. Comment se passe la coopération avec d'autres services nationaux et étrangers (y compris les autorités policières et judiciaires belges) ?

8. Les faits relatés dans les archives doivent-ils être uniquement considérés dans un contexte historique ou peut-on considérer qu'à l'heure actuelle, il y a lieu de craindre ou même d'être certain que le SVR qui a succédé au KGB poursuit des activités d'espionnage ?

9. Quid des relations qui existeraient entre des anciens membres du KGB qui se sont reconvertis dans le monde des affaires et la criminalité organisée ?

10. Les services de renseignement estiment-ils disposer aujourd'hui des moyens nécessaires pour aborder cette problématique de manière efficace et quels sont ces moyens ? Si ce n'est pas le cas, comment vont-ils faire en pratique ?

---

[3] Eu égard à certaines informations, cette mention limite la diffusion aux personnes qualifiées pour en connaître sans attacher à cette limitation les effets juridiques prévus par la loi (art. 20 de l'A.R. du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité).

[4] L'équivalent militaire du KGB

11. Quelles sont les conclusions que la Sûreté de l'Etat et le SGR tirent de leur expérience passée afin de mieux limiter les menaces d'espionnage ? Existe-t-il des documents, directives ou rapports à ce sujet ? Qui en sont, le cas échéant, les destinataires autres que la Sûreté de l'Etat et le SGR eux-mêmes ?

2. GENERALITES

Les concepts de base de l'échange d'informations

La Sûreté de l'Etat est le service spécifiquement chargé de la mission défensive de contre-espionnage par la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (articles 7 et 8).

Il a donc semblé utile au Comité R de donner, dans la perspective du sujet précis concerné par l'enquête, quelques informations de nature plus générale concernant plus particulièrement la Sûreté de l'Etat.

Ces informations ont été fournies par le Service d'enquêtes du Comité R en tenant compte également de l'expérience de certains membres de ce service dans le domaine particulier abordé par la présente enquête.

2.1. Les relations avec les correspondants

2.1.1. Organisation

La loi organique des services de renseignement et de sécurité du 30 novembre 1998 charge la Sûreté de l'Etat d'entretenir des contacts directs avec des autorités étrangères et de veiller à assurer une coopération avec les services de renseignement et de sécurité étrangers[5].

Cette coopération doit être utile à la Sûreté de l'Etat pour remplir ses missions parmi lesquelles figure la recherche, l'analyse et le traitement des renseignements relatifs à toute activité qui menace notamment d'une manière générale les intérêts fondamentaux du pays.[6]

Au sein de la Sûreté de l'Etat, le service chargé des relations internationales est un des services d'intérêt général, responsable des relations bilatérales avec les *«correspondants»*, (c'est-à-dire avec les services étrangers de renseignement et de sécurité) et des relations multilatérales.

Ce service est chargé des dossiers du *«Club»* et de la *«Mec»* (voir point 2.1.2. ci-après).
A cette fin, il assure le suivi de toute la correspondance reçue et transmise à ce sujet, il est chargé d'en vérifier la recevabilité et de s'assurer qu'une suite y est donnée.

Ce service assure également la répartition des informations qui arrivent sous la forme de notes; il organise les contacts et suit l'évolution de chaque service correspondant.

5 Article 20
6 Article 7 1° de la même loi organique des services de renseignement.

2.1.2. Les contacts internationaux

La Sûreté de l'Etat entretient des relations avec une soixantaine de services étrangers ou internationaux répartis sur les cinq continents.

Il va de soi que les relations internationales auxquelles la priorité est donnée sont celles qui se situent dans le cadre de ce qu'il est convenu d'appeler «les pays alliés», en particulier ceux qui sont voisins de la Belgique.

La Sûreté de l'Etat fait partie de certains réseaux d'information auxquels participent tous les autres pays de l'Union européenne. Elle fait partie également de deux associations de coopération, dont il a déjà été question ci-dessus, à savoir : le *«Club»* et la *«Mec»*.

Le *« Club de Berne »*

Il s'agit d'une association de fait des chefs des services de sécurité des pays d'Europe de l'Ouest dont la création remonte à 1965 et qui fonctionne suivant des règles strictes de procédure.

Tous les six mois une réunion a lieu et seuls les chefs des services - ou leur représentant - peuvent prendre des décisions à l'unanimité.

Pour les autres membres des services, il est organisé une fois par an «*Les Cours du Club*» dont le but est d'harmoniser les procédures de formation et de promouvoir les contacts entre les *« middle-rank officers »*

Des groupes de travail sont régulièrement organisés. A l'occasion de ceux-ci des services qui n'appartiennent pas au *«Club»* peuvent également être admis. Cette admission se réalise au cas par cas moyennant une décision prise à l'unanimité.

La « Middle European Conference » (MEC)

La *«Mec»* est une association de fait entre les patrons des services civils de renseignement et de sécurité d'Europe de l'Ouest et d'Europe Centrale

Il convient de souligner que les deux associations (dont la Sûreté de l'Etat est membre ce qui n'est pas le cas du SGR) n'offrent sensu stricto aucune protection légale en ce qui concerne les informations échangées.

Cela ne veut pas dire cependant qu'il n'existe aucune règle. Dans la pratique, la classification de la partie qui donne les informations est strictement respectée et le service qui les reçoit leur confère le degré de classification correspondant[7].

[7] Un parallèle peut être fait avec l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité qui contient en annexe 1 une correspondance entre les degrés de classification en application de conventions ou de traités internationaux qui lient la Belgique, et le degré de classification belge.

2.1.3. L'échange d'informations

Dans son rapport 1997-1998, le Comité canadien de contrôle des services de renseignement utilise la formule suivante : *«Le Comité est conscient de l'importance de la politique du «donnant- donnant» ou de la contrepartie dans le milieu du renseignement*[8] *»*
Il est un fait reconnu que les services de renseignement opèrent dans le monde entier sur la base d'un système de troc consistant pour chaque service à obtenir des informations exclusives qui pourront par la suite être échangées avec d'autres services qui détiennent eux des informations inaccessibles au premier service.

Le principe de l'échange implique celui de la réciprocité.

Lorsqu'un pays avec lequel sont partagés des intérêts communs est menacé, il est évident que le partenaire, qui dispose des informations, a l'obligation de lui prêter assistance.

La *«règle du tiers»* constitue la règle de base de la collaboration entre services. Il s'agit là d'une des règles les plus anciennes et les plus strictes qui trouve son fondement dans une des préoccupations à la base de toute coopération entre service : *la protection des sources.*

L'article 5 §1 qui régit la procédure d'échange de renseignements au sein du *«Club»* formule cette règle de la manière suivante :

«Les renseignements qui sont échangés au sein du Club ne peuvent être adressés à une instance étrangère au Club, ni être utilisés à d'autres fins que celles contenues dans l'information sans l'accord formel du service qui en est à l'origine».

Il s'agit ici non seulement de la règle du tiers, mais également de la règle du service tiers. La préoccupation qui apparaît de la lecture de cet article du statut du *« Club »* a également été formalisée dans d'autres contextes dont certains ont force de loi.

Il faut ainsi mentionner les règlements de sécurité «C-M(55)15» de l'OTAN et «VR 100» de l'UEO qui prévoient explicitement qu'avant toute dissémination d'informations, l'accord préalable doit être donné par celui qui les a fournies.

On retrouve la même logique dans la Convention du 28 janvier 1981 du Conseil de l'Europe, relative à la protection de la vie privée dans laquelle il est stipulé qu'il est dangereux de fournir, par l'intermédiaire d'une autre partie, des informations liées aux personnes à un Etat qui n'est pas partie à la convention[9] .

2.2. Coopération en matière de contre- espionnage

Depuis la guerre froide et l'installation du quartier général de l'OTAN en Belgique (1967), il existait en matière de contre-espionnage une coopération entre les alliés qui était principalement dirigée contre le bloc communiste en général et les pays du pacte de Varsovie en particulier.

8 Rapport annuel du CSARS – 1997-1998, p.7
9 article 12 § 3 b.

Des informations ont ainsi été échangées entre les services de renseignement occidentaux concernant notamment le personnel des ambassades soviétiques (attachés commerciaux, attachés de presse) et celui de sociétés de transport aérien ou d'autres entreprises dans lesquelles aussi bien le KGB que le GRU plaçaient, dans le monde entier, leurs officiers de renseignement sous le couvert de fonctions spécialement réservées à cet effet.

Des données concernant ces personnes, ainsi que celles en rapport avec l'évolution de leur carrière internationale, étaient constamment mises à jour par tous les services de l'ouest et faisaient l'objet d'un échange mutuel.

Outre ce système permanent d'échange de données, il existait également une possibilité de demander des informations par le canal des officiers de liaison des différents services de renseignement occidentaux présents dans les ambassades, ainsi que par l'intermédiaire du «NOS» (Nato Office of Security).

2.3. Le KGB en Belgique

Le territoire belge, lieu d'établissement de toute une série d'institutions internationales (entre autres la CEE et l'OTAN), représentait une cible importante pour les services de renseignement de l'ex-URSS.

C'était la mission de quelques dizaines d'officiers appartenant aux services de renseignement et de sécurité de l'URSS, qui pouvaient aussi compter sur l'aide des autres services analogues des pays de l'Europe de l'Est.

Comme dans tous les pays où le KGB était actif dans le domaine de la collecte du renseignement, il existait aussi en Belgique ce que l'on appelait une *«résidence»* au sein de laquelle les représentants de ces services étaient organisés. Celle-ci était dirigée par le *«résident»* et son adjoint, et comprenait, à côté de spécialistes techniques (décodeurs, personnel de sécurité…), des officiers responsables du travail de renseignement qui étaient répartis en *«lignes».*

Les plus importantes de celles-ci étaient les lignes « P », « X », « KR » et « N ».

La ligne «P » composée d'officiers qui avaient pour tâche de collecter des informations politiques (en ce comprises des informations militaires et des informations économiques générales) était traditionnellement considérée comme la plus importante et la plus productive.

Pour pouvoir remplir leur mission avec efficacité, ces officiers devaient se tenir informés le mieux possible de la situation politique de leur pays de résidence par la consultation des sources ouvertes et leurs contacts avec des personnalités (ou des personnes) du monde politique. On les retrouvait le plus souvent dans le personnel diplomatique ou au sein des agences de presse. Pour la récolte d'informations plus confidentielles, ils essayaient de recruter des agents, principalement dans les milieux politique, journalistique et littéraire.

En dehors de la collecte de l'information, leur mission comportait également le recours à des méthodes appelées «mesures actives», comme celle de chercher à influencer l'opinion publique en faveur de l'URSS (ou en défaveur des opposants à l'URSS).

Dans ce cas, ils avaient recours soit à des écrivains ou à des journalistes qui au travers de livres ou d'articles, éventuellement moyennant rémunération, défendaient des positions préétablies par lesquelles le KGB tentait de manipuler l'opinion publique (le plus souvent et de manière subtile par des attaques contre l'alliance occidentale), soit en ayant recours à des agents d'influence qui induisaient des tendances déterminées dans la société ou à l'intérieur de certains groupes de pression.

La ligne «X» était l'interface au sein de la *« résidence »* du Directorat NT du KGB qui fut constitué en 1963, avec comme tâche principale la collecte d'informations dans les domaines de la technologie nucléaire, de la recherche scientifique, de l'espace, des sciences stratégiques, de la cybernétique et des procédés industriels.

Le Directorat NT se trouvait impliqué dans les opérations et la coordination des activités d'espionnage scientifique, technique et industriel menées dans tous les autres départements du KGB.

Il décidait quel scientifique soviétique recevrait l'autorisation de participer à des conférences internationales et il plaçait également des agents dans chaque groupe quittant le pays.

Depuis sa création, ce Directorat a connu une croissance continue. Au début des années 70, son quartier général comptait quelques centaines d'officiers et il était représenté dans les ambassades des pays importants. De surcroît, il disposait d'un grand nombre de spécialistes dans tous les domaines scientifiques.

Au milieu des années 70, les responsables soviétiques ont réalisé que leur économie était handicapée par des problèmes de transformation des matières premières en produits finis.

Ils essayèrent alors de convaincre des entrepreneurs de créer des entités en Union-Soviétique et de leur livrer leur «know-how» dans les domaines de la technologie et de l'organisation. Cela ne réduisait pas pour autant les efforts consentis pour obtenir par d'autres moyens des informations de nature scientifique et technologique.

Dans les années 80, ils donnèrent une priorité absolue à l'espionnage scientifique et technique en manifestant, dans ce contexte, un intérêt toujours croissant pour la technologie non spécifiquement militaire.

Il s'agissait d'un effort commun auquel tous les autres Etats du bloc de l'Est devaient participer.

Cet effort était spécialement dirigé vers la collecte d'informations dans les secteurs de la technologie, de l'électronique, des mathématiques, de la génétique, en fait dans tous les domaines qui étaient devenus plus ou moins inaccessibles pour les membres du pacte de Varsovie, depuis la création en 1949 dans le cadre de l'Otan, d'un *« Coordinating Committee for multilateral Export Controls »* (COCOM). Ce comité avait comme objectif d'empêcher ou, du moins, de ralentir l'accès de l'Union Soviétique et des Etats du bloc de l'Est à une industrie d'armement moderne.

Les efforts du KGB n'étaient toutefois pas limités au domaine purement militaire des applications de la recherche scientifique, mais visaient aussi toutes les applications industrielles.

Les officiers de renseignement qui travaillaient à l'étranger pour le Directorat NT appartenaient à la ligne X qui devenait graduellement la plus importante. En Belgique, cette ligne a compté entre 4 et 6 officiers, qui pouvaient compter sur l'appui des officiers des autres lignes. Ils appartenaient pour la plupart au personnel des ambassades.

Les fonctions d'attachés commerciaux soviétiques ainsi que les activités de certaines entreprises mixtes belgo-soviétiques constituaient d'excellentes couvertures et offraient des opportunités intéressantes pour entrer en relation avec les acteurs du monde économique et industriel.

Sans pouvoir entrer dans plus de détails, il faut mentionner que la Sûreté de l'Etat a permis d'intercepter certains de ces espions dans les années 80 à 90.

La troisième ligne importante des résidents du KGB était la ligne « KR » (contre-espionnage).

Les officiers de cette ligne n'étaient pas seulement responsables de la surveillance et de la protection des ambassades et de la «résidence», mais ils devaient aussi veiller à ce que la communauté soviétique ne soit pas infiltrée par les services de renseignement du pays d'accueil. A cette fin ils surveillaient étroitement tous les ressortissants soviétiques, ainsi d'ailleurs que leurs collègues des autres lignes, ce qui ne les rendait pas très populaires.

Leur mission comportait également la collecte d'informations concernant les services de police et de renseignement du pays d'accueil et éventuellement l'infiltration de ces services.

Puisqu'ils étaient considérés comme des spécialistes en matière de surveillance et de filatures, ils apportaient aussi régulièrement un appui opérationnel à leurs collègues des autres lignes.

La 4ème ligne importante de la résidence du KGB était la ligne « N », dépendante du «Directorat S».

A côté de la résidence officielle au sein de laquelle les officiers de renseignement oeuvraient et collectaient des informations via des informateurs ou par d'autres moyens, se trouvait dans la plupart des pays que le KGB considérait comme suffisamment important, ce que l'on appelait la *«résidence illégale».* Elle était composée d'agents qui vivaient sous une fausse identité et qui évitaient les contacts avec l'ambassade.

Il s'agissait de membres du KGB qui étaient spécialement formés en URSS et qui, nantis d'un passé personnel étoffé et soigneusement élaboré (*«la légende»*) ainsi que des papiers nécessaires, constituaient un réseau de renseignements.

Entre les deux guerres, ces réseaux illégaux étaient souvent plus importants que les légaux. Ceci résultait du fait que les possibilités d'avoir des représentants officiels étaient très limitées dans certains pays et que peu de fonctions de couvertures pouvaient être prévues pour des officiers du KGB. Après la deuxième guerre mondiale, les représentations soviétiques augmentèrent et l'on a pu offrir davantage de place à des résidents légaux de plus en plus nombreux.

Avant les années 80, on peut dire qu'il subsistait encore en Belgique quelques résidents illégaux dont le rôle consistait principalement à préparer un réseau clandestin de renseignements sur lequel le KGB aurait pu compter dans l'éventualité où, en cas de conflit, le personnel diplomatique aurait dû quitter le territoire.

Dans le cadre de la résidence légale, il y avait également encore quelques officiers du KGB qui représentaient le «Directorat S» et qui devaient offrir un support logistique aux officiers «illégaux».

A côté des lignes les plus importantes (P, X, KR, et N) on trouvait aussi, au sein de «*la résidence»,* la ligne «EM» (contrôle des émigrés), la ligne «SK» (contrôle de la communauté soviétique dans le pays d'accueil) et la ligne «I» (informatique).

Outre ses propres officiers, la résidence du KGB pouvait compter sur la collaboration d' «agents cooptés», c'est-à-dire de ressortissants soviétiques (du personnel d'ambassade, mais aussi des hommes d'affaires ou des scientifiques qui voyageaient régulièrement à l'Ouest) qui, sans appartenir au KGB, étaient cependant disposés à travailler pour ce service en étant davantage impliqués qu'un simple informateur.

Le KGB pouvait compter également sur les efforts des autres services de renseignement des membres du pacte de Varsovie (à l'exclusion de la Roumanie) sur lesquels il avait le contrôle.

Au total, on peut ainsi estimer que durant les années 80, il y avait en permanence une trentaine d'officiers de renseignement du KGB et une quinzaine d'officiers du GRU (renseignement militaire) actifs en Belgique.

En tenant compte du fait qu'ils étaient davantage suivis que les autres lignes et aussi que leurs activités pouvaient être mieux suivies, on peut estimer également que c'était surtout les lignes «P» et «X» qui étaient actives en matière de collecte du renseignement en utilisant des sources humaines.

2.4. Le contre-espionnage à la Sûreté de l'Etat.

L'organisation du contre-espionnage belge a débuté après les années de guerre et s'est développée durant les années les plus tendues de la guerre froide.

Depuis le déplacement du quartier général de l'Otan en Belgique en 1967, notre pays fut une cible désignée pour les services de renseignement des pays du bloc de l'Est contre lesquels l'Alliance était constituée.

A la demande des partenaires du Traité de l'Atlantique Nord, un effort considérable fut demandé aux services de renseignement belges, tant sur le plan du personnel engagé que sur celui de l'organisation des sections qui auraient à «contrer» les activités des services de renseignement des adversaires potentiels.

Il existait une bonne collaboration avec le ministère des Affaires étrangères et l'Office des étrangers, l'OTAN et la CEE. Un échange suivi d'informations fut instauré avec les correspondants des membres de l'Otan.

Jusqu'à la chute du Mur de Berlin en 1990, les efforts de la Sûreté de l'Etat en matière de contre-espionnage restèrent au même niveau. Ces efforts se sont concrétisés par l'interception régulière de diplomates du bloc de l'Est convaincus d'espionnage et qui furent dans la plupart des cas renvoyés. Au cours de la période allant de 1982 à 1986, 7 cas furent identifiés (dont 3 pour la seule année 1983).

En ce qui concerne la section qui s'occupait spécifiquement de l'URSS, 13 affaires au total furent traitées de 1967 à 1986, qui chaque fois conduisirent à faire déclarer des diplomates soviétiques *«persona non grata»* .

A la fin des années 80, cette section fut progressivement démantelée parce que de nouvelles matières (l'extrémisme idéologique, le terrorisme, la prolifération) absorbaient de plus en plus d'énergie et demandaient davantage de potentiel humain.

Nonobstant cette situation, il fut encore possible, en 1990, grâce aux renseignements recueillis, de mettre un terme provisoire aux activités de la ligne P dans notre pays.

Plusieurs personnes furent interpellées par la Sûreté de l'Etat. Une de celles-ci fut poursuivie judiciairement.

Après 1990, et compte tenu du changement de la situation internationale, le démantèlement de la section fut poursuivi.

En 1992, la révélation des noms des agents actifs dans la ligne X a également permis de la neutraliser pendant quelque temps (opération «Glasnost»).

Bien que cette affaire ait donné lieu à des perquisitions et à des mises en détention préventive, aucun des intervenants ne fut poursuivi devant les tribunaux.

Il fut établi que des entreprises avaient fourni, dans le passé, des fonctions de couvertures pour des officiers du KGB (principalement ceux de la ligne «X»). Il est apparu également que certaines d'entre elles avaient des liens avec la maffia russe. Une nouvelle section de la Sûreté de l'Etat s'occupe aujourd'hui des organisations criminelles et de l'Europe centrale et orientale.

Il ressort d'entretiens que le Service d'enquêtes du Comité R a eus avec des membres de la Sûreté de l'Etat, ainsi que de déclarations de l'administrateur général de la Sûreté de l'Etat à la presse en octobre 1999, qu'en ce qui concerne la Russie, un effort allait être fait au niveau des entreprises mixtes principalement dans le cadre de la lutte contre la mafia russe.

Suite aux échos donnés par la presse belge à l'affaire «Mitrokhin», la Sûreté de l'Etat a fait savoir que la priorité serait à nouveau donnée à la lutte contre les activités du SVR[10], principalement dans le cadre de la mission légale de la protection du potentiel économique et scientifique du pays. Le quotidien *«La Dernière Heure»* du 16 septembre 1999, rapporte ainsi les propos de la porte-parole de la Sûreté de l'Etat : *« Avec la chute du mur de Berlin, on imaginait que l'espionnage allait diminuer. Cela a été le cas durant quelques années, mais les faits ont manifestement repris… La Sûreté avait progressivement diminué les enquêtes de contre-espionnage au profit de la lutte contre le terrorisme et le crime organisé, qui sont devenus les premières priorités. Aujourd'hui on constate qu'il faut faire marche arrière et remettre l'accent sur le contre-espionnage. »*

[10] Un des services de renseignement russe qui a repris dans ce domaine les activités de l'ex-KGB.

3. LES RESULTATS DE L'ENQUETE

3.1. Les réponses au questionnaire

Le Comité R se doit de signaler qu'il constate que les réponses quasi-identiques fournies par les deux services aux questions dont l'énoncé est repris au point 1.2. ci-avant ont été classifiées «confidentiel» par le SGR et n'ont fait l'objet d'aucune classification par la Sûreté de l'Etat.

Un courrier a été adressé au chef du SGR en date du 8 mars 2001 lui demandant si cette classification était maintenue ou si elle pouvait être levée en tout ou en partie, afin de permettre au Comité R de faire rapport, comme la loi le prévoit à sa Commission de suivi ainsi qu'aux ministres concernés.

Au moment d'approuver le présent rapport aucune réponse définitive n'est encore parvenue au Comité R.

Celui-ci n'est donc pas en mesure actuellement, compte tenu des dispositions de la loi sur la classification et les habilitations de sécurité du 11 décembre 1998 de reproduire le contenu de ces réponses à destination de personnes ne disposant pas d'une habilitation de sécurité du niveau requis.

3.2 Les constatations et les commentaires du Comité R

3.2.1. Le retard dans la transmission des informations à la Sûreté de l'Etat et au SGR

On peut lire en substance dans l'ouvrage du professeur Christopher Andrew et de Vasili Mitrokhin[11] que ce dernier *était arrivé en Angleterre le 7 septembre 1992. En août 1993 un auteur américain faisait déjà mention de l'affaire dans un livre intitulé « Federal Bureau of Investigation (FBI) » . Il mentionnait le fait que les informations transmises par un ancien collaborateur du KGB concernant des centaines d'américains étaient tellement spécifiques que dès l'été 1993 dans la plupart des grandes villes américaines des agents du FBI avaient été mobilisés pour enquêter sur ces faits.*

Le quotidien américain «The Washington Post» avait obtenu confirmation de ce récit par un informateur anonyme des services de renseignement nationaux et le périodique «Time» avait pour sa part identifié le transfuge du KGB comme étant un ex-collaborateur du Premier Directorat Général.

En octobre 1996, le journal français «Le Monde» révélait que les services de renseignement britanniques avaient transmis à la DST une liste d'environ 300 noms de diplomates et de fonctionnaires qui auraient travaillé pour les services de renseignement soviétiques.

[11] The Mitrokhin Archive pp. 19 et 20

En décembre de la même année, des informations similaires paraissaient dans la presse Allemande. Dans celles-ci, on situait la transmission de données par les britanniques au service de renseignement allemand, le BfV «Bundesamt für Verfassungsschutz».

En juillet 1997, le récit de Mitrokhin paraissait à son tour dans la presse autrichienne et cette fois-ci en relation avec l'existence de caches d'explosifs.

En juillet 1998, le magazine allemand «Focus» publiait l'histoire de l'ex-colonel russe qui en 1992 passait à l'Ouest tout en transmettant aux services de renseignement britanniques des informations manuscrites.

Selon la réponse de la Sûreté de l'Etat, ce service ne fut informé que le 11 juillet 1995 de l'existence d'un transfuge *«qui plus tard a été identifié comme étant Mitrokhin.»*

Cette information intervient donc plus de deux ans après que les Américains (et selon le journal «le Monde», les Français) furent mis au courant et après qu'un livre paru en août 1993 aux Etats-Unis en ait fait mention.

Si le contexte intégral de l'affaire était déjà connu de la Sûreté de l'Etat dès 1996, l'identité de Mitrokhin ne serait arrivée à la connaissance de ce service que par la presse belge dans laquelle les premiers articles ne sont apparus qu'en 1999, à la suite de la découverte des caches contenant des appareils émetteurs récepteurs.

Durant l'entretien que les membres du Service d'enquêtes ont eu avec le responsable désigné du service d'étude de la Sûreté de l'Etat, il est apparu que celui-ci n'était pas au courant des échos que cette affaire avait eus dans la presse des autres pays dès 1993 et dans la presse internationale à partir de 1996.

On peut déduire de ce qui précède que la Sûreté de l'Etat a été informée avec retard et d'une manière apparemment sommaire de l'existence d'un transfuge du KGB.

Au-delà des raisons qui pourraient être à la base d'une telle situation et sans avoir à ce jour connaissance du contenu des informations communiquées et donc de leur plus ou moins grand degré d'intérêt[12], force est de constater pour le Comité R que les membres du service contre-espionnage de la Sûreté de l'Etat semblent avoir montré un intérêt fort limité pour cette affaire, dans l'hypothèse où il a fallu attendre l'intervention des médias belges pour qu'ils soient mis au courant du contexte précis de celle-ci.

Il est apparu des contacts du Service d'enquêtes du Comité R avec le responsable désigné au SGR pour suivre cette enquête, qu'à une exception près, le retard dans la transmission d'informations intéressantes sur le plan militaire n'avait pas eu de conséquences négatives en pratique.

Il faut souligner que la Sûreté de l'Etat et le SGR ont été en mesure de faire le point sur cette situation dans le cadre de l'exécution du protocole d'accord qui les lie depuis 1997. Ils ont ainsi pu confronter et mettre à jour les informations partielles et différentes qu'ils avaient réciproquement reçues.

---

12 D'après une première évaluation par la Sûreté de l'Etat d'une demande du Comité R d'avoir accès au contenu de ces informations, il ressort que la « règle du tiers » s'appliquerait également à l'égard des membres du Comité R et de son Service d'enquêtes, malgré la possession par ceux-ci d'une habilitation de sécurité du niveau « très secret » Le Comité aurait également dans ce contexte à justifier de son « Need to Know »

3.2.2. Le contenu, la valeur et l'exploitation des informations

Il ressort des réponses apportées par les deux services de renseignement nationaux que les informations transmises ne concernaient pas uniquement l'affaire des caches de matériel de transmission révélée dans notre pays par les médias en 1999.

Il convient de constater qu'en application stricte de la règle du service tiers, seules les informations qualifiées de pertinentes par le SGR concernant les caches d'appareils de communications ont pu être communiquées aux autorités judiciaires[13] après avoir reçu l'accord préalable du service qui avait fourni les informations. Le SGR et la Sûreté de l'Etat n'ont eux-mêmes pu échanger les informations qu'ils avaient respectivement reçues du même service tiers qu'après avoir obtenu le même type d'autorisation préalable.

Aucune des autres informations, pour lesquelles, vu leur ancienneté (antérieures à 1985), l'intérêt est qualifié *d'historique*[14] par le SGR et la Sûreté de l'Etat, n'a été, ni n'est encore exploitée actuellement. Celles-ci n'ont pas davantage fait l'objet de communication à des destinataires belges ou étrangers, autres que les services de renseignement concernés par la présente affaire.

Il convient toutefois de noter que des enquêtes ont été faites par la Sûreté de l'Etat dans quelques cas et que les résultats en ont été communiqués à un service de renseignement allié.

4. CONCLUSIONS ET RECOMMANDATIONS

Sous différents aspects, c'est *la complexité de la problématique de l'échange des informations au sein de la communauté nationale et internationale du renseignement*, ainsi que la communication des données soit sous une forme brute, soit après analyse à d'autres autorités et à d'autres pouvoirs (notamment le pouvoir judiciaire et le pouvoir politique) qui est en premier lieu mise en évidence par la présente enquête.[15]

---

13 Il fallait en effet tenir compte de la présence éventuelle d'explosifs présentant un danger pour la sécurité publique

14 A ce sujet , le Comité R souligne que dans cette hypothèse les dispositions de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité trouveraient éventuellement à s'appliquer. Cet article dispose que : « Les données à caractère personnel traitées dans le cadre de l'application de la présente loi sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées, **à l'exception de celles présentant un caractère historique, reconnu par les archives de l'Etat**. .. »
Voir également à ce sujet les rapports annuels du Comité R de 1996, p. 97 – 1997, p.11 et 1999, p. 97 concernant la destruction des archives par nos services de renseignements

15 Le problème n'est semble-t-il pas propre à la Belgique, puisque d'après le journal «*Le Monde*» du 15 septembre 1999 se penchant sur l'affaire Mitrokhin :«*l'opposition conservatrice au Royaume-Uni a demandé pourquoi les services de contre-espionnage n'ont pas cru devoir informer les deux gouvernements de ce cas très particulier et pourquoi le Parlement n'est-il informé qu'après les révélations publiques d'un professeur de Cambridge ».* Parlant d'informations non communiquées par les services de renseignement britanniques aux autorités politiques dans ce contexte, le même article mentionne encore :*« Dans l'affaire Norwood, le MI 5 (service de contre-espionnage britannique) a-t-il abusé de ses droits ? Doit-il les conserver sans un contrôle plus étroit de ses activités par les élus ? C'est tout l'enjeu du débat qui vient de s'ouvrir et c'est pourquoi la commission parlementaire en charge de la surveillance des services de*

Celle-ci montre que l'application de *«la règle du tiers ou du service tiers»* qui fonde la collaboration internationale entre les services de renseignement interdit, que sans autorisation préalable du service qui a donné les informations, celles-ci soient *communiquées* aux autorités politiques et judiciaires nationales du pays qui les reçoit [16].

Dans le cas d'espèce, on justifiera sans doute cette situation par le fait que ces informations n'étaient plus d'actualité (antérieures à 1985), que d'éventuelles infractions – pour autant qu'elles eussent pu être prouvées – étaient prescrites, qu'elles n'avaient donc qu'un intérêt historique et qu'il n'y a donc eu en pratique aucun inconvénient à agir de la sorte. Mais pourquoi l'embargo sur ces informations se justifie-t-il encore aussi longtemps après ?
Compte tenu de l'importance de la règle précitée, peut-on être assuré qu'il en serait autrement dans le cas d'informations présentant un plus grand intérêt actuel ?

Il est indéniable d'autre part que la collaboration avec les services de renseignement internationaux est indispensable pour contribuer à assurer l'efficacité avec laquelle la Sûreté de l'Etat et le SGR doivent remplir leurs missions légales et que «la règle du tiers» qui n'est qu'un exemple de la protection à accorder aux sources d'informations, constitue dans ce domaine un principe incontournable.

Il convient toutefois de tenir compte des dispositions légales nationales qui consacrent aujourd'hui le principe de la communication des données par les services de renseignement et de sécurité à d'autres services et autorités, celui de la protection de ces données par la voie de la classification, ainsi que le principe de la coopération entre les services.

C'est ainsi que la loi du 30 novembre 1998 organique des services de renseignement et de sécurité prévoit en son article 19 alinéa 1er que : *«Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes, conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11 ».*

Le principe de la coopération entre les services, aussi bien au niveau national qu'international, est prévu quant à lui par l'article 20 §1er de la même loi : *« Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une collaboration avec les services de renseignement et de sécurité étrangers.»*

Le § 3 de l'article 20 précité édicte que : «*Le Comité ministériel du renseignement définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article.»*

---

renseignements vient de se voir confier mission d'enquêter plus à fond sur tous les mystères de cette guerre froide qui revient hanter la Grande-Bretagne de l'an 2000. »

16 Il est intéressant de noter que la règle du service « tiers » trouve une application explicite dans le libellé du 2ème alinéa de l'article 5 § 3 de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité :
« *A la demande du service de renseignement et de sécurité, l'organe de recours peut décider que certaines informations figurant dans la déposition d'un membre du service de renseignement visé au § 2, dans le rapport d'enquête ou dans le dossier d'enquête sont secrètes pour un des motifs visés au § 2, alinéa 4, et qu'elles ne pourront être consultées ni par le requérant ni par son avocat.*
Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité ».

En ce qui concerne la protection des informations, la loi relative à la classification édicte en son article 8 l'interdiction *«à l'accès aux informations, documents ou données, au matériel, aux matériaux ou matières classifiées*» à la personne qui *«n'est pas titulaire d'une habilitation de sécurité correspondante»* et qui *« n'a pas besoin d'en connaître et d'y avoir accès pour l'exercice de sa fonction ou de sa mission, sans préjudice des compétences propres des autorités judiciaires.»*

Le Comité R estime que ces nouvelles dispositions sont de nature à apporter dans la pratique des solutions à une plus grande et sans doute à une meilleure communication entre les services de renseignement et les autres services et autorités nationales, pour autant que les destinataires naturels d'informations classifiées prennent, si nécessaire, les mesures appropriées pour répondre aux exigences de la loi, et puissent ainsi avoir accès à ces données pour prendre les décisions propres à leur domaine de compétence et de souveraineté tout en continuant, s'il échet, à assurer la protection de ces données. Le principe de la communication des données consacré par le législateur n'implique pas en effet automatiquement l'usage en l'état de celles-ci (par exemple dans une procédure judiciaire) ou leur diffusion publique.

Dans cette optique, et dans le cadre des principes dégagés par le législateur qui viennent d'être rappelés, le Comité R se demande si, au vu d'une pratique telle qu'elle apparaît de la présente enquête et du contexte général décrit ci-dessus au point 2.1.3., une réflexion, tant sur le plan national que peut être aussi sur le plan européen et international, ne devrait pas être mise en œuvre, concernant notamment l'application de *«la règle du tiers»* et de son contrôle, dans la mesure où cette application pourrait, à certains égards, être susceptible d'une mauvaise interprétation liée à une certaine culture du secret ou même, dans des cas extrêmes, d'un mauvais usage.

Si comparaison n'est pas raison, le Comité R ne peut rester sans rappeler l'expérience malheureuse récente de certaines affaires judiciaires qui a mis en évidence l'importance d'une bonne gestion des informations comprenant e.a. une communication optimale et en temps utile des données. Faut-il rappeler les conséquences dommageables et parfois dramatiques qui peuvent résulter de dysfonctionnements dans ce secteur ?

Le second point que le Comité R retient de la présente enquête est qu'il y a eu de l'aveu même des responsables de la Sûreté de l'Etat (voir point 2.4 ci-dessus page 84 in fine) une évaluation à la baisse de l'évolution des activités d'espionnage qui a entraîné une diminution des moyens consacrés au contre-espionnage. Cette évaluation a été finalement démentie dans les faits.

Pour souligner l'importance de ce constat, rappelons que l'ancien administrateur de la Sûreté de l'Etat déclarait le 9 octobre 1999 au *«Financieel Economische Tijd»* que : *«La Sûreté de l'Etat disposait d'indices selon lesquels au cours des années précédentes des services de renseignement étrangers se livraient en Belgique à de l'espionnage économique et industriel.*» Il ajoutait même : *«Concernant cette guerre économique, appelée également la guerre oubliée, tout le monde se tait. Durant les six années passées à la tête de la Sûreté de l'Etat, jamais aucune puissance étrangère n'a proposé d'organiser à ce sujet une réunion de travail. »* Il ajoutait concernant ce domaine particulier: *«Dans l'Europe de l'an 2000 les intérêts nationaux continuent à jouer un rôle important et l'on ne doit pas s'attendre à ce que cela change dans les années à venir.. »* [17]

[17] Traduction libre

Dans un article paru dans le journal français «Le Monde» du 8 mars 2001, Jacques Isnard rappelle que : *«La fin de la guerre froide Est-Ouest n'a pas mis un terme aux activités des espions de tout poil sur la planète… Après 1989 et la chute du mur de Berlin, l'espionnage s'est – très momentanément – ralenti. L'implosion de l'ex-URSS, à partir de 1991, et l'attrait des pays de l'ancien «bloc» de l'Est pour l'Otan ont relancé la machine comme en témoignent les affaires en cours qui ont la Russie et les Etats-Unis pour théâtres.»*
Le même auteur résume encore ainsi la situation actuelle : *«Tous Etats confondus, les services partent aujourd'hui en quête d'informations qui relèvent moins du militaire, voire de l'opérationnel que du politique, de la finance internationale, du commerce, de l'industrie et, surtout, de la haute technologie. Il s'agit d'assurer, de façon clandestine, par le vol de documents, l'interception des communications ou, par la corruption, des gains technologiques, à des fins civiles et stratégiques, au moindre prix, c'est-à-dire sans devoir débourser des sommes excessives dans l'ordre des études de la recherche ou d'une technique dits de «pointe». L'idéologie n'est plus guère un motif d'espionner, comme du temps de la guerre froide. On espionne pour économiser du temps et de l'argent, en s'appropriant des découvertes des pays censés être les plus avancés.* »

Le Comité R recommande qu'en cette matière particulièrement les moyens nécessaires soient donnés à la Sûreté de l'Etat pour lui permettre d'assurer un maximum d'efficacité dans le cadre d'une mission qui lui est spécifique : le contre-espionnage en matière économique et industrielle. Cette recommandation est appuyée par la constatation qu'apparemment, si l'on se base sur les propos de l'ancien administrateur-général de la Sûreté de l'Etat, ainsi que sur l'analyse citée ci-dessus, en matière de défense du potentiel économique les services nationaux ne peuvent pas compter, comme cela semble être le cas dans les autres domaines (terrorisme, prolifération, etc..), sur un échange d'informations avec les autres services étrangers, même si ce sont d'autre part des services alliés, européens ou non.

Le troisième et dernier point que le Comité R tient à mettre en évidence au vu des constatations de la présente enquête est celui de l'importance des sources ouvertes. Une bonne exploitation de celles-ci par la Sûreté de l'Etat n'apparaît pas des constatations faites par le Service d'enquêtes du Comité R. Celui-ci rappelle ce qu'il mentionnait déjà dans son rapport d'activités de 1996 lorsqu'il rapportait les conclusions d'un congrès organisé à Bruxelles sur les sources ouvertes : *A l'heure où la guerre froide a pris fin, les services se voient confrontés à de nouvelles priorités, tel que le problème délicat de l'espionnage économique.* Concernant à ce sujet le fonctionnement des services de renseignement le Comité R notait : *«De plus en plus d'informations sont publiquement disponibles, et en conséquence la tendance à classifier des documents «secrets» par exemple, est dépourvue de sens. Nombreux, sont ceux qui, parmi les participants à ce congrès, prônent la déclassification d'informations et une plus grande transparence du fonctionnement des services de renseignement. Le meilleur moyen pour garder l'avantage sur son adversaire est de réagir vite, car seule l'information faisant l'objet d'une analyse et d'un traitement est utile.»*

CHAPITRE 3 : RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LE SGR A GÉRÉ L'INFORMATION SUR LA SITUATION MILITAIRE AU KOSOVO

1. INTRODUCTION

Le journal «De Morgen» du 22 octobre 1999 (*« België beducht voor Servische invasie in Kosovo »* a fait état d'une communication du ministre de la Défense nationale, André Flahaut, au Conseil des ministres du 24 septembre 1999. Selon l'article, le ministre possédait des informations du commandement de la KFOR qui n'excluaient pas une prochaine invasion du Kosovo par l'armée et la police serbes. En conséquence de quoi, il avait demandé de mettre en place un « *worst case scenario »* à l'intention des 1.100 soldats belges en mission dans cette région. Toujours selon De Morgen, le porte-parole des forces belges au Kosovo ne semblait toutefois pas prendre cette information au sérieux.

Par ailleurs, une succession de communiqués contradictoires dans la presse posait la question de savoir si l'OTAN, le ministre de la Défense nationale et le commandement des troupes belges au Kosovo disposaient des mêmes informations sur la situation militaire dans cette région.

Dans le cadre de sa mission de contrôle portant sur la coordination et l'efficacité des services de renseignement, le Comité permanent R s'est demandé comment le SGR gérait l'information sur la situation militaire au Kosovo et comment il collaborait avec la Sûreté de l'Etat sur ce sujet.

2. PROCÉDURE

Le Comité permanent R a donc décidé le lundi 8 novembre 1999 d'ouvrir une enquête sur la manière dont le SGR avait géré l'information sur la situation militaire au KOSOVO.

Le 10 novembre 1999, le président du Comité R a adressé une apostille au chef du Service d'enquêtes.

Le président du Sénat a été informé de l'ouverture de cette enquête le 18 novembre 1999 conformément à l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le ministre de la Défense nationale a été informé de l'ouverture de cette enquête le 24 novembre 1999 conformément à l'article 43.1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le Service d'enquêtes du Comité permanent R a procédé à des auditions au SGR dans le courant du mois de février 2000. Il a remis son rapport au Comité le 27 mars 2000.

Le 29 mai 2000, le Comité permanent R a adressé une nouvelle apostille au Service d'enquêtes pour lui demander de vérifier auprès de la Sûreté de l'Etat comment ce service avait collaboré avec le SGR dans le cadre de la problématique du Kosovo.

Le 30 mai 2000, conformément à l'article 43.1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le ministre de la Justice a été informé que l'enquête était étendue à la Sûreté de l'Etat.

Le Service d'enquêtes du Comité permanent R a procédé à des auditions à la Sûreté de l'Etat dans le courant du mois de juin 2000. Il a remis son rapport au Comité le 26 juin 2000.

Le présent rapport a été approuvé le 26 septembre 2000.

Par lettre du 11 janvier 2001, le ministre de la Défense nationale a fait savoir au Comité R que le présent rapport pouvait figurer tel quel dans le rapport annuel.

3. CONSTATATIONS ET CONCLUSIONS

La nature particulièrement secrète des opérations de renseignements en rapport avec la mission de la KFOR au Kosovo ne permet pas au Comité permanent R de rendre publique la moindre information opérationnelle à ce sujet.

Il ressort des constatations du Service d'enquêtes que, pendant la période couverte par la présente enquête, le SGR a été en mesure, avec l'aide de services alliés, d'évaluer concrètement le risque d'invasion du Kosovo par l'armée yougoslave. Bien que considéré comme faible, le risque a été pris en compte. L'évaluation de la situation était permanente et le SGR est resté attentif à tout élément de nature à anticiper ce risque, de manière à permettre aux forces armées belges et aux alliés de réagir en temps utile.

La circulation d'informations sur ce sujet a été fournie et constante entre la Sûreté de l'Etat et le SGR. Des réunions communes d'analyse des risques ont été organisées entre ces deux services conformément à ce qui est prévu dans leur protocole d'accord.

Des notes d'informations ont été régulièrement adressées aux responsables politiques du Royaume afin de leur permettre d'assumer leurs responsabilités en pleine connaissance de cause.

CHAPITRE 4 : RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LE SGR A GÉRÉ L'INFORMATION SUR LA SITUATION GÉNÉRALE AU KOSOVO

1. INTRODUCTION

Le Comité R a pris connaissance d'un article paru dans le journal « Le Soir » du vendredi 12 novembre 1999 intitulé « *Au Kosovo, les belges surveillent sans punir ».* Un passage de cet article relatant les déclarations d'un officier de renseignement « *alias James Bond »* a particulièrement retenu l'attention du Comité : « *Chargé du renseignement, le militaire surveille de loin les criminels en tout genre qui, la plupart du temps, se baladent en grosses limousines allemandes. Le capitaine échange des informations avec ses équivalents français, danois et autres. « Nous avons une image précise de la situation », assure-t-il ».*

Suite à cet article, le Comité R s'est posé quelques questions sur la manière dont le SGR avait géré l'information sur la situation générale au Kosovo. Le Comité R s'est demandé si l'officier cité dans l'article faisait bien partie du SGR ou s'il collaborait avec ce service dans le cadre d'une mission de renseignement au sein de l'opération Belkos 1.

Le Comité R s'est aussi interrogé sur les rapports qui peuvent exister entre des membres du SGR en mission et des journalistes.

- Est-il d'usage qu'un officier chargé d'une mission de renseignement puisse être approché par un journaliste, voir son identité révélée ainsi que l'objet de sa mission et les contacts qu'il entretient avec *ses équivalents* étrangers ?

- Si oui, est-ce conforme aux règles de sécurité des forces armées, aux ordres permanents du SGR ou aux instructions particulières délivrées dans le cadre de l'opération Belkos 1 ?

Si non :
- une infraction a-t-elle donc été commise à l'encontre d'une de ces règles ?
- un préjudice a-t-il été causé au bon déroulement de la mission ? Peut-on en évaluer les conséquences ?
- des mesures ont-elles été prises pour remédier à l'incident et parer à ses éventuelles conséquences dommageables ?

2. PROCÉDURE

Le Comité R a décidé le 2 décembre 1999 d'ouvrir une enquête sur la manière dont le SGR avait géré l'information sur la situation générale au Kosovo.

Le président du Sénat a été informé de l'ouverture de cette enquête le 15 décembre 1999 conformément à l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le 16 décembre 1999, le président du Comité R a adressé une apostille au chef du Service d'enquêtes.

Le ministre de la Défense nationale a été informé de l'ouverture de cette enquête le 17 décembre 1999 conformément à l'article 43.1 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le Service d'enquêtes du Comité R a procédé à des auditions au SGR dans le courant du mois de février 2000. Il a remis son rapport au Comité R le 27 mars 2000.

Il ressort de ce rapport que l'officier cité par l'article de presse n'appartient pas au SGR : il était l'officier S2 (l'officier de renseignement) du bataillon belge au Kosovo (Belkos).

L'article 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements circonscrit la mission de contrôle du Comité R à la Sûreté de l'Etat et au Service général du renseignement et de la sécurité des Forces armées.

Le Comité R n'a donc aucune compétence *rationae materiae* pour enquêter sur les contacts que l'officier S2 précité a entretenu avec la presse bien que celui-ci ait étroitement collaboré avec le SGR.

Le Comité R a donc décidé de limiter ses constatations aux règles générales applicables en la matière et au point de vue du SGR sur les répercussions éventuelles de l'article précité en matière de sécurité de la mission belge au Kosovo.

Le présent rapport a été approuvé par le Comité R le 24 octobre 2000.

Le Comité R a tenu compte d'une précision apportée par le ministre de la Défense nationale dans un courrier du 7 décembre 2000. Par ce même courrier, le ministre a fait savoir au Comité que le présent rapport pouvait figurer tel quel dans son rapport annuel.

3. CONSTATATIONS

La diffusion d'informations par l'armée et les relations des militaires avec la presse font l'objet des ordres généraux J/813 et J/108. L'instruction IF5 sur la sécurité militaire contient également des instructions à ce sujet.

D’une manière générale, les relations des militaires avec la presse étaient jusqu’il y a peu soumises à autorisation préalable.

L’ordre général J/108 F du 9 août 1994 reconnaît cependant que chaque militaire, quel que soit son grade, dispose de la liberté d’exprimer ses opinions de la manière qu’il estime la plus appropriée, comme tout citoyen belge. Il a donc le droit de s’exprimer, en son propre nom, dans la presse sans autorisation préalable.

Il est cependant interdit aux militaires de révéler des informations classifiées à des personnes non habilitées et de faire des déclarations qui nuisent à la sécurité du pays, qui perturbent l’ordre public ou qui mettent en péril la prévention de faits délictueux. Ils ne peuvent également pas mettre l’honneur et la dignité des institutions de l’Etat ou celles des Forces armées en danger.

Dans ces limites, un officier de renseignement a lui aussi le droit de faire des déclarations à titre personnel à la presse.

L’information officielle des Forces armées n’est délivrée que par des porte-parole désignés par les autorités militaires.

Nonobstant la disposition de l’article 19 de la loi du 30 novembre 1998 organique des services de renseignements qui prévoit que le chef du SGR peut désigner une personne qui peut communiquer des informations à la presse, il a été convenu que, dans la pratique, seul le porte-parole du ministre de la Défense nationale peut délivrer une information officielle à la presse en ce qui concerne le SGR

Du point de vue du SGR, aucune infraction n’a été commise à l’encontre d’une des règles précitées et les propos attribués à un officier de renseignement par le journal « Le Soir » du vendredi 12 novembre 1999 n’ont pas compromis la sécurité de la mission des Forces armées belges au Kosovo.

CHAPITRE 5 : RAPPORT DE L'ENQUETE MENEE SUR LE ROLE DU SGR DANS L'OCTROI DES AUTORISATIONS DE PRISES DE VUES AERIENNES (ET DE SUJETS MILITAIRES)

1. INTRODUCTION

En droit interne belge, il est défendu de prendre des photographies d'installations militaires sans l'autorisation de l'autorité militaire (article 120 ter du code pénal [1]). C'est toujours un arrêté ministériel du 28 février 1940 qui détermine les conditions dans lesquelles peuvent être accordées les autorisations de prendre ou de publier des photographies de sujets militaires.

Toute prise de vue aérienne au-dessus du territoire national (quel que soit l'endroit photographié) ainsi que «*le transport d'appareils photographiques à bord d'aéronefs* » sont encore soumis à une autorisation spéciale du ministre chargé de l'administration de l'aéronautique, avec l'accord préalable du ministre de la Défense nationale (arrêté royal du 21 février 1939). La publication de photographies aériennes est également soumise à l'accord préalable du ministère de la Défense nationale. L'arrêté royal de 1939 fixe aussi la procédure à suivre en vue d'obtenir lesdites autorisations. Les infractions à ces dispositions sont passibles de sanctions pénales.

Ces régimes d'autorisation préalable, mis en place à une époque où des préparatifs de guerre étaient à l'ordre du jour, sont encore en vigueur de nos jours. Les demandes d'autorisation de photographies, qu'elles soient aériennes ou au sol, doivent toujours, en principe, être soumises à l'examen préalable du SGR.

La situation a pourtant bien changé depuis cette époque. L'apparition des satellites d'observation de la terre d'une part, la fin de la guerre froide et la signature du traité d'Helsinki du 24 mars 1992 sur le régime «ciel ouvert » d'autre part, ont bouleversé les moyens technologiques de prise de vue, de même que l'environnement juridique international. Cette situation nouvelle ne justifie-t-elle pas que soit réexaminée la pertinence des dispositions prises en 1939, notamment à l'égard de la photographie aérienne au dessus du territoire national ?

---

[1] *« Sera puni d'un emprisonnement de huit jours à un an et d'une amende de 26 à 100 francs :*
1° quiconque, sans l'autorisation de l'autorité militaire, maritime ou aéronautique, aura exécuté par un procédé quelconque des levés ou opérations de topographie dans un rayon d'un myriamètre ou dans tout autre rayon qui sera ultérieurement fixé par le ministre de la Défense nationale, autour d'une place forte, d'un ouvrage de défense, d'un poste d'un établissement aéronautique autre qu'un aérodrome ou aérogare, d'un dépôt, magasin ou parc militaires, à partir des ouvrages avancés, ou aura pris des photographies d'un de ces lieux, ouvrages ou établissements, édité, exposé, vendu ou distribué des reproductions de ces vues ;
2° (…) ».

Quelle est donc encore la raison d'être du contrôle des photographies de sujets militaires (aériennes ou au sol) par le SGR ? Ce contrôle est-il encore possible et utile ? Combien de demandes d'autorisations le SGR doit-il traiter chaque année ? Comment procède-t-il pour instruire ces demandes ? Quel rôle joue le SGR dans l'application des mesures d'inspection prévues par le traité « ciel ouvert » ? Telles sont quelques unes des questions que le Comité R s'est posé sur cette matière.

2 . PROCEDURE

Le Comité « R » a décidé d'ouvrir cette enquête le 2 décembre 1999.

Par apostille du 3 décembre 1999, le président du Comité R a chargé le Service d'enquêtes de poser les questions reprises en introduction au SGR.

Le 3 décembre 1999, le président du Sénat a été averti de l'ouverture de cette enquête.

Par lettre du 6 décembre 1999, conformément à l'article 43-1° de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le chef du Service d'enquêtes a averti le ministre de la Défense nationale de l'ouverture de cette enquête.

Le Service d'enquêtes du Comité R a procédé à diverses vérifications entre le 1er février 2000 et le 26 juin 2000, date à laquelle il a déposé son rapport au Comité R.

Le Comité R a procédé à divers échanges de courriers avec :

- le Directeur général de l'Administration de l'Aéronautique
- le Chef du SGR.

Le présent rapport a été approuvé par le Comité R le 23 janvier 2001.

Le rapport a été transmis au ministre de la Défense nationale le 2 février 2001.

3. L'INTERET PARLEMENTAIRE

Le 16 septembre 1999, M. Yves Leterme, député CVP a posé deux questions parlementaires, l'une au Vice-premier ministre et ministre de la Mobilité et des transports, l'autre au ministre de la Défense nationale. Ces question concernent l'application de la « *réglementation relative à la prise de vues aériennes et au transport d'appareils photographiques à bord d'aéronefs ».*

Le député demande aux ministres si l'arrêté royal du 21 février 1939 est encore d'application à l'heure actuelle et sur quels motifs repose encore son application.

Réponse du ministre de la Défense nationale :

1. *« Cet arrêté royal* (du 21 février 1939) *n'est pas abrogé et est donc toujours d'application. La procédure pour l'octroi d'une telle autorisation est cependant fortement allégée*

2. *Le but de la conservation de cet arrêté royal est de disposer d'un outil en cas de crise en particulier dans la lutte contre le terrorisme.*

3. *a) les demandes annuelles introduites auprès de l'administration de l'Aéronautique sont de l'ordre de 500 (1999).*

   b) en temps normal, il n'est actuellement plus exigé un accord préalable du ministère de la défense nationale.

4. *Etant donné qu'actuellement aucun objectif militaire n'est interdit de publication de photo aérienne, l'article 6[2] n'est pas appliqué.*

4. LA COMMERCIALISATION DES IMAGES SATELLITAIRES AU NIVEAU INTERNATIONAL

Plus de quarante ans après le lancement du premier satellite « *Spoutnik* » en 1957, l'exploitation de l'espace est devenue un enjeu de première importance pour la communauté internationale dans son ensemble et ce, tant dans le domaine civil que dans le domaine militaire et celui du renseignement. La Belgique elle-même se trouve engagée dans des programmes civils d'observation de la Terre.

Les premiers satellites d'observation militaire ont été lancés par les Etats-Unis en 1959 et par l'URSS en 1962. L'information fournie par les satellites a joué un rôle non négligeable dans l'élaboration des stratégies militaires : en permettant de réaliser des cartes topographiques précises, en détectant des objectifs et en permettant de suivre l'évolution de l'arsenal de l'adversaire. Les satellites d'observation, civils et militaires, connaissent aussi des applications dans le cadre de la surveillance de la mise en œuvre des traités internationaux de désarmement ou des mesures de sanctions et de désarmement imposées par l'ONU.

Mais cette situation est de plus en plus marquée par l'intensification de la commercialisation concurrentielle des services spatiaux. Des photos prises par satellites civils deviennent actuellement disponibles pour le grand public avec des degrés de résolution presque aussi élevés que ceux des satellites militaires et à des prix qui deviendront de plus en plus abordables au fur et à mesure que la concurrence commerciale s'installera dans ce secteur.

---

[2] « Aussitôt après l'exécution d'une prise de vues autorisée ou d'un programme de prises de vues autorisé, deux épreuves, munies d'un numéro d'ordre, de tous les clichés pris doivent être soumises à l'examen du ministre de la Défense nationale (Etat-major général de l'armée, 2e section).

Les images commerciales les plus performantes sont actuellement celles fournies par le satellite américain *Ikonos* ; elles sont commercialisées par la société américaine *Space Imaging*. Des sociétés concurrentes telles que *Orbital Imaging* (USA), *Kiberso* (Russie) et *Spot Image* (Europe) fournissent des images d'une résolution plus basse.

Ceci ne manque pas bien sûr de susciter des réticences et des débats au sein du gouvernement américain qui craint la diffusion de pareilles images à des pays belliqueux ou à des éléments hostiles. Ainsi, celui-ci exige que les constructeurs américains puissent contrôler l'obturateur de tout satellite d'observation vendu à des pays étrangers ou exploité pour eux. Les industriels, globalement soutenus par le département du Commerce sont favorables à une libéralisation du marché ; le département d'Etat et le Pentagone y sont hostiles. Au cours de ces dernières années, les industriels n'ont cessé de marquer des points mais il est certain que le gouvernement américain conserva toujours la possibilité d'interdire la vente d'images de certaines zones sensibles des Etats-Unis ou de ses alliés, de poser des limitations techniques (notamment sur les angles de prises de vues) ou de couper à tout moment le flot d'images. Jusqu'à présent , seul le territoire d'Israël ferait l'objet d'une telle restriction de la part des américains.

La crainte demeure donc que n'importe quel Etat, qu'il soit pacifique ou belliqueux, et même que n'importe quelle entreprise criminelle ou organisation hostile, puisse bientôt se procurer les moyens d'observer depuis l'espace les systèmes de défense et de sécurité des Etats de droit démocratiques.

Photos aériennes et photos satellitaires

Les possibilités d'observation de la Terre par satellites ne diminuent en rien l'utilité de l'observation aérienne. Tout d'abord, parce que les capacités d'observation par satellites ne sont pas encore à la portée de tous les pays. D'autre part, parce qu'une photographie aérienne s'obtient encore plus facilement et plus rapidement qu'une photographie par satellite. Enfin, l'observation de la terre par satellites est en passe de perdre son caractère secret et impromptu.

La vitesse moyenne de déplacement d'un satellite autour de la terre est de 7 km par seconde. La durée du cycle d'observation, soit l'intervalle de « revisite », est l'intervalle de temps qui sépare chaque passage du satellite au dessus d'un point observé. Ces temps de « revisite » (entre 24 et 72 heures) ne permettent pas toujours d'obtenir en temps voulu des images donnant des informations sur l'évolution d'une situation (« *current intelligence* »). Plus haute se situe l'orbite, plus grande est la surface d'observation couverte et plus l'intervalle de « revisite » est court. Par contre, la résolution est alors moins grande.

Le satellite étant en position de photographier une zone cible, encore faut-il que les conditions météorologiques ou de luminosité s'y prêtent. A moins d'être équipés de senseurs radars, il n'est pas possible de photographier à travers les nuages ou la nuit.

Les satellites dont le cycle d'observation est long présentent aussi le désavantage de n'offrir que des périodes limitées de transmission des données au sol, c'est-à-dire qu'elles sont limitées aux moments où les satellites sont en vue d'une station réceptrice.

Enfin, les satellites sont relativement rigides d'emploi sur le plan opérationnel ; certains sont manœuvrables, mais dans des limites assez étroites et, souvent au détriment de leur durée de vie puisque chaque manœuvre nécessite une grosse consommation de carburant.

Notons enfin que des systèmes de surveillance spatiale ont été déployés par les grandes puissances en vue de tenir à jour l'inventaire des quelques 8.000 satellites et objets divers en orbite autour de la terre. En rassemblant l'information de sources ouvertes, l'imagerie et les écoutes électroniques, ces réseaux sont en mesure de suivre les mouvements et d'analyser les missions de tous les satellites étrangers.

Ce flux de données permet notamment de lancer des avis de surveillance *SATRAN (Satellite Reconnaissance Advanced Notice)* aux forces armées, qui savent ainsi quand tel ou tel satellite de reconnaissance étranger est en mesure d'observer une aire d'activités militaires classifiée. Ce réseau est également en mesure de procéder à l'interception des communications et signaux des satellites étrangers, qu'ils soient civils ou militaires.

Depuis peu, un réseau international d'astronomes diffuse sur un site web intitulé *Heavens-Above.com* la position de chaque satellite. Ce site est principalement destiné à permettre aux passionnés de l'espace d'observer le passage d'un satellite dans une période déterminée de la nuit.

Le Comité R s'est demandé si ce site ne permettait pas à des organisations terroristes ou criminelles d'être en état de prévoir, au même titre que les puissances militaires, les périodes au cours desquelles il y aurait lieu de camoufler les activités, mouvements ou systèmes d'armes qu'elles désireraient soustraire à la surveillance spatiale. Le Comité R a questionné le SGR et la Sûreté de l'Etat à ce sujet.

Dans une analyse détaillée transmise au Comité R le 23 janvier 2001, le SGR estime en résumé que le site en question ne viole aucune règle de sécurité et ne présente donc aucun danger [3]. Le site ne donne pas en effet la possibilité au consultant de vérifier s'il se trouve dans le cône de visualisation d'un satellite d'observation militaire. Par ailleurs, l'orbite du satellite militaire Hélios, sommairement décrite sur le site, est du domaine public.

Il n'en demeure pas moins que les limites et inconvénients techniques de l'observation satellitaire font en sorte que la photographie aérienne reste et restera encore longtemps un outil utile et efficace de renseignement.

5. LE CADRE JURIDIQUE INTERNATIONAL

L'observation de la terre par satellites est conforme au droit international. Le «traité de l'espace» de 1967 énonce en effet deux grands principes, la liberté de circulation et la liberté d'utilisation des ressources de l'espace circumterrestre.

L'absence de toute souveraineté territoriale dans l'espace extra-atmosphérique et son corrolaire, l'application de la loi du pavillon aux engins spatiaux, fondent donc la légalité internationale des observations stratégiques dans et à partir de l'espace.

L'arrêté royal de 1939 n'est donc pas applicable à l'observation du territoire national à partir de satellites, ni d'ailleurs aux observations aériennes effectuées dans l'espace aérien dans le cadre du traité d'Helsinki du 24 mars 1992 sur le régime « ciel ouvert ».

[3] La Sûreté de l'Etat n'a pas encore fait connaître son point de vue au Comité R au moment de l'approbation du présent rapport.

Ce traité prolonge les engagements que les parties ont pris dans le cadre de la Conférence sur la sécurité et la coopération en Europe (CSCE) de promouvoir une ouverture et une transparence accrues de leurs activités militaires et de renforcer la sécurité par des mesures de confiance et de sécurité.

Les parties considèrent que la création d'un régime « ciel ouvert » applicable à l'observation aérienne est de nature à accroître l'ouverture et la transparence pour faciliter le contrôle du respect des accords existants et futurs de limitation des armements et pour renforcer la capacité de prévention des conflits et de gestion de crises.

Le traité instaure donc des procédures agréées pour permettre aux signataires d'observer sur une base équitable tous les territoires des Etats parties ainsi que leurs forces et activités militaires réciproques.

Les parties ont le droit d'effectuer un certain nombre de vols non armés sur l'ensemble des territoires des autres participants, à condition d'utiliser des avions et des techniques d'observation agréés, suivant des plans de mission et de vol préalablement convenus et contrôlés.

Les pays ayant signé ce traité sont les membres de l'OTAN, la Russie, l'Ukraine, la Biélorussie, la Géorgie, le Kirghistan ainsi que d'autres pays ex-membres du Pacte de Varsovie. Les autres pays sont admis à se joindre au traité. Le parlement belge a ratifié ce traité par la loi du 15 mai 1995 (Moniteur belge 12 décembre 1995).

6. LES CONSTATATIONS DU COMITE R

L'application de l'article 120 ter du code pénal et celle de l'arrêté royal du 21 février 1939 « *réglementant la prise de vues aériennes au-dessus du territoire national et le transport d'appareils photographiques à bord d'aéronefs* » font l'objet de plusieurs notes internes émanant du SGR :

- l'instruction TVR 62 : «*sécurité des prises de vues – prises de vues terrestres – prises de vues aériennes* » qui n'est cependant plus d'application ;
- la section 5 du règlement IF5 : « *sécurité des prises de vues – prises de vues terrestres – prises de vues aériennes* » (version du 8 janvier 1997)
- la liste des objectifs à protéger contre la prise de vues aériennes (version du 30 septembre 1997 et version du 14 décembre 1998).

Ces documents prévoient deux procédures distinctes selon qu'il s'agit de prises de vues terrestres ou de prises de vues aériennes.

6.1. Prises de vues terrestres

Pour les prises de vues terrestres, aucun document photographique, filmé ou télévisé de sujets militaires ne peut être pris ou diffusé sans l'autorisation de l'autorité militaire compétente. Selon le cas, l'autorité militaire compétente est le commandant de camp, de quartier, le chef de corps, le commandant de province, le cabinet du ministre de la Défense nationale, le SID ou le SGR/S.

Le SGR/S est compétent pour les autorisations de reportages filmés ou télévisés sur les troupes à l'exercice, les installations militaires et le matériel militaire.

La directive TVR 62 indiquait les mesures de sécurité que les autorités compétentes devaient prendre en matière d'autorisation de prises de vues. Ce document prévoyait ainsi que toutes les demandes d'autorisations (quelle que soit l'autorité compétente) devaient être adressées pour information à SDRA. Une personne en possession d'une autorisation de photographier des installations militaires devait aussi être accompagnée d'un officier pour vérifier qu'aucun objectif susceptible d'intéresser une puissance étrangère ne soit photographié. Ces instructions ne furent pas reprises dans le document IF5 qui règle actuellement la matière.

6.2. Prises de vues aériennes

En principe, l'administration de l'aéronautique transmet au SGR toute demande de prise de vues aériennes concernant le territoire national, qu'elle émane de civils ou de militaires.

Jusqu'il y a peu, lorsqu'il recevait une telle demande d'autorisation, le SGR consultait une liste confidentielle d'objectifs qu'il convenait de protéger. Cette liste reprenait, par provinces, les installations civiles (exemple : les centrales nucléaires) et militaires (exemple : les aérodromes) qui ne pouvaient être photographiées par voie aérienne. Après examen, le SGR renvoyait son avis à l'administration de l'aéronautique qui octroyait ou non l'autorisation.

En ce qui concerne la publication de photos aériennes, aussitôt après l'exécution des prises de vues autorisées, deux épreuves, munies d'un numéro d'ordre, de tous les clichés pris devaient être soumises à l'examen du SGR. Les photos autorisées de publication recevaient un cachet avec la mention « *publication autorisée* ».

Un exemplaire de ces photos demeurait la propriété de la Défense nationale, l'autre était renvoyé à son propriétaire. Les photos dont la publication n'était pas autorisée appartenaient définitivement à la Défense nationale et restaient en la possession du SGR.

En 1992, le SGR a entrepris des discussions sur l'application de l'arrêté royal de 1939 avec l'administration de l'aéronautique. Celle-ci, qui est compétente dans le cadre des matières réglées par la Convention de Chicago du 7 décembre 1944, a proposé aux autorités militaires d'abroger, ou tout au moins de conditionner, l'application de l'arrêté royal de 1939 à la promulgation de l'état de guerre.

Les autorités militaires n'ont cependant pas souscrit à cette proposition bien que le SGR était tout à fait conscient que cette réglementation était dépassée sur certains points.

En septembre 1998, une réunion s'est tenue au SGR à laquelle participaient des représentants de l'Etat-major, du SGR, de la Sécurité nucléaire et de l'Institut Géographique National (IGN) ; son but était d'examiner l'opportunité d'une modification des règles au sujet des autorisations de prise et de publication des photos aériennes.

Tous les participants à cette réunion ont été d'accord pour reconnaître le bien-fondé des remarques formulées par l'IGN selon lesquelles la commercialisation actuelle de photos satellitaires à haute résolution, aussi valables que les photos aériennes classiques, ne permettait plus d'exercer un quelconque contrôle sur leur prise ou leur diffusion.

Dès lors, on a estimé que les mesures restrictives encore en application quant à la publication des photos aériennes d'objectifs militaires étaient devenues quelque peu obsolètes.

Cependant, le SGR a aussi estimé qu'une suppression totale de toute législation en la matière serait un handicap en cas de situation de crise ; elle priverait la Défense nationale de moyens suffisants de poursuite à l'encontre de personnes malveillantes, que ce soit en matière d'espionnage proprement dit ou de recherches de renseignements par des organisations subversives ou terroristes. Le SGR a constaté également qu'une photo aérienne pouvait s'obtenir dans des délais beaucoup plus courts qu'une image satellitaire.

Il fut donc décidé de maintenir en vigueur la législation actuelle, tout en assouplissant son application, en particulier dans le domaine de l'autorisation de publication.

Un premier aménagement de cette disposition fut de faire désigner un officier de sécurité, titulaire d'une habilitation de sécurité, dans chaque grande firme utilisatrice de photos aériennes qui, elle-même devait être en possession d'une habilitation de sécurité.

L'officier de sécurité était mis en possession de la liste confidentielle des objectifs à préserver après avoir été dûment « briefé » par le SGR ; il était alors habilité pour statuer au nom du SGR. Il existe encore actuellement deux de ces firmes belges qui disposent d'officiers de sécurité.

Une deuxième mesure fut de supprimer de la liste confidentielle des objectifs à protéger contre les prises de vues aériennes tous les objectifs qui s'y trouvaient mentionnés. Cette liste actuellement vierge existe donc encore pro forma et la possibilité d'y faire à nouveau figurer des objectifs à protéger en cas d'absolue nécessité demeure.

Les firmes qui souhaitent prendre et publier des photos aériennes du territoire belge ne doivent donc plus être titulaires d'habilitations de sécurité aussi longtemps que la liste des objectifs à protéger restera vierge.

D'autre part, les photos aériennes militaires n'étant plus à présent classifiées, leur publication peut être autorisée automatiquement à moins que n'y figurent des renseignements complémentaires ou des annotations les rendent sensibles.

Pour les photos aériennes prises par des civils, l'administration de l'aéronautique applique toujours le principe selon lequel toutes les prises de vues aériennes sont soumises à une autorisation préalable délivrée par ce service. Cette autorisation est délivrée exclusivement à une personne physique (le photographe) et n'est pas cessible. Elle est valable pour une période de deux ans.

En principe, l'accord préalable du ministre de la Défense nationale n'est donc plus requis, quelle que soit la nationalité du photographe. La délivrance de l'autorisation par l'administration de l'aéronautique implique automatiquement la délivrance de l'autorisation de publication. Les autorisations délivrées par cette administration sont transmises a posteriori pour information au ministère de la Défense nationale. Le SGR reste donc informé des autorisations accordées de manière à lui permettre d'exercer un contrôle.

L'ensemble des dispositions précitées est d'application depuis le 1er janvier 1999.

Néanmoins, lorsqu'elle délivre une autorisation d'effectuer des prises de vues aériennes au-dessus du territoire belge, l'administration de l'aéronautique notifie cette décision au moyen d'un formulaire pré-imprimé qui mentionne que le photographe doit éviter des prises de vues d'installations militaires et leur publication.

Ceci résulte d'une recommandation en ce sens que le SGR a encore adressée en 1999 à cette administration, nonobstant les nouvelles dispositions.

En outre, l'administration de l'aéronautique mentionne également que l'accord préalable du parquet peut être nécessaire pour des photographies aériennes d'événements d'actualité comme des incendies ou des accidents graves et que cet accord est toujours demandé par la voie du service de Sécurité militaire.

Ceci résulte d'une procédure que les autorités judiciaires appliquaient autrefois avant la mise en vigueur des nouvelles dispositions mais qui n'est plus appliquée depuis lors.

6.3. L'application du traité « ciel ouvert »

Le SGR déclare n'avoir reçu aucune compétence dans l'application du traité « ciel ouvert » étant donné que les prises de vues réalisées dans le cadre de ce traité ne sont pas destinées à être publiées.

6.4. Nombre de demandes traitées

Le nombre de demandes traitées par le SGR était de 1.097 en 1997, 1.950 en 1998, 245 en 1999 dont une quarantaine en provenance de ressortissants hors UE. Aucune demande de prise de vues, ni de publication n'a été refusée.

7. CONCLUSIONS

Tout le monde s'accorde à reconnaître que les dispositions de l'arrêté royal du 21 février 1939 « *réglementant la prise de vues aériennes au-dessus du territoire national et le transport d'appareils photographiques à bord d'aéronefs* » sont devenues obsolètes, tant par l'apparition de la technologie des satellites d'observation, que par l'adhésion de la Belgique au traité d'Helsinki du 24 mars 1992 sur le régime « ciel ouvert ».

Cependant le SGR estime qu'une suppression totale de toute législation en la matière serait un handicap en cas de situation de crise ; elle priverait la Défense nationale de moyens suffisants de poursuite à l'encontre de personnes malveillantes, que ce soit en matière d'espionnage proprement dit ou de recherche de renseignements par des organisations subversives ou terroristes.

Le SGR estime donc devoir conserver un moyen de contrôle a posteriori sur les prises de vues aériennes. La solution retenue a été de ne pas abroger l'arrêté royal du 1939 tout en allégeant fortement la procédure pour l'octroi des autorisations, et en se réservant ainsi la possibilité d'en rétablir une stricte application.

Le Comité R se demande néanmoins si l'article 120 ter du code pénal et l'arrêté royal du 21 février 1939 ne devraient pas être revus et adaptés compte-tenu du nouvel environnement juridique international d'une part, de l'évolution technologique en matière d'observation spatiale et aérienne, d'autre part.

Le Comité R pense que la protection des objectifs militaires à l'égard de prises de vues à des fins hostiles ou d'espionnage pourrait être assurée dans un cadre juridique similaire à la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

CHAPITRE 6 : RAPPORT DE L'ENQUÊTE SUR «LA SURVEILLANCE ÉVENTUELLE D'UNE MANIFESTATION SYNDICALE DE MILITAIRES PAR LE SGR »

1. INTRODUCTION

Le mercredi 19 juillet 2000 eut lieu une manifestation de militaires devant le cabinet du ministre de la Défense nationale organisée par la CCSP (centrale chrétienne des services publics) à l'appui de revendications salariales.

Une information est parvenue au Comité R selon laquelle des membres du SGR auraient été présents sur les lieux de cette manifestation et auraient cherché à relever l'identité des participants en les interrogeant discrètement, sans toutefois réussir à passer inaperçus.

Le Comité R a voulu vérifier cette information et savoir s'il était coutumier pour le SGR de surveiller, directement ou indirectement, des manifestations syndicales de militaires. Dans l'affirmative, comment une telle surveillance peut-elle se justifier par rapport aux missions légales du SGR ? Ne serait-elle pas contraire aux droits de libre expression et d'association dont jouissent les militaires à l'instar des autres citoyens ?

2. PROCEDURE

Réuni le mercredi 23 août 2000, le Comité R a décidé d'ouvrir une enquête sur «*la surveillance éventuelle d'une manifestation syndicale de militaires par le SGR*».

Par apostille du 28 août 2000, le président du Comité R a chargé le Service d'enquêtes de procéder à des vérifications auprès du SGR.

Le président du Sénat, a été averti de l'ouverture de cette enquête par lettre du 31 août 2000, conformément à l'article 32 de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements.

Le ministre de la Défense nationale, a été averti de l'ouverture de cette enquête par lettre du 31 août 2000, conformément à l'article 43-1° de la même loi.

Le Service d'enquêtes du Comité R a procédé à l'audition du chef du service de la sécurité militaire du SGR en date du 18 octobre 2000.

Le Service d'enquêtes a déposé son rapport au Comité R le 20 octobre 2000.

Ce rapport a été examiné par le Comité R le 14 novembre 2000, à la suite de quoi une apostille complémentaire a été adressée au Service d'enquêtes le 17 novembre 2000.

Le rapport complémentaire du Service d'enquêtes a été remis au Comité R le 19 février 2001.

Le présent rapport a été approuvé par le Comité R le 22 février 2001.

Par courrier du 25 avril 2001, le Ministre de la Défense nationale a fait part au Comité R qu'il n'avait aucune remarque à formuler quant à la publication du présent rapport.

3. CONSTATATIONS

Comme dans chaque cas de manifestation organisée sur la voie publique, le rassemblement syndical de militaires organisé le 19 juillet 2000 devant le cabinet du ministre de la Défense nationale par la CCSP (centrale chrétienne des services publics) à l'appui de revendications salariales a fait l'objet d'une surveillance de la part de la gendarmerie en vue du maintien de l'ordre.

Une rumeur a couru parmi les manifestants selon laquelle le SGR aurait été présent parmi eux. Cependant, le Comité R a constaté qu'aucun ordre n'avait été donné au SGR en vue de surveiller cette activité syndicale. Aucun élément de l'enquête ne permet de conclure qu'il en aurait été autrement dans la réalité. Aucun membre du SGR n'a été présent sur les lieux de cette manifestation. Il n'y a eu aucun échange d'informations entre la gendarmerie et le SGR à son sujet.

Le SGR a pour ligne de conduite de ne pas surveiller les activités syndicales des militaires aussi longtemps qu'aucune activité menaçante pour le pays ou pour la sécurité des forces armées ne s'y développe.

CHAPITRE 7 : RAPPORT DE L'ENQUÊTE SUR LA MANIÈRE DONT LA SÛRETÉ DE L'ETAT S'ACQUITTE DE SA NOUVELLE MISSION DE PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE

1. INTRODUCTION

« Aujourd'hui, les conflits ne sont plus systématiquement ouverts ni déclarés. Les agressions économiques notamment sont plus sournoises, elles peuvent déstabiliser gravement nos sociétés modernes. Le XXIème siècle, qui sera celui de la complexité, nécessite dès aujourd'hui la conception et la mise en oeuvre d'une stratégie globale répondant au défi. La cohérence et l'efficacité de cette démarche ne seront garanties que si la société civile et l'Etat maintiennent des échanges permanents et translatéraux ».

Marc LADREIT de LACHARRIERE
Président de l'Institut d'études et de recherches pour la sécurité des entreprises (Paris)

1.1. Objet de l'enquête

Au cours de l'année 1998, alors que le Parlement débattait du projet de loi organique des services de renseignement et de sécurité, le Comité R a mené une enquête en vue de sensibiliser les autorités politiques sur l'importance de cette nouvelle mission de protection du potentiel scientifique et économique ([1]).

Dans les recommandations résultant de son enquête, le Comité R avait préconisé la création d'un organe de concertation entre les ministres concernés par cette matière et les entreprises détentrices d'un potentiel scientifique et économique vital pour la Belgique. Le Comité R avait également indiqué qu'il ne faudrait pas négliger de fournir à la Sûreté de l'Etat les moyens qu' elle réclamait, au risque de voir la future disposition législative rester lettre morte.

1 Comité R - rapport d'activités 1998, p. 70 (fr.).

Depuis lors, est entrée en vigueur la loi du 30 novembre 1998 organique des services de renseignement et de sécurité dont l'article 7 donne à la Sûreté de l'Etat entre autres missions, celle *"de rechercher, d"analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer (...) le potentiel scientifique et économique défini par le Comité ministériel* (du Renseignement) ».

Deux années après la mise en vigueur de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, le Comité R a examiné de quelle manière la Sûreté de l'Etat avait pris en charge sa nouvelle mission.

Pour ce faire, le Comité R a d'abord réuni et consulté une abondante documentation issue de sources ouvertes (articles de presse, livres, revues spécialisées, websites, etc.) afin de se forger une idée générale sur la problématique de la protection du potentiel scientifique et économique. A partir de sa propre recherche, le Comité R a élaboré un rapport d'ordre général repris en introduction du présent rapport d'enquête.

1.2. Procédure

Le Comité R a décidé d'ouvrir cette enquête le 14 février 2000.

Le Comité R a examiné les documents et notes internes de la Sûreté de l'Etat dont il était en possession en vertu de l'article 33 de la loi organique du 18 juillet 1991 relative au contrôle des services de polices et de renseignements : il y a recherché toutes les informations disponibles et toutes les instructions données à propos de l'exécution de la nouvelle mission.

Le 2 mars 2000, les membres du Comité R ont entendu Madame G. Timmermans, administrateur général a.i. de la Sûreté de l'Etat, dans le cadre de l'enquête complémentaire demandée par le Sénat sur le système d'interception « Echelon ». A cette occasion, des questions ont aussi été posées sur l'exécution de la nouvelle mission de protection du potentiel scientifique et économique.

Pour se familiariser avec les pratiques du renseignement (ou intelligence) économique, le Comité R a envoyé un de ses membres à Paris les 16 et 17 mai 2000 pour assister à un séminaire intitulé "*Maîtriser les outils de la veille et de l'Intelligence économique »*.

Par apostille du 7 juin 2000, le Président du Comité R a chargé le Service d'enquêtes de procéder à certaines vérifications.

Par courrier du 7 juin 2000, conformément à l'article 43-1° de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements, le Ministre de la Justice a été averti de l'ouverture et de l'objet de l'enquête par les soins du Chef du Service d'enquêtes.

Le mardi 4 juillet 2000, le Comité R a tenu une réunion d'information avec deux représentants de la Fédération des Entreprises de Belgique, MM. Marc Verschaeve, directeur administratif, et Yvan De Mesmaeker (ir.), conseiller en sécurité.

Le Service d'enquêtes a transmis son rapport au Comité R le 23 novembre 2000.

Des courriers ont été échangés avec la Sûreté de l'Etat sur le sujet.

Le présent rapport a été approuvé le 23 janvier 2001.

Le Ministre de la Justice a formulé des remarques dont le Comité R a tenu compte dans le présent rapport.

Dans son courrier du 13 mars 2001, le ministre de la Justice estimait opportun avec l'accord du Comité R de transmettre ce rapport au groupe de travail relevant du Cabinet de Monsieur le Premier Ministre chargé de préparer les directives du Comité ministériel de renseignement.

1.3. L=intérêt parlementaire

1.3.1. Le Parlement belge

Outre les amendements déposés à l'occasion de la discussion du projet de loi organique des services de renseignement et de sécurité, le Comité R a relevé les questions et interpellations parlementaires suivantes sur le sujet :

- Questions n° 870/1 et 870/2 du 16 février 1998 posée par le sénateur Boutmans (Agalev) aux ministres des Affaires économiques et de la Défense nationale. A la connaissance du Comité R, aucune réponse n'a encore été donnée à cette question à la date d'approbation du présent rapport ([2]). La question portait sur l'application de la loi du 10 janvier 1955 concernant la mise en oeuvre des inventions et des secrets de fabrique intéressant la défense du territoire ou la sûreté de l'Etat ([3]).

- Interpellation n° 84 de M. le député Bourgeois (VU-ID), le 20 octobre 1999, au ministre de la Justice sur "*la guerre économique et le rôle de la Sûreté de l'Etat et du Parquet »* ([4]).

A ces questions et interpellations, on peut aussi également joindre les récents débats au Parlement belge concernant la problématique du réseau d'interception "Echelon ». Le rapport STOA présenté au Parlement européen cite en effet quelques cas dans lesquels des firmes européennes auraient été évincées de marchés importants par suite de l'interception de leurs communications au cours de transactions commerciales internationales (Panavia European Fighter Aircraft consortium, Thomson CSF, Airbus industrie).

---

2 22 janvier 2001

3 Sénat, Questions et réponses - bulletin 1-69

4 Chambre - 2e session de la 50e législature (HA 50 COM 025)

1.3.2. Le Parlement européen

Réuni le mercredi 5 juillet 2000 à Strasbourg, le Parlement européen s'est prononcé sur la constitution d'une commission temporaire d'enquête sur le système d'interception des télécommunications "Echelon ». Au cours des discussions préalables qui se sont tenues au sein de la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures, le député allemand Martin Schulz (PSE) a déclaré le 5 avril 2000 que l'espionnage économique n'était pas seulement pratiqué par les Etats-Unis et le Royaume Uni, mais aussi par d'autres pays comme la France, les Pays-Bas et ... la Belgique ([5]).

2. ESSAI DE DESCRIPTION GÉNÉRALE DE LA PROBLÉMATIQUE

Décrire la mission de protection du potentiel scientifique et économique confiée à la Sûreté de l'Etat nécessite que soient posées les quatre questions fondamentales suivantes :

1) Qu'est-ce que le potentiel scientifique et économique d'un pays et, singulièrement, celui de la Belgique ?

2) Qui sont les acteurs concernés par le développement du potentiel scientifique et économique d'un pays ?

3) A quelles menaces est exposé le potentiel scientifique et économique d'un pays ?

4) Quelles actions et quels moyens un service de renseignement peut-il mettre en oeuvre pour protéger le potentiel scientifique et économique d'un pays ?

2. 1. Qu'est-ce que le potentiel scientifique et économique d'un pays ?

Le premier rapport que le Comité R a consacré à cette matière faisait déjà apparaître la difficulté de cerner la notion de potentiel scientifique et économique. Au sens des articles 7, 1° et 8, 4° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, on entend par "*potentiel scientifique et économique »* , « *la sauvegarde des éléments essentiels du potentiel scientifique et économique »*. Il appartient au Comité ministériel du Renseignement et de la Sécurité de définir plus avant cette notion.

En juillet 2000, le Conseil des ministres a pris connaissance d'une note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale. Le Comité R a cherché dans ce document quelques éléments susceptibles de préciser davantage la notion de potentiel scientifique et économique.

---

[5] cf. www.europarl.eu.int/ - déclaration aussi disponible sur : homeusers.brutele.be/cdc/euro.htm

Cette note indique que l'économie est désormais fondée sur la connaissance; elle souligne qu'environ 50% de la croissance économique est liée aux nouvelles technologies et aux nouveaux produits. La recherche scientifique est donc devenue une préoccupation majeure tant au niveau européen que national. En Belgique, la politique scientifique ressort des Services fédéraux des Affaires scientifiques, techniques et culturelles (SSTC en abrégé).
La note d'orientation ne donne guère d'indications sur les recherches scientifiques de pointe effectuées en Belgique; elle souligne cependant la qualité des recherches, des technologies et des applications spatiales en Belgique. Le ministre de l'Economie et de la Recherche scientifique annonce seulement son intention de procéder à une évaluation du potentiel scientifique présent dans les "pôles d'attractions technologiques » (PAT) et « Pôles d'attractions Inter universitaires » (PAI) en Belgique. Il annonce aussi son intention « *de mettre à la disposition des centres de recherches fédéraux et des Interfaces universités-entreprises des universités belges, des agents chargés de la prospection dans les secteurs de pointe afin de renforcer notre capacité de transferts technologiques ».*

La notion corollaire de **sécurité économique**, objectif général auquel doivent en principe tendre tous les gouvernements, a été définie comme suit par le Service canadien du renseignement de sécurité : « *L'époque où la question de la sécurité mondiale primait sur les préoccupations d'ordre économique et les conflits régionaux dans les relations internationales est révolue. L'interdépendance économique et la concurrence internationale croissantes sont devenues des sources importantes de tensions et de conflits entre les puissances mondiales. Dans ce climat d'incertitude, les pays industrialisés qui désirent vivement maintenir leur niveau de vie et les pays en développement qui sont tout aussi déterminés à améliorer le leur sont poussés à utiliser tous les moyens à leur disposition pour améliorer leur productivité et assurer leur* ***sécurité économique****. L'un de ces moyens est l'espionnage économique (...) »* ([6]).

En France, la sécurité économique consiste à veiller à ce que les moyens, connaissances ou informations permettant de préserver les intérêts essentiels de la nation, soient conservés sous le contrôle français et qu'ils soient développés et adaptés en permanence à l'évolution du contexte et des risques géo-stratégiques mondiaux ([7]).

Au Canada, on entend par sécurité économique le fait de maintenir des conditions propres à favoriser une augmentation relative soutenue et à long terme de la productivité du travail et du capital, ce qui assure à la population un niveau de vie élevé et en progression constante, et garantit un environnement économique équitable, sûr et dynamique, propice aux innovations, aux investissements intérieurs et étrangers, ainsi qu'une croissance soutenue ([8]).

---

6 « La sécurité économique », rapport du Service canadien du renseignement de sécurité paru dans *« Série d'aperçus »* n° 6, mai 1998 - www.csis-scrs.gc.ca

7 « *De la défense économique à la sécurité de l'économie »*, Jean-Louis Levet - rapport du Commissariat général du Plan, 1997

8 « Série d'aperçus » n° 6 - mai 1998, publication du Service Canadien de Renseignement de Sécurité.

2. 2. Qui sont les moteurs du potentiel scientifique et économique d'un pays ?

A cet égard, la situation se caractérise par la diversification et l'hétérogénéité croissante des moteurs du potentiel scientifique et économique d'un pays. A côté de l'Etat lui-même, de ses infrastructures (physiques ou virtuelles), de ses services, entreprises publiques autonomes (SNCB, Belgacom, etc.), on trouve les entités fédérées (communautés et régions), les universités, hautes écoles et autres organismes d'intérêt public, les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires de recherches, ainsi que leurs personnels qui, chacun avec une logique propre, les uns de service public, les autres de profit, occupent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

Ceci implique qu'une liste de secteurs d'activités vitales à protéger dans ces différents secteurs soit établie en définissant un ordre de priorité. Il faut toutefois être conscient que les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises.

Les responsables politiques, dirigeants, fonctionnaires, cadres, chercheurs et autres membres du personnel participant au développement du potentiel scientifique et économique, doivent être conscients des activités qui peuvent menacer leur secteur et du rôle qu'ils peuvent jouer pour le protéger.

2. 3. A quelles menaces est exposé le potentiel scientifique et économique d'un pays ?

Les menaces issues d'une volonté humaine malveillante sont de plusieurs natures parmi lesquelles:

- le terrorisme, le sabotage visant la destruction physique d'infrastructures;
- la déstabilisation de l'économie par la corruption, l'introduction et le blanchiment de capitaux provenant d'activités criminelles ([9]), la désinformation, etc...
- la prédation de l'information ou l'espionnage.

Le présent rapport visera plus particulièrement cette dernière forme de menace qu'est l'espionnage. Il tentera de distinguer cette activité du renseignement ou de l'intelligence économique.

[9] Voir à ce sujet ce qu'en disent les rapports annuels d'activités de la Cellule de Traitement des Informations Financières

3. L'ESPIONNAGE - LE RENSEIGNEMENT ÉCONOMIQUE - L'INTELLIGENCE ÉCONOMIQUE - DÉFINITIONS GÉNÉRALES.

Le présent rapport aura plusieurs fois recours aux notions de "renseignement économique", "intelligence économique", "espionnage économique et industriel". Ces concepts font l'objet de nombreuses définitions plus ou moins semblables selon les écoles. Le Service Canadien du Renseignement de Sécurité retient les définitions suivantes.

L'espionnage économique est le fait pour un gouvernement d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques ([10]).

L'espionnage industriel est le fait, pour un organisme du secteur privé ou ses représentants, d'utiliser ou de faciliter l'utilisation de moyens illégaux, clandestins, coercitifs ou trompeurs pour avoir accès sans autorisation à des renseignements économiques ou technologiques en propriété exclusive, afin d'en retirer des avantages économiques ([11]).

Dans un document interne soumettant des propositions à l'approbation du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'Etat écrit : "*Si le mandant de l'espion est de nationalité belge, il s'agit d'espionnage industriel et ce domaine n'est pas du ressort de la sûreté de l'Etat. Si par contre, le mandant est originaire d'un pays étranger, il s'agit d'espionnage économique et la lutte contre cette activité s'inscrit parfaitement dans le cadre des missions de la Sûreté de l'Etat.*" Pour ce service, ce serait donc la nationalité du mandant de l'espion qui ferait la différence entre espionnage économique et espionnage industriel.

Le Comité R a interrogé l'administrateur général de la Sûreté de l'Etat sur ce point de vue à l'égard duquel il émet de nettes réserves. En effet, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises.

Le renseignement économique et **l'intelligence économique** sont deux notions complémentaires mais cependant distinctes.

On entend par **renseignement économique** toutes les informations économiques à caractère politique ou commercial, y compris les données technologiques, financières, commerciales en propriété exclusive, ainsi que les informations gouvernementales, qui sont susceptibles de contribuer directement ou indirectement à l'accroissement de la productivité ou à l'amélioration de la position concurrentielle des puissances étrangères qui en font l'acquisition ([12]).

---

10 « Série d'aperçus » n° 6 - mai 1998, publication du Service Canadien de Renseignement de Sécurité.

11 Idem.

12 « Série d'aperçus » n° 6 - mai 1998, publication du Service Canadien de Renseignement de Sécurité

L'intelligence économique ([13]) peut être définie de plusieurs manières. En France, on la considère généralement comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques ([14]). Stevan Dedijer, premier universitaire à avoir formalisé l'intelligence économique dans les années 70 à l'université de Lund (Suède), estime pour sa part qu'elle doit avoir pour rôle de nourrir les *"intuitions des décideurs"*. Mais certains n'hésitent pas à présenter l'intelligence économique comme une utilisation efficace de l'information à travers des activités de lobbying et d'influence, voir même de corruption.

Une équipe française de recherche associée au Centre des Hautes Etudes de l'Armement (CHEAr) estime que *"parce que la concurrence ne s'assimile pas à la guerre, le renseignement économique n'est pas une forme de renseignement comme les autres. En effet, il utilise essentiellement des méthodes ouvertes et ses multiples acteurs sont autant publics que privés. Plus qu'un espionnage économique inadapté, le véritable enjeu est de créer un réseau d'intelligence économique, favorisant la diffusion de l'information au sein de l'économie nationale et dépassant certains travers culturels tels que la rétention d'informations"* ([15]).

Certains auteurs estiment que l'intelligence économique, selon qu'elle est pratiquée par les entreprises ou les Etats, n'obéit pas toujours à la même logique dans les deux cas. Et ceux-ci de développer le tableau suivant ([16]) :

L'intelligence économique	**des entreprises**	**des Etats**
a pour objectif final	le développement de l'entreprise,	la puissance économique,
cible	les produits,	le marché mondial,
recherche d'abord	l'information centrée sur les métiers,	l'information centrée sur les réseaux,
pratique	le lobbying,	l'influence,
recherche l'information	dans le marché privé de l'information,	dans le processus du renseignement,
transmet l'information	au PDG, au conseil d'administration,	à l'autorité politique responsable de l'économie
est imprégnée	de la culture d'entreprise,	de la culture du renseignement.

13 Cet anglicisme est souvent préféré par les francophones au terme français « renseignement économique », car il leur paraît mieux refléter la richesse de cette activité et l'étendue des connaissances et de la culture qu'il met en oeuvre.

14 Rapport du Xième plan français (février 1994) « *Intelligence Economique et stratégique des entreprises* » (souvent désigné sous l'appellation « rapport Martre »).

15 « *Le renseignement économique : enquête sur un faux débat* » - Nicole Chaix, Philippe Dubost, Arnaud Voisin dans « Les cahiers de la sécurité intérieure » n° 30 1997 - IHESI

16 D'après « *une approche française de l'intelligence économique* » - Christian Harbulot - 1995

Dans la réalité, la pratique de l'intelligence économique par les entreprises et celle des Etats ne sont probablement pas aussi clichées que le voudraient ces auteurs. Le Comité R retiendra pour sa part que les objectifs de l'intelligence économique pratiquée par les entreprises ne coïncident pas toujours avec la préservation de la puissance économique de la Nation.

4. LA DIFFICILE PROTECTION DES SECRETS ÉCONOMIQUES, SCIENTIFIQUES ET TECHNOLOGIQUES NATIONAUX DANS UNE SOCIÉTÉ D'OUVERTURE INTERNATIONALE, D'INFORMATION ET DE PROGRÈS TECHNOLOGIQUES

Il convient de situer la protection des secrets scientifiques et économiques dans le contexte de la mondialisation, de la société de l'information et des progrès technologiques.

4. 1. L'ouverture de la politique scientifique de l'Union européenne et du gouvernement fédéral.

Le premier rapport que le Comité R a consacré à cette matière faisait déjà apparaître la difficulté de sensibiliser les universités et les centres de recherche à la protection de leurs travaux d'autre part : "*Les universités et les centres scientifiques ont toujours été une cible privilégiée en matière de renseignement. L'esprit d'ouverture et le manque chronique de méfiance des chercheurs vis-à-vis de leurs collègues et homologues étrangers ont de tout temps fait de ces centres publics de recherche une cible facile pour les agents des services de renseignement.*" ([17])

Le sommet des Chefs d'Etats et de Gouvernements de l'Union européenne qui s'est déroulé à Lisbonne en mai 2000 s'est fixé comme objectif stratégique de développer l'économie de la connaissance la plus compétitive et la plus dynamique du monde. A cet égard, l'Union européenne a notamment prévu, à court et à moyen termes, la mise sur pied d'indicateurs européens pour la recherche et le développement, la création d'un grand réseau européen à haute vitesse pour les communications électroniques, la mise sur pied d'un brevet communautaire et la levée de toute entrave à la mobilité des chercheurs.

La mise en contact des chercheurs, leur collaboration mutuelle et leur mobilité sont considérées comme des conditions essentielles à la création d'un espace européen de recherche. Pour le rendre attrayant aux chercheurs du monde entier, il est prévu d'encourager l'extension des "Pôles d'attractions technologiques" (PAT [18]), des "Pôles d'attractions Inter universitaires" (PAI [19]), de même que de créer un système de bourses pour les scientifiques des pays tiers.

---

17 Comité R, rapport d'activités 1998, p. 70 et suivantes.

18 Centres de recherches fédéraux dédiés aux secteurs industriels classiques ou nouveaux pour y stimuler l'innovation.

19 Programmes fédéraux de financement de recherches universitaires.

La rencontre de cet objectif, auquel chaque Etat membre a souscrit, nécessite un plan de convergence européen ainsi qu=une coordination des matières scientifiques dans notre pays. A*Seule, en effet, une cohérence globale des efforts de recherche assurera l=indispensable effet de masse permettant à l=Europe de garder une place crédible dans la confrontation qui l=associe aux Etats-Unis et au Japon*@ ([20]).

Notons enfin que les accords européens établissant des associations entre les Communautés européennes, leurs Etats membres et certains Etats de l=ancien bloc de l=Est comportent tous un volet relatif à la coopération dans les domaines de la science et de la technologie. Ces accords prévoient notamment des échanges d=informations, l=organisation de réunions scientifiques communes, des programmes communs de recherches et développement qui visent à favoriser le progrès scientifique et le transfert de technologies et de savoir-faire.
Le ministre de l=Economie et de la Recherche scientifique compte procéder à une évaluation du potentiel scientifique présent dans les Apôles d=attraction technologiques@ (PAT) et APôles d=attractions Inter universitaires@ (PAI) en Belgique. Il veut également faire inscrire dans la nouvelle phase des APAI@ l=obligation de participer à des équipes de recherche du Nord et du Sud du pays, mais aussi européennes, voire plus largement internationales.

A cet égard, la Belgique a, comme tous les pays avancés en la matière, grand intérêt à renforcer l=accueil de chercheurs étrangers afin d=accroître son propre potentiel.

Le ministre souhaite donc proposer des mesures fiscales en faveur des chercheurs étrangers engagés en Belgique dans un post-doctorat.

Dans un tel contexte de mondialisation et d=ouverture d=esprit scientifique, la difficulté apparaît clairement de cibler les secrets à protéger pour assurer la pérennité du potentiel scientifique et économique du pays ainsi que le veut la loi organique des services de renseignement et de sécurité.

4. 2. La protection des secrets technologiques et économiques dans une société en mutation.

L=analyse contenue dans la présente section s=inspire des travaux de l=éminent juriste français Bertrand Warusfel, maître de conférences à la faculté de droit de Paris V, auteur d=une thèse sur la protection du secret ([21]). Selon Bertrand Warusfel, la transformation profonde - due pour l=essentiel aux progrès techniques - que connaît notre société A*modifie fondamentalement la valeur des principaux paramètres de l=équation du secret*@. Trois caractéristiques décrivent cette modernité :

- la diversification des facteurs de puissance : à côté des facteurs traditionnels de la puissance politique, diplomatique et militaire, les enjeux de puissance et les luttes stratégiques se déplacent vers l=économie, la technologie et la culture, ce qui conduit à la prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret;

20 Note d'orientation du ministre de l'Economie et de la Recherche scientifique relative à l'évolution de la politique scientifique fédérale.

21 Bertrand Warusfel, : *Contre-espionnage et protection du secret - Histoire, droit et organisation de la sécurité nationale en France*, juin 2000 - éditions *Lavauzelle.*

- la diversification des acteurs de la puissance : à côté des Etats, les acteurs économiques, qu'ils soient nationaux ou supranationaux, jouent un rôle stratégique de plus en plus important;

- la transformation des lieux et des supports de la puissance : la nouvelle donne oppose la délocalisation de la puissance et l'immatérialité des ressources de l'information à l'ancien ordre basé sur la territorialité, la matérialité du pouvoir et l'appropriation physique des ressources.

  Les moyens et supports du secret sont aujourd'hui essentiellement des systèmes électroniques d'informations vulnérables aux manipulations et aux techniques d'interceptions des communications ([22]).

Le Comité R considère par ailleurs que la mondialisation de l'économie constitue aussi une caractéristique nouvelle de notre société. En effet, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent plus difficile l'attribution d'une nationalité aux entreprises. Comment déterminer dans ces conditions ce qui constitue le caractère national du potentiel économique et scientifique à protéger ?

Des représentants de la Fédération des Entreprises de Belgique (FEB) ont fait part au Comité R qu'ils considéraient comme belge toute entreprise implantée sur le territoire national et qui y crée une valeur ajoutée, quelle que soit la nationalité de ses actionnaires ou de ses dirigeants.

4. 3. La prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret

Jusqu'il y a peu en effet, ces secrets n'étaient protégés que de manière périphérique. En Belgique, ils ne figurent pas parmi les secrets qui intéressent la défense du territoire ou la sûreté de l'Etat et dont la protection est organisée par un certain nombre de dispositions figurant au chapitre II du titre I[er] du livre II du code pénal (intitulé *«crimes et délits contre la sûreté extérieure de l'Etat»*) et par des lois particulières.

Cependant, aux termes de la loi du 10 janvier 1955 *«relative à la divulgation et à la mise en oeuvre des inventions et des secrets de fabrique intéressant la défense du territoire ou la sûreté de l'Etat»*, la divulgation volontaire ou par négligence de ces inventions et secrets de fabrique est passible de sanctions pénales. Il faut cependant prouver que l'auteur de la divulgation ne pouvait ignorer qu'elle était contraire aux intérêts de la défense du territoire ou de la sûreté de l'Etat. A cet égard, le ministre qui a la propriété industrielle dans ses attributions (le ministre des Affaires économiques) et le ministre de la Défense nationale peuvent déclarer conjointement que la divulgation d'une invention ou d'un secret de fabrique est contraire aux intérêts de la défense du territoire ou de la sûreté de l'Etat et qu'elle est interdite pendant la période qu'ils déterminent.

22 Lire à ce sujet "*Development of surveillance technology and risk of abuse of economic information"*, by Duncan Campbell - working document for the *Scientific and Technological Options Assesment (STOA)* panel - European Parliament - http://www.gn.apc.org/duncan/stoa.htm

Les deux ministres précités, agissant conjointement, peuvent également déterminer et contrôler temporairement les conditions d'exploitation, d'invention et de mise en oeuvre de certains brevets qu'ils estiment devoir maintenir secrets; ils peuvent même en interdire temporairement leur exploitation ou leur mise en oeuvre, ou bien encore réserver à l'Etat, et à lui seul, le droit de les exploiter en tout ou en partie.
Ces mesures peuvent être levées à tout moment, partiellement ou totalement, par décision des ministres dont elles émanent. Le titulaire du droit sujet à interdiction ou limitation peut solliciter cette mainlevée. Des sanctions pénales sont aussi prévues pour les infractions à ces mesures.

La loi de 1955 fixe une procédure par laquelle le ministre des Affaires économiques soumet une demande de brevet au ministre de la Défense nationale en vue de la mise en oeuvre des mesures précitées.

Cette loi prévoit encore que "*lorsque, dans l'intérêt de sa défense, un Etat étranger interdit la divulgation d'une invention, objet d'une demande de brevet, le ministre ayant la propriété industrielle dans ses attributions s'abstiendra, sur requête de cet Etat ou du déposant qui établira la preuve de l'interdiction, de la communiquer au public et de délivrer des copies de sa description, aussi longtemps que durera cette interdiction*". Une telle requête ne peut toutefois être prise en considération que s'il existe une convention entre la Belgique et l'Etat étranger auteur de l'interdiction. La question parlementaire n° 870 relative à l'application de cette loi de 1955 posée le 16 février 1998 par le sénateur Eddy Boutmans (Agalev) est restée sans réponse à la date d'approbation du présent rapport ([23]).

Jusqu'au vote de la loi du 11 décembre 1998 "*relative à la classification et aux habilitations de sécurité*", la loi de 1955 était la seule en droit belge qui attribuait à une autorité politique la responsabilité de décréter le secret d'informations à caractère économique.

Entre 1949 et 1994, la Belgique a participé à la concertation COCOM (Coordinating Committee) des pays occidentaux regroupés à l'initiative des Etats-Unis en vue d'exercer un embargo sur les exportations d'une série de produits et de technologies militaires, nucléaires mais aussi, et surtout, civiles à double usage (civil et militaire) à destination de l'URSS, de la Chine et des autres pays communistes.

A ce titre, la Belgique a publié et tenu à jour pendant environ quarante ans une liste commune établie par le COCOM de produits et technologies soumis à contrôle, sous la forme d'un "*avis aux importateurs et exportateurs relatif aux produits et technologies soumis au contrôle de la destination finale*".

Par ailleurs, la Belgique participe à différentes initiatives internationales destinées à limiter la prolifération de certaines technologies et armes de destruction massive. L'ensemble de ces produits et technologies contrôlés est regroupé au sein d'une liste unique de contrôle des produits et technologies à double usage mise au point par les Etats membres de l'Union européenne ([24]). Cette réglementation européenne assure un contrôle harmonisé sur les exportations extra-communautaires tout en permettant la libre circulation au sein de l'Union de la quasi-totalité des produits et technologies à double usage.

---

23 Sénat - Questions et réponses 24 mars 1998 (bulletin n° 1-69) question n° 870/1

24 Règlement CE n° 3381/94 du Conseil, du 19/12/1994 instituant un régime communautaire de contrôle des exportations de biens à double usage.

A cette réglementation européenne, il faut ajouter l'Arrangement de Wassenaar du 19 décembre 1995, entré en vigueur en juillet 1996, qui regroupe trente-trois Etats, parmi lesquels les pays de l'ancien COCOM et certains autres pays industrialisés ou anciens membres du bloc de l'Est, comme la Russie, la Hongrie, la Pologne, la Slovaquie et la République tchèque.

Chacun de ces pays s'est engagé à ne pas autoriser l'exportation de biens ou technologies civiles à double usage ainsi que des matériels de guerre vers des pays dont *"le comportement irresponsable menace la paix et la sécurité internationale" (roge states).*

Il faut cependant souligner que le premier but de ces conventions internationales n'est pas la protection du potentiel scientifique et économique en soi. Elles ont été conçues plus en vue du maintien de la stabilité mondiale et de la non prolifération des armes de destruction massive que de la simple sécurité nationale. C'est la raison pour laquelle certains produits figurant sur ces listes n'ont aucune valeur de haute technologie.

La protection des intérêts économiques est prise en compte dans la loi du 11 avril 1994 *relative à la publicité de l'administration*. Les articles 4 et 5 de cette loi instituent et organisent le droit des particuliers de prendre connaissance d'un document administratif ou d'un document à caractère personnel d'une autorité administrative fédérale, de le consulter sur place, d'obtenir des explications à son sujet et d'en recevoir une copie. La demande de consultation doit cependant être rejetée lorsque l'intérêt de la publicité ne l'emporte pas sur la protection de certains intérêts collectifs parmi lesquels figurent *"un intérêt économique ou financier fédéral, la monnaie, le crédit public"* ainsi que *"le caractère par nature confidentiel des informations d'entreprises ou de fabrication communiquées à l'autorité"*.

Enfin, les secrets intéressant le potentiel scientifique et économique du pays peuvent désormais faire l'objet d'une classification au sens de la loi du 11 décembre 1998 *relative à la classification et aux habilitations de sécurité*.

Le titulaire d'une habilitation de sécurité qui, dans l'exercice de ses fonctions, utilise ou laisse utiliser *"de manière inappropriée"* des documents, informations ou matériels classifiés est passible de sanctions pénales. Cette infraction est sanctionnée qu'elle ait été commise de manière délibérée, ou par négligence grave ([25]).

4. 4. La protection du secret au sein des entreprises et des centres de recherches a pour conséquence une mutation des acteurs du secret.

Si donc le contenu du secret évolue, il en va de même aussi bien pour ses producteurs, que pour ses détenteurs, ses protecteurs et ... ses "prédateurs". Alors que le système classique de protection a d'abord été conçu en fonction d'un secret militaire ou d'un secret produit par l'autorité publique, géré par elle et ponctuellement confié à des personnes extérieures *"qui ont besoin d'en connaître"* pour participer eux-mêmes à l'action de cette autorité, la nouvelle réalité économique et stratégique bouleverse le contexte. Celui-ci se caractérise par la diversification et l'hétérogénéité croissante des acteurs, parmi lesquels les entreprises privées novatrices et à forte valeur ajoutée, les laboratoires, ainsi que leurs personnels qui, avec une logique autonome de profit, occupent à présent une place majeure, non seulement dans l'économie marchande, mais aussi dans la recherche scientifique, technologique, les services collectifs, la culture et les relations internationales.

---

25 Article 11 de la loi du 11 décembre 1998 *relative à la classification et aux habilitations de sécurité*.

Cette nouvelle situation a été partiellement prise en compte par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité puisque l'autorité compétente peut imposer la possession d'une habilitation de sécurité à des personnes morales ou physiques pour la passation et l'exécution de certains contrats ou marchés publics en rapport avec la Défense nationale, l'énergie nucléaire et la sécurité (article 12 alinéa 1). L'alinéa 2 du même article dispose : "*Dans les cas déterminés par le Roi, la présente loi s'applique également aux habilitations de sécurité demandées par des personnes morales ou physiques qui souhaitent obtenir une habilitation de sécurité en vue d'accéder à l'étranger à des informations, documents ou données, à des matériels, matériaux ou matières classifiées, à des locaux, des bâtiments ou des sites, dont l'accès est réservé au titulaire d'une habilitation de sécurité*". A cet effet, les entreprises titulaires d'une habilitation de sécurité doivent désigner un membre de leur personnel, lui même titulaire d'une habilitation de sécurité, pour remplir la fonction d'"*officier de sécurité*". Cette fonction consiste à veiller à l'observation des règles de sécurité dans l'entreprise.

4. 5. La difficulté de connaître l'ampleur du phénomène de l'espionnage économique.

Les responsables d'entreprises victimes d'actes d'espionnage économique hésitent souvent à porter plainte pour de tels faits. Ils craignent en effet la publicité négative qu'une telle affaire pourrait entraîner pour leurs firmes ainsi que la perte de confiance des clients, des fournisseurs, des actionnaires, etc....
Dans une enquête effectuée aux Etats-Unis en 1995 par le *National Counterintelligence Center,* 42 % des dirigeants d'entreprises interrogés ont déclaré qu'ils n'avaient jamais signalé de faits d'espionnage aux autorités alors même qu'ils se savaient victimes de tels actes. En outre, même si les responsables de grands groupes industriels reconnaissent qu'ils sont concernés par l'espionnage économique, il ne leur est pas facile de savoir de quelle manière des informations ont été obtenues à leur sujet. Il leur est particulièrement impossible d'affirmer que des marchés ont été perdus en raison d'écoutes et d'interception de leurs communications.

Selon l'avocat Fernand de Visscher, spécialiste du droit de la propriété industrielle, on trouve peu de cas d'espionnage industriel ou commercial dans la jurisprudence belge, la preuve de telles infractions étant difficile à apporter ([26]).

4. 6. L'approche américaine des secrets économiques et commerciaux.

L'espionnage économique et la manière de s'en prémunir sont des matières qui préoccupent le Congrès américain de manière intense. En 1996, celui-ci a adopté l'*Economic Espionage Act (EEA)* qui tend à réprimer l'appropriation indue des *trade secrets* (les secrets commerciaux) aussi bien par des services de renseignement ou gouvernements étrangers que par des concurrents nationaux.

Aux Etats-Unis, la manière de protéger les *trade secrets* diffère fondamentalement de la manière de protéger les secrets de la sécurité nationale. Ces derniers sont protégés par un rigoureux système de classification qui incrimine la possession même d'une information classifiée par une personne non habilitée, et ce, quelle que soit la manière dont elle a été acquise.

26 La Libre Belgique 16 janvier 2001 p. 15 : « *Que les espions lèvent le doigt ... »*

La particularité de l'*Economic Espionage Act* est de ne pas incriminer la prise de connaissance d'un secret commercial en soi; c'est seulement la manière déloyale, trompeuse ou malhonnête utilisée pour prendre connaissance (ou tenter de prendre connaissance) d'un tel secret qui peut l'être. Pour qu'une information soit considérée comme telle, elle ne doit pas être répandue dans le domaine public, elle doit être la source d'une valeur économique pour son détenteur et celui-ci doit avoir pris des mesures raisonnables pour la garder secrète. Ceci n'empêche donc personne de tenter de percer ou de comprendre le secret d'un concurrent pourvu que les moyens employés soient honnêtes (par exemple : par l'analyse de sources ouvertes). Ce système de protection des secrets commerciaux repose donc sur la responsabilisation des acteurs économiques eux-mêmes ([27]).

5. QUELQUES MANIÈRES DE COLLECTER LE RENSEIGNEMENT ÉCONOMIQUE, SCIENTIFIQUE OU INDUSTRIEL

L'information d'ordre économique, scientifique, technologique ou industrielle est devenue objet de recherche et même de prédation. La littérature relative à l'intelligence économique ou aux services de renseignement livre de nombreuses manières de recueillir ce type d'information, des plus classiques aux plus sophistiquées. La plupart des méthodes décrites consistent dans une recherche systématique des sources ouvertes, mais certaines s'apparentent néanmoins à de l'espionnage pur et simple. Les méthodes les plus classiques et brutales sont le vols de documents, la fouille des poubelles, la subornation de personnes, la corruption, le chantage, les menaces, etc.... Des techniques de manipulation peuvent également être mises en oeuvre, sans parler des technologies nouvelles. En voici quelques aperçus :

5. 1. La surveillance des scientifiques en voyage à l'étranger

Un rapport présenté le 25 juin 2000 par le "*General accounting Office*" (GAO) au Congrès des Etats-Unis a recensé 75 tentatives récentes d'espionnage à l'étranger sur des savants nucléaires américains. Ce rapport, basé sur le compte-rendu de centaines de voyages effectués par des scientifiques de par le monde expose des cas de mises sous écoute dans des hôtels, de fouilles d'effets personnels, ou bien encore d'offres de services de prostituées.

Le GAO recommande que les voyages de certains scientifiques à l'étranger soient soumis à l'autorisation préalable des services de contre-espionnage.

5. 2. Les chercheurs universitaires en stage à l'étranger

Les laboratoires universitaires peuvent aussi être la cible de services de renseignement. La technique consiste à y envoyer des étudiants boursiers ou des chercheurs stagiaires pour y recueillir des informations importantes d'ordre scientifique. Le séjour terminé, l'étudiant-chercheur rentre dans son pays d'origine où il sera soigneusement "débriefé" de ses connaissances techniques et scientifiques fraîchement acquises.

---

27 "*OSINT - An american legal and practical perspective"* by Richard Horowitz, attorney at Law, EUFIS - Brussels 19 october 2000.

Le monde académique se montre en général assez ouvert à la diffusion du savoir et à la coopération internationale, d=où la facilité pour n=importe quel chercheur de recueillir des informations sans même les avoir demandées. C=est la raison pour laquelle les services de sécurité devraient être attentifs à la présence de stagiaires étrangers dans des laboratoires de recherches de pointe.

5. 3. La prise de participation dans une société

Certaines entreprises engagées dans la veille technologique disposent de fonds d=investissement afin de prendre des participations dans des sociétés de haute technologie.

Une personne Aneutre@, agissant pour le compte d=une compagnie (ou d=un Etat) qui désire rester dans l=ombre, procède grâce à des sociétés-écrans et des relais à la prise de participation dans la société cible, par exemple lorsque celle-ci est fournisseur dans un secteur de pointe.

Cela permet d=avoir accès à des informations d=ordre technologique, éventuellement à du matériel classifié ou de vendre du matériel soumis à embargo.

5. 4. Le détournement de brevets d=invention

Le brevet entraîne le monopole d=exploitation d=un procédé ou d=une invention au profit de son inventeur mais il ne garantit aucunement sa confidentialité. Bien au contraire, la documentation contenue dans les brevets constitue une source ouverte extrêmement riche de renseignements. C=est d=ailleurs la raison pour laquelle certaines entreprises hésitent à déposer des brevets pour certaines de leurs inventions dont elles désirent garder le secret.

5. 5. Les faux appels d=offres

Un Etat fait savoir par des appels d=offres qu=il désire se rendre acquéreur d=une licence d=exploitation ou d=une usine livrée clé sur porte. Aussitôt sollicitées, les grandes sociétés réagissent en dépêchant sur place leurs ingénieurs commerciaux.

Les tractations traînant en longueur, les sociétés en lice fournissent de plus en plus d=informations sur leur offre sans y voir malice, espérant obtenir le marché. Elles livrent ainsi des renseignements qu=attendait le pays demandeur.

Une firme privée peut aussi agir de la sorte en se présentant, via un cabinet d=investigation, comme client potentiel.

5. 6. Les fausses annonces de recrutement

Les cabinets de recrutement peuvent aussi servir à la collecte de renseignements d'ordre économique. La méthode consiste à publier une annonce alléchante capable de retenir l'attention de cadres ou de chercheurs d'une entreprise cible. Les personnes intéressées par une meilleure proposition salariale, des conditions de recherche améliorées et divers avantages (appartement et voiture de fonction, indemnités diverses, etc.) expédient leur C.V. Celles-ci sont convoquées pour un entretien au cours duquel elles sont longuement interrogées sur leur qualification, leurs travaux antérieurs et actuels. Désireuses d'obtenir le poste, elles sont susceptibles de chercher à se faire valoir en livrant des informations confidentielles qui ne manqueront pas d'intéresser la société concurrente ou l'Etat caché derrière le bureau de recrutement.

5. 7. Les réseaux d'informateurs des entreprises

Certaines entreprises mettent sur pied de véritables réseaux de correspondants spécialisés chargés d'observer et de recueillir des renseignements de nature informelle, non structurée. Ils utilisent, pour transmettre leurs informations aux analystes, des formulaires standardisés aussi appelés "capteurs d'informations". Ce sont soit des "voyageurs" de l'entreprise, soit des représentants, qui par leurs contacts privilégiés avec les fournisseurs, les sous-traitants, les clients, peuvent obtenir de l'information fraîche sur les besoins, les projets, les évolutions des concurrents.

5. 8. La fréquentation des expositions, des colloques, congrès, foires et salons

Ces rassemblements d'experts constituent une source considérable d'information pour les professionnels de l'intelligence économique, ... et pour les espions. Les comptes rendus en sont systématiquement étudiés. Les prospectus intéressants sont récoltés pour être passés au scanner et introduits dans des banques de données. Des échantillons sont analysés, des pièces sont photographiées - parfois clandestinement -, des spécimens sont acquis (ou dérobés) pour être décortiqués. Les questions débattues en séances contiennent des informations très intéressantes, les conversations de couloirs, autour d'un "drink", également.

5. 9. L'interception des communications (COMINT) ([28]).

L'existence d'un réseau global d'interception des communications baptisé "Echelon" mis en place par les Etats-Unis et par les autres Etats membres de l'alliance UKUSA ([29]) a été médiatisée dès septembre 1998 par une série de rapports destinés au Parlement européen ([30]).

---

28 Le concept Comint (communication intelligence) est défini comme étant la collecte de renseignements effectuée par la surveillance des télécommunications et l'interception de leur contenu.

29 Il s'agirait d'une entente secrète de 1947 organisant la coopération entre les Etats-Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande en matière de renseignements.

30 Comité R, rapport d'activités 1999, titre II A. Chapitre 3.

Selon le quatrième rapport "*development of surveillance technology and risk of abuse of economic information (an appraisal of technologies for political control) - part 4/4*", ce système orienté à l'origine vers le bloc de l'est, aurait été détourné de sa finalité militaire initiale bien avant l'effondrement des régimes communistes. Le chapitre 5 intitulé "*Comint and economic intelligence*" contient quelques passages intéressants qui indiquent notamment : "*Comint involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunication became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments.(...) Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint*".

La législation des pays membres de l'alliance UKUSA autorise en effet leurs agences de renseignement ainsi que certains ministères à programmer la recherche de renseignements d'ordre économique ou commercial et à en recevoir par le recours au Comint.

Ainsi, la loi américaine *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique. Mais le rapport STOA cite plutôt des cas (sans en apporter la preuve, il est vrai) dans lesquels des firmes européennes auraient été évincées de marchés importants par suite de l'interception de leurs communications au cours de transactions commerciales internationales (Panavia European Fighter Aircraft consortium, Thomson CSF, Airbus industrie).

5.10. Les nouvelles technologies de la communication

L'espionnage s'attaque à présent aux techniques modernes de communications électroniques. Le piratage des fichiers informatiques, le cyberterrorisme, etc... sont des techniques susceptibles d'être utilisées en vue de saboter les infrastructures d'un Etat ou d'une entreprise. Des spécialistes de l'informatique fouillent en permanence des sites web d'entreprises concurrentes afin de forcer illégalement les réseaux et de saisir de façon frauduleuse toute une série de données précieuses. Il est également possible de récupérer un ordinateur portable et d'en tirer une copie du disque dur.

6. LE RÔLE DES SERVICES DE RENSEIGNEMENT EN MATIÈRE ÉCONOMIQUE (À L'ÉTRANGER)

6. 1. Généralités

Quelles actions et quels moyens un service de renseignement peut-il mettre en oeuvre pour protéger le potentiel scientifique et économique d'un pays ? D'autres pays que la Belgique ont confié à leurs services de renseignement la mission de protéger leur potentiel scientifique et économique. Cette mission peut se concevoir de manière défensive et de manière offensive.

Durant les longues années de la guerre froide, la préoccupation des services de renseignement était la recherche d'information macro-économique pour comprendre les grandes tendances de l'économie mondiale et anticiper ses évolutions. Les services de renseignement du monde entier ont déployé une part considérable de leurs activités à se poser des questions sur le fonctionnement des systèmes économiques dans les pays communistes. A lire la littérature consacrée à l'action de ces services à cette époque, ceux-ci n'auraient pourtant pas été en mesure d'apprécier correctement la situation économique de ces pays. Par exemple, le PIB de l'URSS, ses capacités de production et sa situation financière auraient été largement surévaluée, d'où l'incapacité de prévoir l'effondrement final du système communiste à partir de 1989.

Aujourd'hui, la nature de la prospective économique a changé. L'utilisation des services officiels de renseignement pour promouvoir les activités économiques de la nation est devenu une réalité. Des pays comme le Japon et les Etats-Unis concentrent leurs efforts sur des marchés et des zones à fort potentiel de croissance. Certains pays européens comme l'Allemagne et la France leur emboîtent le pas dans cette direction.

Le renseignement économique peut être recherché pour de multiples raisons d'ordre stratégique telles que, prévoir l'évolution des prix de certaines denrées, connaître à l'avance la position de certains pays dans des négociations commerciales, surveiller le commerce des armes, les technologies sensibles, évaluer la stabilité politique et économique d'un pays,
etc ...

6. 2. Le Japon

Au Japon, l'économie a pris rang de priorité absolue. C'est dès le milieu du XIX^{ème} siècle que ce pays a accordé au traitement de l'information technologique et industrielle une importance nationale, en la considérant comme une ressource à exploiter de manière collective. L'Etat nippon se consacre donc tout entier au service de ses entreprises et des priorités économiques, au point d'y consentir des efforts sans commune mesure avec ce qui se passe ailleurs dans le monde.

Certains ouvrages évaluent à 480 milliards de francs belges le budget de la recherche d'informations au Japon ([31]) essentiellement financé par le secteur privé. C'est ainsi que le ministère du Commerce et de l'Industrie (MITI - Ministry of International Trade and Industry) dispose d'une organisation spécialisée dans le renseignement économique et commercial, le JETRO (Japanese External Trade Organisation), qui entretient plusieurs dizaines de bureaux à l'étranger, pour l'essentiel voués à la recherche de l'information et, au-delà, du renseignement.

L'Agence des sciences et des techniques (STA), chargée de la recherche scientifique sous la tutelle du premier ministre, octroie de nombreuses bourses pour permettre à des étudiants japonais de poursuivre leurs études à l'étranger. Cette agence dispose d'un Centre de renseignement scientifique et technologique (le JICST). Les compagnies commerciales japonaises, qui emploient près de 60.000 personnes dans le monde, offrent également un cadre parfait pour le recueil d'informations, par le biais d'une infinité de contacts dans les pays où elles sont implantées. De très nombreuses entreprises disposent de leur propre système de collecte, extrêmement élaboré.

31 DST, police secrète - Roger Faligot et Pascal Krop - Flammarion

Cette stratégie de renseignement scientifique et technologique est coordonnée au plus haut niveau avec le service de renseignement du premier ministre, le *Naichô*. L'Etat japonais et les entreprises fonctionnent donc en parfaite symbiose.

6. 3. Les Etats-Unis

Il existe depuis 1977 un département de la NSA (*National Security Agency*) qui a pour mission de fournir des données au « *Departement of Commerce* » susceptibles d'être utilisées en vue de soutenir des intérêts économiques et commerciaux.

L'approche américaine est beaucoup moins centralisatrice et beaucoup plus libérale que celle du Japon. Un des objectifs actuels de la politique générale des Etats-Unis est de défendre et de promouvoir leurs intérêts économiques, publics et privés, partout dans le monde, dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Le débat est longtemps demeuré vif aux Etats-Unis entre les tenants de la thèse voulant que les services de renseignement mettent leur moyen au service des entreprises, et ceux qui optent pour une position plus conforme avec les principes libéraux exigeant que les affaires de l'Etat ne soient pas confondues avec celles du secteur privé. Dans la première hypothèse, le principal problème réside dans la manière dont les services et les entreprises doivent coopérer afin de ne pas favoriser certains industriels aux dépens d'autres, et de ne pas fausser le jeu normal de l'économie de marché.

Le débat sur cette question est devenu un thème central de discussion sur le rôle des services secrets dès la fin de la guerre froide.

En avril 1992, le directeur de la CIA Robert Gates, s'exprimant devant la Chambre des représentants, affirmait clairement son opposition à la pratique de l'espionnage économique et industriel ([32]). Cette attitude n'était cependant pas celle d'un de ses prédécesseurs, l'amiral Stanfield Turner, en poste de mars 1977 à janvier 1981 qui regrettait l'attitude timide de son service en cette matière : *"J'ai fait de gros efforts pour aider le monde américain des affaires; mais les professionnels de la CIA m'ont dit qu'il ne s'agissait pas là de dossiers intéressant la sécurité nationale"* ([33]).

Parvenu à la présidence des Etats-Unis, Bill Clinton a considéré la consolidation des zones d'influence commerciales américaines traditionnelles, de même que la conquête de nouveaux marchés, comme l'une des priorités de son mandat en matière de politique étrangère. En 1993, il a offert l'appui de la communauté américaine du renseignement aux compagnies privées en créant le "*National Economic Council"* parallèlement au "*National Security Concil*".

Aux Etats-Unis, le renseignement économique est donc considéré comme une composante essentielle de la sécurité nationale, bénéficiant d"une priorité équivalente à celle du renseignement diplomatique, militaire et technologique.

---

32 Washington Post, 14 mars 1993, cité par Jean Guisnel « Guerre dans le cyberespace », 1995

33 Time Magazine, 28 mai 1990, cité par Jean Guisnel « Guerre dans le cyberespace », 1995

En 1994, le directeur de la CIA, James Woolsey déclarait : *"Nous n'espionnons pas au profit de firmes privées. Mais nous portons les cas de corruption pratiquée par des étrangers à la connaissance de la Maison Blanche, du Département d'Etat et du ministère du Commerce, qui ensuite tentent de redresser la barre, souvent avec succès ».*

Le 14 juillet 1995, Bill Clinton a félicité chaudement la CIA d'avoir su découvrir des cas de corruption qui auraient permis de soustraire des milliards de dollars de contrats à des entreprises américaines. « *Votre travail a contribué à la prospérité américaine »* a-t-il déclaré.

En 1997, un ancien directeur adjoint de la CIA, John Gannon, devenu président du « *National Intelligence Concil »* a expliqué que les missions de renseignement économique sont de deux ordres :

- au plan stratégique, il s'agit d'alerter sur les tendances économiques internationales qui peuvent avoir un impact sur les intérêts américains; plus spécifiquement cela signifie anticiper les crises économiques, les menaces sur l'offre énergétique mondiale, évaluer les performances économiques de certains Etats, surveiller l'impact économique des sanctions internationales;

- au niveau tactique, il s'agit de fournir une information et une analyse sur les enjeux économiques importants aux responsables américains, en appui à leurs processus quotidiens de décision et à leurs interactions avec leurs homologues étrangers. Il convient notamment de "*s'assurer que tous les pays jouent avec les mêmes règles du jeu économique »*.

Les officiels de la CIA pensent donc qu'ils ne doivent pas mener directement des actions contre des firmes étrangères pour le compte d'entreprises américaines, mais qu'ils doivent contenir l'espionnage économique clandestin à des domaines tels que les négociations commerciales, la protection des firmes nationales contre la pénétration par des agents secrets étrangers et la mise à jour de corruption rendant difficile la compétition dans des nations en développement ([34]).

Le livre de Jean Guisnel « *Guerre dans le Cyberespace »*, paru en 1995, décrit pourtant quelques cas dans lesquels l'intervention des services de renseignement américains a sans doute permis à des firmes américaines de décrocher d'importants contrats internationaux. Parmi ceux-ci, on relève déjà les cas cités par Duncan Campbell dans son rapport présenté en février 2000 au Parlement européen sur le réseau « Echelon »([35]).

La discussion de ce rapport a d'ailleurs donné lieu à une nouvelle justification de la pratique du renseignement économique de la part des services de renseignement américains. En effet, James Woolsey, n'étant plus alors directeur de la CIA, a confirmé que son service avait bien surveillé des firmes européennes en compétition avec des firmes américaines au cours d'importantes transactions internationales et ce, parce que les européens auraient eu recours à la corruption pour obtenir les marchés convoités ([36]). Seuls les gouvernements étrangers faisant l'objet de ces manoeuvres auraient été avertis que les américains ne le prenaient pas à la légère. Et M. Woolsey de critiquer l'interventionnisme des gouvernements européens qui

---

34 Los Angeles Times, 15 juillet 1995 cité par Jean Guisnel dans « Guerres dans le Cyberespace », 1995

35 Les cas des firmes « Panavia European Fighter Aircraft consortium », « Thomson CSF » et « Airbus industrie » sont cités dans le rapport *STOA « development of surveillance technology and risk of abuse of economic information - part 4/4 »"*

36 Wall Street Journal, 7 mars 2000.

soutiennent, souvent de manière déloyale, leurs entreprises plus coûteuses et moins performantes que les entreprises américaines : « *it is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith* » lance-t-il à l'adresse des gouvernements européens.

Si ceux-ci voulaient bien réformer leurs économies étatiques, pour les conduire à plus d'efficacité et d'innovation, ils ne devraient plus avoir recours à la corruption et les américains n'auraient plus besoin de les espionner, conclut M. Woolsey. Mais s'il admet que la CIA pratique le renseignement économique, il affirme aussi que 95 % des informations collectées proviennent de sources ouvertes.

Il répète que son service n'est pas engagé dans des opérations d'espionnage économique au profit d'entreprises ou de sociétés américaines. Au cours de ces dernières années, la presse a cependant rapporté des cas d'agents américains (dont certains ayant le statut de diplomate) expulsés de pays européens sous l'accusation d'espionnage économique.

Le *Federal Bureau of Investigation* (c-à-d la police judiciaire fédérale) semble quant à lui jouer un rôle purement défensif en la matière. En 1998, un responsable de la sécurité nationale au FBI a affirmé lors d'une audition au congrès que les services de renseignement étrangers jouaient un rôle de premier plan dans l'espionnage industriel et économique au profit de leurs propres entreprises nationales, visant particulièrement les technologies de pointe, les brevets, mais aussi des informations confidentielles sur des contrats, des appels d'offre, des stratégies commerciales, etc.

Le 13 septembre 2000, « l'*International Economic Policy and Trade Subcommittee* » de la Chambre des représentants a organisé une nouvelle série d'auditions afin d'évaluer les évolutions de l'espionnage économique contre les entreprises américaines. Des cabinets d'investigation et d'intelligence économique américains ont d'ailleurs tenté d'estimer les pertes occasionnées à l'économie américaine par l'espionnage économique : les estimations oscillent entre 42 et 200 millions $ par an.

Le FBI surveille donc de manière particulièrement attentive les firmes de communication étrangères qui cherchent à s'implanter aux Etats-Unis. Le FBI redoute en effet que ces opérateurs étrangers ne profitent de leur contrôle sur des réseaux américains pour mettre sur écoute des entreprises pour le compte des services de renseignement de leurs pays. De même, le FBI surveille les opérations de prise de contrôle d'entreprises américaines par des groupes étrangers dans le cadre d'une loi fédérale qui permet au président des Etats-Unis d'interdire toute acquisition « *pouvant affecter la sécurité nationale ».*

Le *Economic Espionage Act* de 1996 permet au FBI et à d'autres agences fédérales de pratiquer des interceptions de communications à des fins de contre espionnage économique.

6. 4. Le Canada

Le "*Service Canadien du Renseignement de Sécurité* » (SCRS) a créé une structure spécialisée dans le conseil de contre-espionnage au profit des entreprises.

Dans son rapport d'activités de 1998, le Comité R avait relevé la difficulté qu'éprouvait le SCRS à circonscrire sa mission dans le cadre d'une définition trop large de la notion de sécurité économique.

Cette mission de sécurité économique se trouve décrite de manière plus précise dans une publication périodique éditée par ce service et intitulée « Série d'aperçus » (n° 6 de mai 1998).

Un des principaux objectifs du SCRS est de surveiller les activités menées au Canada par des officiers de renseignements étrangers, connus ou présumés, et d'empêcher des visiteurs, étudiants ou délégués étrangers soupçonnés d'activités de renseignement d'entrer au Canada.

Le mandat du SCRS en matière d'espionnage économique est d'enquêter sur les activités clandestines de gouvernements étrangers qui sont susceptibles de nuire aux intérêts économiques et commerciaux du Canada.

Le SCRS s'efforce de prévenir le gouvernement lorsque les règles du jeu équitables de la concurrence sur le marché libre sont délibérément infléchies contre le secteur industriel canadien.

Le SCRS ne s'intéresse pas à l'espionnage industriel, c'est-à-dire à l'espionnage exercé par une firme du secteur privé contre une autre. Lorsque ces activités sont de nature criminelle, ce sont les services d'application de la loi (law enforcement) qui enquêtent.

Le SCRS fait état d'un cas où un gouvernement étranger est soupçonné d'avoir intercepté des conversations téléphoniques entre un homme d'affaires canadien en voyage à l'étranger et le siège de son entreprise au Canada. Les canadiens avaient discuté en détail de négociations en cours, notamment d'une offre minimale précise. Le lendemain, la société concurrente étrangère a fait une contre-proposition correspondant à cette offre minimale.

Le SCRS précise plus loin que l'espionnage économique n'est pas seulement le fait de gouvernements traditionnellement hostiles au Canada, mais qu'il existe des signes que certains pays considérés comme amis s'y livrent également.

6. 5. La France

La loi du 16 juillet 1980 réprime notamment toute communication à une autorité publique étrangère, *"de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin » .* La définition que l'article 410 du nouveau code pénal (1992) donne des "*intérêts fondamentaux de la nation"* couvre explicitement « *les intérêts essentiels de son potentiel scientifique et économique ».*

La loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications prévoit des motifs qui justifient la conduite d'interceptions administratives de communications. Parmi ces motifs, on trouve le terrorisme, la criminalité organisée, la sécurité nationale, mais aussi la sauvegarde du potentiel économique et scientifique. Au cours de l'année 1999, 4.577 interceptions de sécurité ont été autorisées en France dont 186 à des fins de sauvegarde du potentiel économique et scientifique ([37]), soit 4 %.

La France a très tôt engagé ses services de renseignement dans des opérations d'espionnage et de contre-espionnage économique. Le fait que l'économie française se soit trouvée largement nationalisée après la Seconde Guerre Mondiale a joué très largement en ce sens.

37 Commission nationale de contrôle des interceptions de sécurité - 8ème rapport d'activité 1999

A la fin des années quatre-vingt, la Direction Générale de la Sécurité Extérieure (DGSE) a été impliquée dans différentes affaires d'espionnage économique aux Etats-Unis ([38]). Les pays anglo-saxons ne seraient pas ainsi les seuls à intercepter les télécommunications par satellites à des fins de renseignement économique.

Le livre de Jean-Jacques Cécile intitulé « *le renseignement français à l'aube du XXIème siècle* » ([39]) mentionne le cas d'une information d'ordre économique interceptée par la DGSE et qui aurait directement profité à l'industrie automobile française alors en concurrence avec une firme allemande pour l'installation d'une usine en Amérique latine. L'amiral Pierre Lacoste, directeur de la DGSE de 1982 à 1985, estimait pourtant que son service ne devait pas courir le risque d'être pris dans des opérations "agressives » contre des entreprises d'Etats amis ([40]).

Claude Silberzahn, directeur de la DGSE de 1989 à 1993, estime quant à lui que ce service ne peut agir au profit des entreprises : c'est l'Etat qu'il se doit de servir. Mais s'il est un domaine où les services de renseignement doivent pleinement jouer leur rôle au service de la collectivité, c'est celui de l'économie souterraine, illégale et parfois maffieuse, et de la finance criminelle ([41]). En 1991, la DGSE a donc créé un service spécialisé en matière de détection des flux financiers illicites. Ce service collabore avec Tracfin.

Un décret du Président de la République a créé le 1er avril 1995 un **Comité pour la compétitivité et la sécurité économique** (CCSE) d'abord placé sous l'autorité du Premier ministre, puis sous celle du ministre de l'Economie, des Finances et du Plan et dont le Secrétariat Général de la Défense Nationale (SGDN) assure le secrétariat. Composé de sept membres, le CCSE était chargé de mettre en oeuvre les recommandations du rapport « Martre » en matière d'intelligence économique. Ce Comité a cependant échoué dans sa mission et il a été mis fin à son existence en juillet 1998.

Un rapport de 1997 rédigé par le **Commissariat général du Plan** et intitulé « *de la défense économique à la sécurité de l'économie »* examine quels devraient être « *les leviers offensifs de l'Etat dans le domaine de la sécurité économique »*.

Il prône notamment le renforcement des pouvoirs du gouvernement afin qu'il puisse s'opposer à des acquisitions stratégiques, l'établissement de sanctions pénales en cas d'infraction au secret d'entreprise, la définition d'une politique nationale des normes et brevets, l'organisation d'un réseau de veille technologique et concurrentielle ciblé sur des thèmes stratégiques, le développement de stratégies d'influences offensives et enfin l'accroissement des capacités d'enquête de la Police judiciaire, des Renseignements généraux, de la DST et des Douanes en matière de criminalité économique.

La Direction de la Sécurité du Territoire (DST) a compétence pour rechercher et prévenir, sur le territoire de la République française, les activités inspirées, engagées ou soutenues par des puissances étrangères et de nature à menacer la sécurité du pays et, plus généralement, pour lutter contre ces activités.

---

38 Lire à ce sujet : Claude Silberzahn, »*Au coeur du secret »,* pages 172 et 173; Jean Guisnel, « *Guerres dans le cyberespace »* 1995;

39 Editions Lavauzelle, 1998 - chapitre 9, page 189.

40 Pierre Lacoste, « *les entreprises doivent apprendre à se protéger »,* Capital, février 1995.

41 Claude Silberzahn, *« Au coeur du secret »,* page 177.

Pour l'exercice de ses missions, et dans le cadre des instructions du Gouvernement, la DST est notamment chargée de participer à la sécurité des points sensibles et des secteurs clés de l'activité nationale, ainsi qu'à la protection des secrets de défense.

La DST comporte donc une sous-direction de la protection du patrimoine en charge des dossiers économiques et dont les effectifs ont été considérablement étoffés ces dernières années. La DST a pris pour habitude, depuis la fin des années quatre-vingt, de rencontrer des industriels afin de les sensibiliser à la nécessité de protéger leurs réseaux d'ordinateurs, de surveiller leurs stagiaires étrangers, et de se méfier singulièrement des étudiants venant de pays « amis ». La DST organise des conférences destinées aux cadres d'entreprises sur la manière de mieux protéger leurs secrets de fabrication, le produit de leurs recherches et leurs fichiers « clients ». Le service de protection du patrimoine de la DST offre aux entreprises en relation avec elle une liaison par Minitel leur permettant de s'enquérir des dernières évolutions en matière de menaces contre le tissu économique français.

D'une manière générale, l'agressivité accrue de pays étrangers, même partenaires économiques et politiques de la France, comme les Etats-Unis, le Japon ou l'Allemagne, fut la justification de ce repositionnement de la DST avant même l'effondrement de l'URSS;

Les relations sont aujourd'hui si étroites entre le monde de l'entreprise et les services français de renseignement que les plus grandes firmes liées aux domaines les plus sensibles - surtout dans le secteur de l'armement - recrutent régulièrement des fonctionnaires du contre-espionnage qui quittent le service de l'Etat. La Direction du Renseignement Militaire (DRM) développe également des relations avec les industries françaises.

Plusieurs universités et hautes écoles françaises se sont attachées à intégrer l'intelligence économique dans leurs programmes de cours et de formation, souvent avec l'aide, ou même à l'initiative d'anciens militaires et de responsables de la sécurité nationale.

Ainsi, l'Institut des Hautes Etudes de Défense Nationale (IHEDN) dépendant du ministère de la Défense nationale organise des cycles de cours sur la question; de hauts responsables des services de renseignement français y ont pris la parole.

Cet institut a entrepris de dresser un panorama complet des pratiques d'intelligence économique en France au moyen d'un questionnaire destiné à toutes les entreprises françaises occupant plus de 200 personnes ([42]).

L'Institut d'Etudes et de Recherches pour la Sécurité des Entreprises (IERSE) à Paris a pour vocation de fournir une formation universitaire en matière de sûreté des installations et d'intelligence économique à des cadres de haut niveau. Cet institut est le fruit d'un partenariat entre organismes publics et privés importants tels que l'Université de Paris I, la Gendarmerie nationale, la direction générale des douanes et droits indirects, le club de défense économique de l'entreprise et le mouvement des entreprises de France ([43]).

L'Ecole de Guerre Economique (sic) fondée en 1997, notamment par un général en retraite, « *propose un enseignement sur les méthodes d'attaque et de défense auxquelles sont confrontées les entreprises dans la compétition économique mondiale* ».

42 www.ihedn.fr

43 www.ierse.org

Le programme d'enseignement de cette école comporte notamment des cours sur la « stratégie d'utilisation de l'information », « l'approche professionnelle des sources ouvertes », « la guerre de l'information », les « parades contre la désinformation », le « cycle du renseignement », etc. ([44]).

On peut également citer l'Université Sophia Antipolis à Nice, les cours de l'amiral e.r. Lacoste (ex chef de la DGSE) à l'Université de Marne-la-Vallée, etc... .

6. 6. L'Allemagne

Selon Henri Martre, rapporteur pour le Commissariat général du Plan français ([45]), le système d'intelligence économique le plus performant en Europe est le modèle allemand. Celui-ci s'appuie avant tout sur un profond sentiment collectif de « patriotisme économique » et un consensus sur la notion d'intérêt économique national. Cette culture est un des atouts de la compétitivité allemande.

Le *« Bundesnarichtendienst »* (BND), c'est-à-dire le service de renseignement extérieur de la RFA, serait le centre vers lequel converge l'ensemble des flux d'informations économiques ([46]). Le gouvernement allemand considérant l'Asie comme une zone prioritaire en termes stratégiques pour le redéploiement des forces, tant sur le plan économique que sur celui du renseignement, ce n'est pas un hasard si le BND a ouvert des postes à New Delhi, à Pékin, à Djakarta, à Tokyo, à Manille, à Séoul et à Taiwan.

Le BND a mis en place une banque de donnée pour les entreprises qui s'implantent dans ces régions du monde ([47]). Le BND rédige des rapports à l'intention du ministère fédéral de l'Economie, notamment pour inviter les industriels allemands à la vigilance dans leurs relations avec certains pays cherchant à acquérir des systèmes de haute technologie.

Il existe aussi un organisme fédéral chargé de coordonner les initiatives dans le domaine de l'intelligence économique : l' « *Arbeitsgemeinschaft für die Sicherheit des Wirtschaft »* (ASW). Cet organisme entretient des contacts avec le service fédéral de renseignement, le *« Bundesampt für Verfassungsschutz »* (l'office de protection de la Constitution ou BfV). Selon un rapport du BfV de 1997, 62 % des affaires d'espionnage mises à jour en Allemagne concernent le potentiel scientifique et économique du pays, 19 % concernent des affaires politiques et administratives, 8% se situent dans le domaine militaire et 11 % dans d'autres secteurs. Des activités d'espionnage commanditées par des services de renseignement russes à l'encontre d'entreprises privées allemandes seraient en nette augmentation. Le rapport annuel du BfV de 1999 confirme que les activités du service de renseignement extérieur russe, le SVR, ainsi que des pays de la CEI sont principalement orientées vers l'espionnage économique, scientifique et technique.

---

44 www.ege.escala.fr

45 Rapport de Henri Martre : *Intelligence économique et stratégie des entreprises,* la documentation française

46 DST, police secrète - Roger Faligot, Pascal Krop - Flamarion

47 *Une approche française de l'intelligence économique* - Christian Harbulot - novembre 1995

Dans un entretien accordé au mensuel français « *Le Monde du Renseignement* » ([48]), M. Peter Frisch, le chef du BfV déclare que la notion de « *patrimoine économique stratégique* » a conduit une partie des 2218 agents du BfV à choisir certaines entreprises afin de développer des collaborations avec elles.
A ce jour, elles sont 1600 à avoir établi des partenariats avec le BfV au niveau fédéral. Dans chacune d'elles, un salarié assure des fonctions de délégué à la sûreté économique et de correspondant pour le service de renseignement. Les sociétés concernées appartiennent, non seulement à l'industrie de l'armement, mais aussi à la construction automobile, à la pétrochimie et aux secteurs des hautes technologies. Ce dispositif est doublé par un réseau régional, avec de semblables partenariats gérés par les *« Landesamt fûr Verfassungsschutz »*, c'est-à-dire les services de renseignement des länders.

6. 7. La Grande-Bretagne.

La législation anglaise assigne une mission de protection de l'intérêt du bien-être économique du Royaume-Uni tant pour le Security Service (act 1989) que pour « *The Secret Intelligence Service (act 1994 »)* ([49]). Aucune des deux lois ne définit le concept de bien-être économique (*economic well being)*. Le « *Government Communications Head Quarter » (GCHQ)* est spécialement chargé par la loi d'intercepter des communications étrangères pour le compte du gouvernement, notamment « *... in the interest of the economic well-being of the United Kingdom ... in relation to the actions or intentions of persons outside the British Islands ».* Des cibles économiques et commerciales peuvent être désignées par le *« Overseas Economic Intelligence Committe »* du gouvernement, par la section économique du « *Joint Intelligence Committee »* et même par le Trésor et la Banque d'Angleterre.

Les ministres concernés doivent désigner les entreprises clés pour l'économie britannique. Ils donnent des directives par le canal du « *Joint Intelligence Committee »* (JIC).

Ils demandent, par exemple, aux services de renseignement de s'informer sur la manière dont le prix du pétrole va varier de manière à permettre au ministre d'adapter sa politique financière. Les services de renseignement travaillent donc pour l'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.

---

48 Le Monde du Renseignement n° 375, 3 février 2000.

49 Cfr; A*Etude de la législation du Royaume-Uni relative aux services de renseignement et de sécurité*@, rapport annuel d=activités du Comité R 1998.

6. 8. Les Pays-Bas.

Jusqu'il y a peu, les Pays-Bas ont disposé d'un service de renseignements extérieurs, *de inlichtingendienst buitenland (IDB)*, dissout en 1994. Selon Bob de Graaf et Cees Wiebes, auteurs d'un ouvrage intitulé « *Villa Maarheeze* » ([50]), l'IDB possédait une section économique chargée de collecter des renseignements en faveur du ministère des Affaires économiques, de l'Agriculture et de la Pêche. Le recueil du renseignement s'effectuait principalement via des hommes d'affaires néerlandais voyageant ou séjournant à l'étranger. L'IDB entretenait aussi des contacts avec la direction des grandes entreprises hollandaises avec lesquelles il échangeait des informations d'ordre économique de première importance.

Selon de Graaf et Wiebes, l'IDB aurait intercepté des offres commerciales étrangères transmises par télécommunications pour les communiquer à des entreprises nationales.

Après la dissolution de l'IDB, ses opérations ont été transférées au *Binnenlandse Veiligheids Dienst* (BVD, homologue néerlandais de la Sûreté de l'Etat), dont les missions légales ont été définies comme suit :

- collecter des renseignements sur des organisations et personnes qui, par les buts qu'elles se fixent ou par leurs activités, permettent de supposer sérieusement qu'elles représentent un danger pour la démocratie, la sécurité ou pour d'autres intérêts vitaux de l'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 inclut la protection de l'économie nationale. Dans ce cadre, le BVD enquête sur les activités des services de renseignement étrangers dirigées contre les intérêts économiques des Pays-bas. Dès sa création le BVD a rempli une mission de sécurité, particulièrement à l'égard des entreprises travaillant pour l'armée et de celles qui pourraient être victimes de sabotage. La loi hollandaise sur les services de renseignement autorise le BVD à attirer l'attention des entreprises sur les mesures de protection à prendre. Ce service peut également signaler certaines formes de concurrence illicite. En 1994, la mission du BVD relative au domaine économique a été redéfinie comme suit par un groupe « Economische Veiligheidsbelangen » (Intérêts de sécurité économique) associant le ministère des Affaires économiques et des représentants d'entreprises.

1. Les entreprises disposent d'un éventail important d'informations qui sont la proie de l'espionnage économique;

2. des marchés ne sont pas obtenus par les firmes néerlandaises car les concurrents étrangers de ces firmes utilisent des moyens peu avouables tels que des écoutes ou des informateurs pour gagner ces marchés;

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

---

50 *Geschiedenis van de inlichtingendienst buitenland - Sdu uitgeverij, Den Haag - 1999.*

Il a donc été décidé que les activités du BVD devaient porter sur ces trois menaces spécifiques. Le BVD s'occupe aussi de menaces telles que :

- le recueil par des services de renseignement étrangers de données économiques essentielles concernant des firmes néerlandaises;
- le lancement de campagnes de presse calomnieuses dans le but de discréditer des entreprises néerlandaises.

Le ministre de l'Intérieur a établi une liste confidentielle des entreprises présentant un intérêt vital pour les Pays-Bas et dont le BVD doit assurer la protection.

Les Pays-Bas semblent donc avoir adopté une politique purement défensive mais qui associe de manière active le monde économique et le monde politique.

6. 9. La Russie et les pays de la Communauté des Etats Indépendants.

En avril 1994, le président de la Fédération de Russie, M. Boris Eltsine a tenu un discours à l'intention des responsables et des collaborateurs des services de renseignement extérieur de son pays (SVR et GRU) dont l'extrait suivant est très clair au niveau des objectifs qui leur étaient assignés : *« Ce que nous attendons du Renseignement extérieur, ce sont des informations indispensables à l'adoption par l'Etat de décisions capitales touchant à la politique étrangère et intérieure de la Russie, à la mise en oeuvre de nos orientations économiques et du progrès scientifique et technique ».*

Le rapport d'activités du service de renseignement allemand « *Bundesamt für verfassungsschutz* » (BfV) pour l'année 1999 donne quelques informations sur les activités de renseignement économique et scientifique auxquelles se livrent les services de renseignement russes, ukrainiens et bellarusses. Selon ce rapport, la collecte de renseignements d'ordre économique, scientifique et technique occupe à présent la première place dans les priorités de ces services.

Le SVR, service de renseignement extérieur russe, occupe environ 15.000 personnes. Selon son attaché de presse, ce service a reçu pour mission de créer à l'étranger des conditions favorables pour les intérêts économiques russes en vue d'attirer des investisseurs étrangers vers ce pays.

Pour collecter leurs informations, les services de renseignement russes font usage aussi bien de sources ouvertes, que de moyens humains et techniques clandestins, tels que l'interception des communications. Comme sources ouvertes, ils utilisent la littérature, les bibliothèques, les banques de données, l'internet, ils visitent des foires et missions commerciales, ils fréquentent des colloques et conférences et essayent d'y nouer des contacts intéressants. Pour le recueil clandestin de renseignements, les services russes utilisent des officiers de renseignements envoyés sous couvertures dans leurs ambassades et consulats, dans des agences de presse, dans des firmes d'Etat ou dont la majorité du capital est détenue pas des citoyens russes.

Toujours selon le BfV, le FSB (le service de renseignement intérieur) surveille à l'intérieur du pays les membres des ambassades et des postes consulaires étrangers, les hommes et femmes d'affaires venus en visite en Russie ainsi que les cadres et le personnel des firmes étrangères établies dans ce pays.

6. 10. Autres pays (en bref).

La Chine populaire : l'académie des sciences chinoise offre chaque année des bourses à de nombreux professeurs d'universités, responsables de laboratoires et chefs de recherches de pays étrangers pour qu'ils s'associent à des plans de recherches chinois. (Source : « *Le Monde du Renseignement* » n° 338 02/07/1998).

La section renseignement et contre espionnage économique et financier du ministère de la sécurité chinoise (« Guoanbu ») a notamment reçu pour mission d'empêcher les étrangers de se procurer l'information économique qui n'a pas été préalablement triée par les autorités. Ce tri est effectué conjointement par le Guoanbu, le ministère du commerce extérieur et de la coopération économique et le département de propagande du Comité central du parti communiste chinois. (Source : LMR n° 304 30/01/1997).

La Chine nationaliste est elle aussi considérée comme l'un des pays les plus efficaces en renseignement économique. (Source : LMR n° 356 08/04/1999).

La Suède : plusieurs entreprises suédoises pratiquent l'Intelligence économique en toute discrétion depuis le début du siècle. Ceci peut expliquer leurs succès commerciaux dans le monde. L'université de Lund s'est spécialisée dans cette matière.

Israël : les services de renseignement français redoutent l'efficacité commerciale des entreprises israéliennes d'intelligence économique ou de sécurité informatique implantées à Paris. Certaines de ces sociétés comptent parmi leurs cadres des anciens membres du Mossad (LMR n° 392 - 26/10/2000).

7. LES SOCIÉTÉS COMMERCIALES SPÉCIALISÉES EN INTELLIGENCE ÉCONOMIQUE

7. 1. Généralités.

De plus en plus nombreuses sont aussi les sociétés privées qui se spécialisent au profit de grands groupes industriels, (notamment de l'armement) dans l'intelligence économique ou dans l'investigation financière. Certaines d'entre elles procèdent pour le compte de leurs clients à de véritables enquêtes de sécurité préalables à l'embauche de personnes.

Elles peuvent aussi procéder à des enquêtes financières en cas de soupçons de fraudes, de détournements, d'OPA inamicale, etc. Les animateurs de ces sociétés ont, eux aussi, souvent appartenu à des services de police ou de renseignement avant de se reconvertir dans le renseignement économique. Aux Etats-Unis, la NSA et la CIA ont en effet encouragé la reconversion d'une partie de leur personnel vers le secteur privé.

Il existe un "Annuaire Européen des Professionnels de l'Intelligence Economique" édité par la "Société d'Intelligence Economique et Concurrentielle Appliquée" (SIECA). Ce manuel se veut exhaustif mais certaines sociétés ont néanmoins refusé d'y figurer.

On peut distinguer sept catégories de prestations en rapport avec l'intelligence économique :

- les détectives privés;
- le renseignement commercial;
- les cabinets d'audit
- les cabinets de veille technologique;
- les sociétés d'intelligence économique;
- les intermédiaires;
- le lobbying.

Néanmoins, ce monde des sociétés et cabinets d'intelligence économique est fort disparate et en constante évolution. Il convient donc d'éviter de donner aux sociétés ainsi désignées une définition trop formelle.

Les sociétés privées d'investigation et de sécurité suivent en effet les mêmes évolutions que les grands cabinets d'audit. Elles élargissent leurs gamme de services, s'affranchissent des limites de leur métier d'origine et opèrent de multiples fusions, acquisitions ou séparations. Les groupes majeurs qui semblent se dessiner aujourd'hui sont pour la plupart américains.

On peut notamment citer :

- *Pinkerton*, détenu par le groupe suédois *Securitas AB,*
- *Kroll Associates,* qui s'est récemment séparé de *O'Gara,* et qui a été repris par *Blackstone Capital Partners III (BCPIII),*
- *Decision Strategy Fairfax Group (DSFX)*,
- la firme britannique *Control Risks Group (CRG).*

Certaines de ces firmes ont leur siège en Europe (Paris, Londres, etc.). La firme *Control Risks Group* dispose d'une agence à Anvers.

Certaines firmes éditent des rapports d'analyse de risques contenant des informations pointues et précises pour les industriels qui désirent investir à l'étranger. Il s'agit de rapports portant sur la situation politique, sociale et économique des pays visés, sur les intérêts des groupes rivaux, sur les menaces terroristes, les pratiques de corruption, sur l'influence des groupes criminels ou celle des groupes de pression. Ainsi, par exemple, le rapport "*2000 Outlook*" de la firme "*Control Risks Group*" se penche sur les mouvements de protestation contre la mondialisation, avec l'hypothèse que l'un d'eux pourrait basculer un jour dans l'action violente contre les multinationales. Ce rapport indique même des cibles potentielles ainsi que des dates auxquelles des activistes pourraient entrer en action.

Il existe également des sociétés qui offrent sur le marché des services destinés à identifier et à suivre tous les auteurs de campagnes de dénigrement sur l'internet, cette nouvelle forme d'activisme dirigée quelquefois contre des industries ou certains secteurs d'activités. L'une de ces sociétés, établie aux USA, s'est proclamée "*the premier internet intelligence agency*". Leurs prestations se basent sur des logiciels de recherche sur l'internet, effectuant des passages dans les "newsgroups" et sur certains sites. Ainsi, une firme française "*Net Intelligenz*" surveille, étudie et analyse tous les forums et conversations entre internautes pour le compte de ses clients. Grâce à un logiciel très puissant, l'agence peut, tel un moteur de recherche, analyser l'ensemble des lieux de conversation virtuels pour y dénicher des mots ou des expressions-clés.

Cette masse de données est traitée par des scientifiques, sociologues, sémiologues qui en font une analyse ciblée selon la demande du client.

On voit aussi apparaître dans l'organigramme de certaines entreprises multinationales, notamment chez les industriels de l'agro-alimentaire, des secteurs énergétiques (pétrole, nucléaire, etc.), des compagnies aériennes, etc., des cellules de décisions appelées *"war rooms"*. Celles-ci sont chargées de gérer les crises, de répondre aux conséquences d'accidents industriels de plus en plus fréquents, de contrer les attaques de la concurrence, mais aussi de maîtriser l'information à caractère stratégique de l'entreprise et de s'attaquer à la conquête de nouveaux marchés. Certaines de ces *"war rooms"* sont animées par d'anciens membres de services de police ou de renseignement.

Une nouvelle forme de surveillance du personnel sur les lieux de travail apparaît enfin aux Etats-Unis et en Grande Bretagne. L'on y voit en effet des grandes firmes mettre en place des équipes d'enquêteurs informatiques chargés de copier les disques durs des salariés, à leur insu, et de les passer au crible pour trouver, soit d'éventuelles fautes commises au travail, soit des preuves informatiques de vols de secrets industriels. Ces spécialistes se servent d'outils informatiques et de techniques conçus à l'origine pour l'usage des services de police ou de renseignement.

Les législations américaines et britannique permettent aux employeurs de recourir à cette *"médecine légale informatique"* qu'ils justifient par la nécessité de se défendre.

7. 2. La nécessité d'un débat juridique et d'un contrôle sur l'activité des sociétés de renseignement privé.

Dans son plan de sécurité ([51]), le gouvernement fédéral constate la tendance à de plus en plus faire appel à des acteurs privés dans le domaine de la sécurité (entreprises et services internes de gardiennage, de sécurité, détectives privés, etc.). Dans certains domaines de sécurité très concrets, il existe même une coopération et une concertation entre les acteurs privés et les autorités.

Si certains pans de l'activité des firmes de renseignement économique sont régis par la loi du 19 juillet 1991 organisant la profession de détective privé (cette loi vise notamment le recueil par des personnes physiques d'informations relatives à l'état civil, à la conduite, à la moralité et à la solvabilité de personnes, ainsi que la recherche d'activités d'espionnage industriel), qu'en est-il par exemple de l'exploitation systématique de banques de données ? Il existe aussi une loi du 10 avril 1990 sur les entreprises de gardiennage et de sécurité, mais elle ne vise que leurs activités de surveillance et de protection physique des biens et des personnes.

La nécessité d'un débat juridique et d'un contrôle sur la légalité des activités privées d'intelligence se fait donc plus pressante à mesure que les offres de renseignement économique privé se multiplient. Même l'exploitation des sources ouvertes, c'est-à-dire celle pratiquée à partir d'informations accessibles au public, n'exclut pas le respect de certaines règles de droit ([52]).

---

51 Sénat (2-461/1) et Chambre des représentants (doc 50 0716 / 001) - 13 juin 2000.

52 Ainsi par exemple, la Commission de la protection de la vie privée a récemment estimé que le traitement de données personnelles tirées de la consultation et de l'exploitation systématique d'informations jurisprudentielles diffusées par des moyens électroniques tombait sous le coup de la loi. *« La possibilité, à partir de banques de données jurisprudentielles centralisées, voire exhaustives, de retrouver l'historique judiciaire d'une personne, engendre des risques en matière de protection des données sans commune mesure avec ceux liés aux modes traditionnels d'accès ou de publication de la jurisprudence »* (décision n° JZ97CN3-1 du 23/12/1997).

Comme le souligne le plan fédéral de sécurité, A*afin de soumettre les acteurs privés de la sécurité à un contrôle démocratique, il convient de voir si les Comités permanents de contrôle des services de police et de renseignements peuvent apporter leur contribution en la matière dans les limites de leur mission légale*@.

Le Comité R estime en effet qu=un contrôle de l=autorité est indispensable sur la pratique du renseignement économique par des firmes privées. Selon le Comité, cette mission de contrôle incombe en premier ressort aux services du gouvernement fédéral. Une part de ce contrôle entre notamment dans la mission de protection du potentiel économique et scientifique confiée à la Sûreté de l=Etat. S=il entrait dans les intentions du Parlement d=associer le Comité R à cette nouvelle mission, cela nécessiterait une adaptation de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, car celle-ci ne lui donne aucune compétence pour contrôler directement l=activité des sociétés de renseignement économique.

8. LE RÔLE DES SERVICES DE RENSEIGNEMENT BELGES EN MATIÈRE DE PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE : CONSTATATIONS DU COMITÉ R

8.1. Les attentes et les propositions des milieux économiques belges

En 1986, peu après les attentats des CCC, un groupe de travail de la Fédération des entreprises de Belgique (FEB) s=est mis en place pour édicter des lignes directrices de sécurité aux chefs d=entreprises. En 1994, des experts en sécurité de divers secteurs industriels et d=entreprises ont créé une A*Plate-forme de concertation permanente pour la protection des entreprises*@ (PCPE). Les secteurs les plus concernés étaient notamment la distribution, l=alimentation, la chimie, Fabrimetal, Sabena, Belgacom, le secteur pétrolier, les banques, les assurances, le secteur sidérurgique et l=industrie du tabac. Les experts en sécurité de ces secteurs se sont penchés sur tous les aspects de la protection des entreprises contre les risques d=origine criminelle. Des contacts ont été établis avec les autorités publiques et leurs services compétents, notamment la Sûreté de l=Etat et le SGR.
En 1995, la PCPE a adressé à ces autorités un mémorandum exprimant les attentes et les propositions des milieux industriels belges en matière de sécurité des entreprises. Ce document a été réactualisé en juin 2000. L=espionnage économique y apparaît comme l=une des préoccupations majeures de la FEB parmi lesquelles on trouve aussi les attaques armées, les vols, les agressions violentes et les attentats.
La FEB appelle à une redynamisation de la concertation entre pouvoirs publics et secteur privé, elle plaide pour une A*gestion intégrale de la sécurité*@ et formule des propositions, parmi lesquelles deux concernent directement les services de renseignement :

- la création au sein du ministère de la Justice d=une structure permanente de contact avec le secteur privé : A*Cette structure, composées de représentants des services de police, <u>des services de renseignement</u> et de la magistrature, devrait informer régulièrement la FEB, quant aux menaces pesant sur les entreprises et définir les projets de coopération entre le public et le privé*@. L=objectif est ici d=analyser en permanence les formes de criminalité qui constituent une menace contre les entreprises.

- *"l'organisation de cours et cycles de formation <u>pour le personnel dirigeant</u> des services de police, <u>des services de renseignement</u> et de la magistrature, consacrés à l'organisation de l'entreprise et aux formes de criminalité dont les entreprises sont victimes."* Pour la FEB, le personnel de ces services manque en effet d'expertise dans les domaines de la criminalité touchant les entreprises; il doit donc pouvoir disposer d'une formation adéquate axée sur la réalité des entreprises. *"Il s'indique, par ailleurs, de mettre des "techniciens" à la disposition des services de police et/ou des parquets pour des enquêtes spécifiques visant le potentiel technologique et économique de notre pays".*

Dans son plan de sécurité de juin 2000, le gouvernement fédéral déclare que les ministres de la Justice et de l'Intérieur poursuivront la concertation mise en place au sein de la PCPE et qu'un groupe de travail mixte chargé de la criminalité économique devra prêter attention aux modes criminels suivants : criminalité informatique, blanchiment d'argent, corruption et espionnage économique.

8.2. La Sûreté de l'Etat

Le Comité R s'est demandé comment la Sûreté de l'Etat concevait et préparait sa nouvelle mission de protection du potentiel scientifique et économique. S'agit-il pour ce service d'une approche active de l'intelligence économique au profit des entreprises belges (veille technologique, concurrentielle, lobbying, exploitation des sources ouvertes, ...) ou bien d'une démarche sécuritaire avec sensibilisation au phénomène de l'espionnage économique ainsi qu'aux mesures de sécurité pour s'en prémunir. Dans l'un ou l'autre cas, quels sont les moyens humains affectés à cette mission, les méthodes de travail mises en oeuvre, les relations de la Sûreté de l'Etat avec les entreprises, avec les universités, etc ... ?

A. Historique de l'intérêt que porte la Sûreté de l'Etat à la protection du potentiel scientifique et économique.

Pendant la guerre froide, les services de renseignement belges se sont cantonnés aux implications militaires éventuelles du transfert de hautes technologies dans le strict respect des directives prescrites par le comité COCOM (exemple, l'affaire Pégard).

C'est en 1986 que commencent des pourparlers entre des représentants de la Sûreté de l'Etat et le Directeur général du département de la recherche scientifique du ministère des Affaires Economiques. C'est de cette époque que datent les premiers contacts de la Sûreté de l'Etat avec la Fédération des Entreprises de Belgique (FEB). Une conférence a alors été donnée par des membres de la Sûreté de l'Etat à quelques dizaines d'industriels. Ce premier effort de sensibilisation ne semble cependant pas avoir été suivi d'effets.

Jusqu'en 1998, la protection du patrimoine scientifique et économique du pays ne figurait pas comme telle parmi les sujets de préoccupation de la Sûreté de l'Etat. Néanmoins, dans le cadre de la lutte contre la prolifération d'armes N.B.C. ([53]), ce service a toujours recueilli et analysé des renseignements en vue d'empêcher l'exportation de matériel ou le transfert de technologies sensibles à destination de pays jugés "à risques", d'organisations maffieuses ou terroristes.

53 Armes N.B.C. = armes nucléaires, bactériologiques et chimiques.

C'est dans ce cadre que la Sûreté de l'Etat a établi ses premiers contacts avec des firmes commerciales, des universités et des centres de recherche.

Entre 1995 et 1997, la Sûreté de l'Etat a pris part aux travaux de la "*Plate-forme permanente de concertation pour la protection des entreprises"* (PCPE) mise en place par la Fédération des Entreprises de Belgique (FEB) suite au mémorandum sur la sécurité des entreprises. Plusieurs réunions officielles de concertation entre les autorités publiques et le monde des entreprises ont eu lieu, notamment deux tables rondes mettant en présence représentants de la FEB et les ministres de la Justice et de l'Intérieur. Ont également participé à cette concertation les procureurs généraux, les magistrats nationaux, ainsi que des responsables de la police et de la gendarmerie. Le but de ces réunions était de réaliser un échange d'informations amélioré entre les entreprises privées et certaines instances officielles en charge de la sécurité.

A la suite de ces réunions, des briefings ont été donnés par la Sûreté de l'Etat à la FEB sur le fonctionnement de ce service et concernant les sectes. Par manque de personnel et de moyens, ces contacts sont toutefois restés sporadiques et aucune des initiatives prises n'a vraiment été menée à son terme. Depuis 1997, les contacts officiels entre FEB et autorités ont cessé au sein de la PCPE. Des réunions se sont poursuivies dans ce cadre, mais seulement en présence d'experts privés de la sécurité des entreprises.

Le 9 octobre 1999, le journal "*De Financieel Economische Tijd*" publie une interview de Monsieur B. Van Lijsebeth, devenu Procureur du Roi à Anvers, dans lequel celui-ci évoque l'espionnage économique et industriel qu'il qualifie de *"guerre oubliée".* Il estime qu'il faut compter en cette matière avec les services de renseignement étrangers. A cette date, les services extérieurs de la Sûreté de l'Etat ont déjà produit une dizaine de rapports d'information depuis le début de l'année 1999. Interpellé au sujet de l'interview précitée, le ministre de la Justice a questionné la Sûreté de l'Etat. Ce service lui a fait savoir qu'il n'existait aucune preuve concrète que des services de renseignement et de sécurité étrangers soient, en ce moment, actifs en Belgique sur le plan de l'espionnage économique ou industriel. Néanmoins, des sources ouvertes font état de la réorientation de l'activité des services de renseignement de l'espionnage militaire vers l'espionnage économique.

En 1997 et 1998, la Sûreté de l'Etat a informé le ministre de la Justice que l'ambassade de Cuba à Bruxelles recherchait des informations universitaires de nature économique, mission pour laquelle cette ambassade avait même recruté du personnel([54]).

Le 28 octobre 1999, le ministre de la Justice a annoncé qu'un membre de son cabinet participerait à la plate-forme de concertation permanente sur la sécurité industrielle. Cette intention a été confirmée par le plan fédéral de sécurité. Ce forum devrait pouvoir mettre en oeuvre un plan de collaboration entre la Fédération des Entreprises de Belgique et les pouvoirs publics. Selon le ministre, c'est dans ce cadre que la Sûreté de l'Etat pourra jouer un rôle proactif.

[54] Chambre 28/10/99 - réponse du ministre de la Justice à l'interpellation n° 84 de M. Bourgeois.

B. Les actions entreprises par la Sûreté de l'Etat.

Les actions antérieures à la loi organique du 30 novembre 1998.

Une série de documents préalables à l'adoption de la loi organique du 30 novembre 1998 témoignent de la volonté de l'Administrateur général de la Sûreté de l'Etat de préparer son service à l'exercice de la nouvelle mission de protection du patrimoine scientifique et économique. Les documents intéressants à cet égard sont les suivants.

S Dans une note adressée le 25 mars 1997 au secrétaire général du ministère de la Justice, M. Van Lijsebeth évalue les besoins futurs du cadre des services extérieurs pour l'exercice des missions décrites par le projet de loi organique des services de renseignement et de sécurité.

- Une note de travail datée du 5 février 1998 décrit la nouvelle mission de protection du potentiel économique et scientifique qu'entend confier à la Sûreté de l'Etat le projet de loi organique des services de renseignement et de sécurité. Ce document a été transmis au ministre des Affaires économiques.

  La menace de l'espionnage économique et scientifique est décrite comme suit : *"Les effets de l'espionnage économique et scientifique se manifestent très concrètement par la perte de contrats importants, de marchés, d'emplois, par le vol de nouvelles technologies... Les pertes imputables à l'espionnage sont difficiles à chiffrer car les victimes de l'espionnage acceptent rarement de les dénoncer. On peut cependant affirmer, notamment sur base de ce qui a été découvert dans d'autres pays européens, que le coût de l'espionnage économique est considérable pour les entreprises et pour l'économie du pays. Des répercussions importantes se font sentir dans les secteurs de la défense et des technologies avancées, dans le domaine de la recherche et au niveau de la politique étrangère.*

  L'espionnage économique et scientifique, favorisé par la croissance de la concurrence économique, constitue donc non seulement une menace financière et sociale, mais également une menace certaine à l'égard de la sécurité nationale » ».

Le 28 novembre 1997, le Comité ministériel du renseignement a chargé le collège du renseignement et de la sécurité « *d'approfondir l'analyse des menaces d'atteintes, en ce compris par l'espionnage économique, à certains secteurs socio-économiques, de formuler des propositions pour lutter contre ces menaces et d'examiner dans quelle mesure associer à ces travaux le département des Affaires économiques ».*

Le collège du renseignement et de la sécurité a confié cette mission à la Sûreté de l'Etat qui a elle-même formulé les propositions d'actions suivantes dans une note du 5 février 1998 :

1) "Faire l'inventaire des secteurs qui risquent d'être visés :

S *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;*

S *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 et leurs origines par des contacts avec les secteurs visés, et organisation d'échanges d'informations".* (Plus loin, les menaces sont ainsi décrites : "*Espionnage par des entreprises étrangères, concurrence déloyale internationale, tentative d'OPA illicite d'entreprises belges par des intervenants étrangers, etc.. Recherches d'activités clandestines de gouvernements ou administrations étrangers et leurs services de renseignement").* Selon la Sûreté de l'Etat, ne seraient donc pas inclus dans sa mission, l'espionnage industriel développé par une firme contre une autre au niveau du secteur privé national.

3) Elargir ou adapter les recherches dans les domaines classiques (espionnage (politique), terrorisme, extrémisme idéologique, sectes nuisibles, crime organisé, prolifération de matières NBC, protection de personnes, nombreuses tâches de recherche et d'avis administratifs,...) couverts par le service aux besoins de la protection économique et scientifique.

4) Sensibilisation et conseils aux institutions économiques et scientifiques quant aux mesures de sécurité à prendre (personnel, protection des données, protection physique, communications, etc...).

5) Assister à ou organiser des réunions de concertation avec les instances officielles concernées.

6) Fournir des analyses de la menace et proposer des mesures à prendre aux autorités.

7) Prévenir le gouvernement belge lorsque les règles du jeu propre à l'économie de marché sont délibérément faussées au détriment des intérêts belges.

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

La note du 5 février 1998 se poursuit en estimant de manière minimale le besoin en personnel supplémentaire à la Sûreté de l'Etat pour réaliser cette nouvelle mission. Vu l'ampleur de la nouvelle mission, l'estimation provisoire du 25 mars 1997 est jugée manifestement insuffisante. En annexe, on trouve une liste - non exhaustive - des départements et services de l'Etat concernés par la nouvelle mission de protection du potentiel économique et scientifique.

Les actions postérieures à la loi organique du 30 novembre 1998.

La "*protection du potentiel scientifique et économique"* figure bien à présent dans les missions définies par les directives internes de la Sûreté de l'Etat. La mission est même étendue à la "*protection du patrimoine industriel*" conçu comme une part du potentiel économique et qui comprend l'ensemble des activités économiques de production de biens. Une nouvelle section a été créée spécifiquement chargée de la protection du potentiel économique et scientifique.

Le 28 mars 2000, l'administrateur général a.i. a fait part au nouveau ministre de la Justice de la manière dont elle concevait l'exécution de cette nouvelle mission. Les termes de cette note sont assez semblables à ceux de la note du 5 février 1998. La demande de personnel pour la nouvelle mission porte sur 50 unités pour les services extérieurs et 28 unités pour les services administratifs (scientifiques, économistes, ingénieurs, etc.). Le 11 avril 2000, le ministre a marqué son accord avec ces propositions à soumettre au CMRS.

Le Conseil Ministériel du Renseignement et de la Sécurité prépare des directives afin de définir le potentiel scientifique et économique à protéger en application de l'article 7 de la loi organique des services de renseignement et de sécurité. Le Comité R n'a pas encore connaissance du résultat de ses travaux.

Entre-temps, le cabinet du ministre de la Justice a participé à plusieurs réunions de la "plate-forme de concertation permanente sur la sécurité industrielle" en présence de représentants de la FEB. Les propositions issues de cette plate-forme de concertation ont effectivement été examinées en juillet 2000 par la Sûreté de l'Etat laquelle a transmis son avis au ministre de la Justice le 1er août 2000.

Cet avis préconise notamment :

1) "la mise en place d'une action de prévention conjointe FEB/SE, concrétisée par la présentation d'exposés de sensibilisation auprès d'entreprises appartenant à des secteurs exposés;

2) la constitution et la réactualisation d'une liste prioritaire de secteurs d'activités et de technologies de pointe permettant une protection efficace et rapide des entreprises concernées;

3) le recueil de renseignements plus spécifiquement relatifs aux activités, au sein du monde économique, d'organisations sectaires, de la criminalité organisée ou d'espionnage par des puissances étrangères. Cette collecte d'information permettra d'analyser la menace latente et la mise en place éventuelle de mesures protectrices".

La Sûreté de l'Etat demande par ailleurs que ses agents puissent prendre part à des formations au sujet de l'organisation de l'entreprise et des formes de criminalité dont celle-ci est victime.
Elle préconise la mise en place d'une cellule "criminalité informatique et télécommunications" au sein d'une agence fédérale pour la protection informatique et le cryptage.

L'administrateur général de la Sûreté de l'Etat a présenté cette note au cabinet du ministre de la Justice au cours de deux réunions qui se sont tenues les 2 août et 6 septembre 2000.

La section chargée du potentiel scientifique et économique a déjà établi une série de contacts avec des responsables d'entreprises privées et publiques, de fédérations patronales, d'universités, de ministères et autres administrations publiques. Les autres sections des services extérieurs de la Sûreté de l'Etat sont en outre habilitées à recueillir des informations en rapport avec le potentiel scientifique et économique lorsque les menaces émanent soit des pays, soit des milieux extrémiste, sectaire ou criminel qu'elles traitent.

Le service d'analyse chargé des organisations criminelles et du contre-espionnage (qui peuvent notamment avoir des *"conséquences déstabilisatrices sur le plan politique ou socio-économique"*) a d'abord été chargé de recevoir et de traiter les rapports relatifs à la protection du potentiel scientifique et économique. Depuis septembre 2000, cette nouvelle compétence est confiée au service d'analyse qui est également compétent en matière d'armes et de prolifération. L'espionnage est également traité par les services d'étude de certaines régions du monde selon l'origine géographique des activités d'espionnage détectées.

Au 30 novembre 2000, une septantaine de rapports d'information ainsi que cinq rapports d'analyse

concernant la protection du potentiel scientifique et économique ont déjà été rédigés.
La Sûreté de l'Etat s'y montre notamment sensible à l'influence occulte qu'une secte pourrait tenter d'exercer sur les grands décideurs économiques du pays.

En attendant de recevoir les directives nécessaires du Comité ministériel du renseignement et de la sécurité, la Sûreté de l'Etat n'utilise ces rapports qu'à des fins purement internes. De même, des discussions d'ordre général ont eu lieu sur le sujet avec le SGR mais il n'a encore été procédé à aucun échange d'informations. Quelques contacts préparatoires ont été établis avec des services de renseignement étrangers, mais aucune collaboration officielle.

A plusieurs reprises, l'administrateur général de la Sûreté de l'Etat a demandé que le Comité ministériel du renseignement et de la sécurité (CMRS) se prononce sur la manière dont son service devait communiquer des renseignements aux ministres, aux autorités administratives et judiciaires, aux services de police, aux instances et personnes compétentes conformément à l'article 19 alinéa 1 de la loi organique des services de renseignement et de sécurité.

8.3. Le SGR

En 1997, M. Van Lijsebeth, alors administrateur général de la Sûreté de l'Etat, avait déclaré au Comité R que la sauvegarde du potentiel scientifique et économique du pays serait une mission toute nouvelle que la Sûreté devrait accomplir seule, c'est-à-dire en excluant le SGR. En effet, la loi organique des services de renseignement et de sécurité n'a pas donné au SGR la mission de rechercher, d'analyser et de traiter le renseignement relatif aux activités qui menacent le potentiel scientifique et économique du pays.

Cependant, dans le cadre de la loi du 10 janvier 1955 sur la propriété industrielle, la section du SGR chargée de la *Sécurité militaire et industrielle* assure la gestion des informations et brevets "classifiés" conjointement avec le ministre des Affaires économiques pour contrôler les conditions d'exploitation, d'inventions et de mise en oeuvre des secrets de fabrique portés à la connaissance de sociétés commerciales, dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l'OTAN.

Il s'agit en l'occurrence d'appliquer les procédures inhérentes au dépôt, à la gestion et la levée du secret des brevets, des inventions et des informations "classifiés" qui, à ce titre, ne peuvent être divulgués conformément à la loi.

Le SGR établit et diffuse des directives de sécurité industrielle et contrôle leur application auprès des sociétés industrielles installées sur le territoire national. Si l'installation est située dans un autre pays, le SGR veille à ce que ce contrôle se fasse dans le pays concerné par l'autorité nationale compétente de ce pays. Le SGR agit de la même manière sur le territoire national pour les brevets "classifiés" par un Etat étranger, dans le cadre de l'article 12 de la loi en question.

Le SGR effectue également les enquêtes en vue de l'octroi des habilitations de sécurité aux firmes, à leurs administrateurs et à leur personnel dans le cadre de leurs activités spécifiques au profit de la Défense nationale ou de l'OTAN. La finalité de ces enquêtes est de vérifier l'intégrité des administrateurs et du personnel de ces firmes, aussi bien sur le plan de la fiabilité, de la loyauté et de la discrétion que sur les plans financier et commercial.

9. CONCLUSIONS ET RECOMMANDATIONS

Deux ans après que lui ait été attribuée la mission de protéger le potentiel scientifique et économique du pays, la Sûreté de l'Etat se montre sensibilisée à ce sujet à travers différentes notes internes et documents préparatoires adressés au ministre de la Justice. Toutefois, la Sûreté de l'Etat n'estime pas être encore en mesure de remplir cette nouvelle tâche de manière opérationnelle.

Cette situation est due au fait que la Sûreté de l'Etat,

- n'a pas encore reçu les directives du Comité ministériel du Renseignement et de la Sécurité définissant le potentiel scientifique et économique à protéger ainsi que le prescrit l'article 7, 1° de la loi du 30 novembre 1998;

- n'a pas reçu les moyens humains supplémentaires nécessaires.

Le Comité R recommande que ces deux obstacles soient levés pour permettre à la Sûreté de l'Etat de remplir sa nouvelle mission.
En attendant, une section prépare le terrain en établissant une série de contacts destinés à sensibiliser les milieux économiques et scientifiques à la problématique.

Le Comité R est conscient de la difficulté de protéger les secrets scientifiques et économiques dans le contexte actuel de la société de l'information dominée par les progrès technologiques et caractérisée autant par son mondialisme que par son ouverture d'esprit scientifique. La mondialisation des entreprises et la globalisation des procédés au niveau mondial rendent d'ailleurs difficile l'attribution d'une nationalité à un potentiel scientifique et/ou économique. C'est notamment la raison pour laquelle le Comité R estime non pertinent le critère de nationalité du mandant de l'espion retenu par la Sûreté de l'Etat pour distinguer l'espionnage économique (pour lequel elle serait compétente) de l'espionnage industriel (affaire privée pour laquelle elle ne serait pas compétente). A l'instar de la FEB, le Comité R tend à considérer comme appartenant au potentiel scientifique et économique du pays, toute entreprise, tout laboratoire ou tout centre de recherche exerçant son activité sur le territoire national et y développant une valeur ajoutée. Le Comité R a fait part de ce point de vue à l'administrateur général de la Sûreté de l'Etat. C'est au Comité ministériel du Renseignement et de la Sécurité qu'il appartiendra de trancher.

L'importance prise par le secteur privé et les enjeux liés au patrimoine scientifique et économique du pays créent en effet de nouveaux besoins de sécurité dans le monde scientifique et celui des entreprises. Dans notre pays, certains de ces besoins ont été définis par la Fédération des Entreprises de Belgique.

Ceci doit être un sujet d'attention pour le parlement et le gouvernement dans la mesure où notre pays compte nombre d'entreprises, souvent de petites dimensions, impliquées dans la recherche et le développement de technologies de pointe.

Si les besoins de sécurité ne sont pas suffisamment pris en compte par les autorités publiques et par nos services de renseignement, soit les entreprises et les laboratoires de recherche continueront à sous-estimer les risques qu'ils courent, soit ils se tourneront vers les firmes privées de renseignement et de sécurité. A cet égard, la montée en puissance des sociétés de renseignement privées en matière économique suscite des interrogations profondes quant à leur éthique, leur cadre juridique et leur contrôle démocratique.

C. ENQUETES A L'INITIATIVE DU SERVICE D'ENQUETES

ENQUETE SUR L'INTERVENTION DU SGR A PROPOS D'UN EVENTUEL INCIDENT DE SECURITE A L'INTERIEUR D'UNE ENCEINTE MILITAIRE

1. PROCEDURE

Au mois de février 1999, le Comité R réceptionne un courrier de son Service d'enquêtes. Ce dernier souhaite en effet prendre en considération l'éventualité d'une provocation à caractère néo-nazi s'étant déroulée à l'occasion d'un meeting aérien organisé les 5 et 6 septembre 1998 sur la base de Kleine Brogel.

Deux organes de presse, à la connaissance du Comité R, en ont fait une relation, photo(s) à l'appui.

Le 10 février 1999, le Comité R fait donc parvenir son accord au chef du Service d'enquêtes et se charge, à la même date, de notifier l'ouverture de cette enquête aux présidents respectifs de la Chambre et du Sénat, en conformité avec l'article 46 § 3 de son règlement d'ordre intérieur et la loi organique de contrôle des services de police et de renseignement du 18 juillet 1991, telle qu'elle était en vigueur à cette époque.

Le 12 février 1999, le chef du Service d'enquêtes adresse à son tour notification de l'ouverture de cette enquête au ministre de la Défense nationale, en exécution de l'article 43.1 de la même loi organique.

Le Service d'enquêtes du Comité R dépose un rapport en date du 31 mars 1999.

Une apostille complémentaire lui est adressée le 21 décembre 1999 et le rapport d'enquête final sera déposé le 11 septembre 2000.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 12 mars 2001.

Le 12 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas de commentaire à formuler au sujet de ce rapport. Toutefois, il a souligné que : « *faisant référence à mes réponses aux questions parlementaires antérieures, je saisis l'occasion de confirmer mon point de vue, déjà exprimé antérieurement, que des organisations d'extrême droite ne sont pas du tout à leur place lors d'événements organisés par la Défense nationale ».*

2. L'INTERET PARLEMENTAIRE

Sans prétendre à l'exhaustivité, le Comité R a relevé l'existence de questions parlementaires à ce sujet, à l'adresse du vice-premier ministre et ministre de la Défense nationale, soit celles du 30 octobre 1998 des députés Rony Cuyt et Lode Vanoost ainsi que celle du 27 octobre 1998 du sénateur Erdman.

Il y est essentiellement question d'une organisation nommée « Soldiers of fortune » qui serait liée à l'extrême droite américaine.

Le ministre a porté à la connaissance des intervenants qu'une autorisation de tenir un stand a été délivrée à un homme originaire du pays de Galles s'étant fait connaître sous l'appellation de « Soldiers of Fortune ».

A ce moment personne ne savait rien de ses éventuels liens avec l'extrême droite et les contrôles organisés avant et pendant la manifestation n'avaient rien révélé d'anormal. Le ministre a en outre déclaré que les organisations d'extrême droite ne peuvent être tolérées aux manifestations de masse organisées par l'armée.

3. CONSTATATIONS

Le Service d'enquêtes du Comité R a pris contact avec le SGR et s'est d'abord entretenu avec le commissaire principal chargé de la problématique du terrorisme et de la subversion.

Ce dernier précise que la sécurité est essentiellement du ressort de l'autorité militaire qui organise la manifestation. La responsabilité de la présence de particuliers et de sociétés exerçant une activité sur le site incombe donc au chef de Corps de l'Unité organisatrice.

Le meeting de Kleine Brogel représente toutefois une exception.

C'est donc à l'occasion de ce suivi spécifique et de l'intérêt ultérieurement manifesté par le ministre de la Défense nationale que le SGR a pu fournir incidemment quelques éléments d'information relatifs au stand « Soldiers of Fortune ».

Selon les déclarations faites aux enquêteurs du Comité R , l'organisateur était connu des autorités militaires de Kleine Brogel dans la mesure où il avait déjà sollicité, et obtenu, lors d'un air show antérieur en 1995, l'autorisation de vendre divers colifichets, style ; « british army berets, cap badges, clothing, boots, coffee mugs and zippo lighters with military crets on, etc… ».

L'autorisation délivrée attirait l'attention du candidat sur le fait que ni la base de Kleine Brogel, ni le Gouvernement belge, ne sauraient être tenus pour responsables d'accidents ou d'incidents dans lesquels seraient impliqués les membres du personnel de ce stand.

Cette connaissance a fait que la demande d'autorisation de « Soldiers of Fortune » introduite en 1998 n'a pas été relayée vers le SGR, puisqu'il s'agissait d'un « habitué » dont le stand n'avait précédemment provoqué aucun incident.

Vérification faite a posteriori, le responsable du stand n'était pas connu de la documentation du SGR, pas plus qu'il n'est ressorti d'une consultation ultérieure d'un service allié que l'intéressé aurait été en liaison avec l'extrême droite. Il n'y a toutefois pas eu, à ce niveau, de consultation de la Sûreté de l'Etat, qu'il s'agisse du gérant du stand ou de l'organisation « Soldiers of Fortune ».

Le SGR s'est montré catégorique sur l'absence de toute constatation par ses agents de la présence d'objets revêtus de sigles néo-nazis, contrairement au contenu d'une photo publiée dans la presse, montrant une personne cagoulée tendant une chope sur laquelle apparaît une croix gammée.

C'est cette absence de constatation qui explique pourquoi aucun rapport n'a été dressé quant à la présence d'activisme de ce type.

Il n'y a pas non plus eu de mouvement de foule aux abords du stand, de telle sorte que le SGR forme l'hypothèse que l'incident n'a pu en tout état de cause qu'être furtif, et n'exclut pas qu'il se soit agi d'une provocation.

Le SGR n'a pris connaissance de la photographie litigieuse qu'en raison de sa publication dans la presse et est intervenu à la suite de la demande du ministre de tutelle, résultant elle-même des questions parlementaires.

4. SYNTHESE DE L'ENQUETE

L'enquête a révélé que le SGR était - exceptionnellement - présent lors de l'une des manifestations « ouvertes » organisées par une Unité de la Défense nationale.

Il appert que les raisons de la présence du SGR au meeting show étaient d'un autre ordre que la surveillance du stand « soldiers of fortune ».

Les deux agents du SGR n'ont rien remarqué, qu'il s'agisse d'objets litigieux ou d'attroupement consécutif à un incident, mais ils n'excluent pas une survenance furtive. Pour leur part l'éventualité d'une manipulation reste une hypothèse de travail, que rien de concret n'a cependant étayé.

Informés a posteriori par la presse et à la suite de l'interrogation du ministre de la Défense nationale, ils ont cherché des informations tant internes qu'auprès d'un service allié, à la fois sur le gérant du stand et sur l'organisation nommée « soldiers of fortune » mais n'ont recueilli aucun élément susceptible de relier l'un ou l'autre à l'extrême droite.

Pour le surplus le Comité R a, fin 1999, brièvement parcouru d'initiative le Web et a ainsi pu constater qu'à l'adresse suivante : « http://www.sofmag.com » résidait un site abritant une trentaine de pages et semblant constituer une vitrine officielle du « mouvement » « Soldiers of Fortune » sans pour autant informer davantage. A l'époque un examen rapide du site n'avait pas permis d'y déceler la présence d'emblèmes à caractère nazi.

5. CONCLUSIONS

Le SGR n'a rédigé aucun rapport relatif à un possible incident qu'il n'a pas personnellement constaté. Rien ne permet donc de confirmer ni d'infirmer l'information véhiculée par la presse.

Les renseignements recueillis par le Service d'enquêtes du Comité R proviennent de l'audition des agents qui étaient en mission sur place et des quelques recherches effectuées à la suite de la parution de photos dans la presse et de la demande en ce sens formulée par le ministre de la Défense nationale.

L'enquête menée par le Comité R a permis d'apprendre que le SGR n'était qu'exception-nellement concerné par la sécurité des activités s'exerçant sur le site d'une Unité militaire « ouverte », soit lorsqu'un ou plusieurs participants potentiels appartiennent à la liste des organisations suivies par ce service. En dépêchant deux agents à Kleine Brogel, le SGR a donc satisfait à sa mission générale.

Le Comité R constate toutefois qu'en ce dossier, ni la Sûreté de l'Etat ni les autorités judiciaires n'ont été consultées par le SGR. Sans aller jusqu'à prétendre que le contenu de celui-ci rendait cette double démarche indispensable, il tient à rappeler ici, à toutes fins utiles, que la loi du 30 novembre 1998 a instauré le principe de « coopération mutuelle aussi efficace que possible ».

D. PLAINTES DE PARTICULIERS ET DENONCIATIONS

CHAPITRE 1 : RAPPORT RELATIF À L'ENQUÊTE DE CONTRÔLE CONCERNANT LE SGR SUITE À UNE PLAINTE DE PARTICULIER

En vertu de l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et pour des raisons tenant à la confidentialité ainsi qu'au respect de la vie privée des personnes, le Comité permanent R a décidé de ne publier ici qu'une partie succincte du rapport (21 pages) qui a été adressé au ministre compétent ainsi qu'au Sénat, comme la loi précitée le prévoit en son article 33, 3ème alinéa.

1. LA PROCÉDURE

Le Comité R a reçu, le 29 avril 1999, une lettre contenant une dénonciation émanant d'un membre des forces armées.

Dans cet écrit l'intéressé estimait avoir été abusé par le Service Général de Renseignement et de la sécurité des Forces armées (SGR) à l'occasion d'un contrôle de la sécurité du système informatique dans le service où il était détaché.

Il était convaincu que ses droits n'avaient pas été respectés dans un contexte où il avait été amené à démissionner de cette fonction particulière sous des conditions qu'il qualifiait d'inacceptables.

Le 5 mai 1999, le plaignant était entendu de manière circonstanciée par le chef du Service d'enquêtes du Comité R, en présence du président de celui-ci. A cette occasion, il a confirmé sa plainte en y apportant de nombreuses précisions.

Des indices d'infractions pénales semblant apparaître des faits tels que décrits par le plaignant, la décision fut prise d'en aviser les autorités judiciaires en application des articles 29 du code d'instruction criminelle et 46 1er alinéa de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

A ce stade, et vu cette transmission aux autorités judiciaires, le Comité R a estimé opportun, dans le but de ne pas interférer dans l'enquête pénale, de ne pas ouvrir immédiatement une enquête de contrôle et d'attendre pour ce faire les résultats des investigations judiciaires.

Ces dernières furent confiées au Service d'enquêtes du Comité R en application de l'article 40, 3ème alinéa de la loi du 18 juillet 1991, organique du contrôle des services de police et de renseignements, en dehors de toute compétence de contrôle du Comité R, qui n'a pas eu accès aux données du dossier judiciaire en cours de traitement.

L'information pénale aboutit en août 1999 à *« une décision de classement sans suite par défaut d'éléments constitutifs d'infraction.»*

Ayant été informé du classement sans suite de l'enquête judiciaire, le plaignant déposa, le 27 octobre 1999, une nouvelle demande d'enquête auprès du Comité R reprenant les mêmes termes que ceux de sa plainte initiale[1] .

Par décision du 28 octobre 1999, le Comité R a donc ouvert une enquête de contrôle.

Conformément à l'article 32 de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991, l'ouverture de cette enquête a été notifiée, le 29 octobre 1999 à Monsieur A. De Decker, Président du Sénat.

Par courrier du même jour, et en application de l'article 38 § 2 de la loi organique du 18 juillet 1991 précitée, l'autorisation de consultation et de prise de copies des pièces du dossier judiciaire a été demandée aux autorités compétentes. Cette autorisation a été accordée par courrier du 3 novembre 1999.

Le chef du Service d'enquêtes du Comité R a averti Monsieur le ministre de la Défense nationale par courrier du 8 novembre 1999, conformément à l'article 43.1 de la loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignements.

Le Service d'enquêtes a transmis le 15 mars 2000 les résultats de ses investigations, ainsi que l'ensemble du dossier contenant les pièces y afférentes, au Comité R qui a ainsi pu prendre connaissance du versant judiciaire de l'enquête.

Deux membres du Comité R ont eu un entretien avec le plaignant en date du 30 novembre 2000.

La version publique du présent rapport a été approuvée par le Comité R lors de sa réunion plénière du 6 mars 2001.

La version intégrale du rapport a été envoyée au ministre de la Défense nationale et au Président du Sénat le 15 février 2001. Le présent rapport leur a été envoyé le 13 mars 2001.

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il était d'accord pour la publication de ce rapport.

2. CONCLUSIONS ET RECOMMANDATIONS

2.1 Le Comité R souligne que les autorités judiciaires n'ont décelé aucun élément constitutif d'infraction pénale dans les faits rapportés par le plaignant à charge des membres du SGR et que, sur cette base ainsi que sur celles des constatations ultérieures de l'organe de contrôle, aucune violation par ce service des droits que la Constitution et la loi confèrent aux personnes n'a été relevée[2]

---

1 Pour éviter toute confusion, le Comité R rappelle qu'il n'a aucune compétence judiciaire et que la requête du plaignant ne peut donc s'entendre comme une demande de révision de la décision des autorités judiciaires

2 Crf. l'article 1er de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

2.2 La loi organique du 30 novembre 1998 prévoit pour le SGR une série de missions parmi lesquelles, outre l'aspect du renseignement, on trouve : *« la protection des systèmes informatiques et de communications militaires ou ceux que le Ministre de la défense nationale gère. »*

Il est clair pour le Comité R, comme pour l'actuelle direction du SGR, que toutes ces missions nécessitent, pour garantir à la fois l'efficacité des services et la protection des droits fondamentaux des citoyens l'élaboration d'un cadre légal complémentaire suffisamment clair et précis pour permettre, notamment dans le contexte de la sécurité informatique, d'identifier et de neutraliser toute tentative d'intrusion dans les systèmes des Forces armées ou du Ministère de la Défense nationale, sans empiéter, d'aucune manière sur les compétences propres des autorités judiciaires.

Le Comité R rappelle régulièrement la nécessité de doter les services de renseignement et de sécurité de compétences légales élargies, de matériel performant et de davantage de personnel spécialisé.

La raison n'est autre que de permettre à ces services de se hisser à un niveau d'efficacité supérieur à celui qu'ils sont actuellement susceptibles de mettre en œuvre. Le présent dossier, pour lequel le Comité R a cherché à chaque ligne à faire la part du subjectif et de l'avéré, sans jamais prendre parti pour l'une ou l'autre des thèses en présence, a eu le grand mérite d'attirer son attention sur les risques liés à des dérapages potentiels dans l'utilisation de méthodes de travail proches de celles de la police et qui pourraient mettre en péril les libertés et les droits fondamentaux des citoyens.

Il va de soi que le perfectionnement de l'outil doit aller de pair avec un perfectionnement du contrôle de l'usage de celui-ci. Il est en effet incontestable que les atteintes et les dommages occasionnés par un éventuel dysfonctionnement d'un outil performant seront d'autant plus conséquents.

Dans cette optique, le Comité R recommande dès lors de doubler l'attribution par le législateur de moyens complémentaires aux services de renseignement et de sécurité d'un contrôle adéquat et effectif en matière d'usage de ces moyens.

2.3 Enfin, le Comité R ne peut que constater qu'aucun dossier de cette enquête informatique n'était conservé dans les archives du SGR. Une telle procédure est bien certainement contraire à l'esprit de la loi du 18 juillet 1991 et est en pratique de nature à entraver et même à empêcher tout contrôle ultérieur.

En l'absence d'un dossier complet et inventorié, le Comité R ne peut en effet s'assurer « a posteriori » qu' « in tempore non suspecto » le comportement des membres des services de renseignement s'inscrivaient bien dans le cadre légal des missions spécifiques d'un tel service.

CHAPITRE 2 : RAPPORT CONCERNANT LA DENONCIATION PAR UN PARTICULIER DE DYSFONCTIONNEMENTS PRESUMES A LA SURETE DE L'ETAT

1. LA PROCÉDURE

A sa demande le plaignant fut entendu par le Service d'enquêtes du Comité R le 24 janvier 2000.

Il relata en substance que depuis le début de 1998, il avait fourni occasionnellement des informations à l'une des sections locales de la Sûreté de l'Etat et qu'après environ deux années de collaboration, il venait d'être mis fin à cette dernière sur ordre du siège central de cette administration à Bruxelles. Il estimait que cette décision résultait du contenu de certaines informations dérangeantes qu'il avait transmises.

Suite à cette déposition, le Comité R a décidé le 26 janvier 2000 d'ouvrir une enquête de contrôle.

En application de l'article 32 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, le président du Sénat a été averti de l'ouverture de la présente enquête par courrier du 4 février 2000.

Le même jour une apostille était adressée au chef du Service d'enquêtes du Comité R.

Celui-ci, en application de l'article 43 § 1 de la loi précitée, a avisé le Ministre de la Justice de l'ouverture de l'enquête de contrôle en date du 7 février 2000.

Le Service d'enquêtes du Comité R a clôturé son enquête par un compte-rendu de ses constatations dressé le 30 mars 2000.

Le Comité R a approuvé le présent rapport en date du 23 janvier 2001.

Le 4 avril 2001, le ministre de la Justice, se basant sur une note de la Sûreté de l'Etat, faisait savoir qu'il ne partageait pas la recommandation du Comité R de réglementer par une législation générale l'utilisation d'informateurs par la Sûreté de l'Etat.

2. LES ÉLÉMENTS DE LA PLAINTE

Le plaignant, qui situe son action dans la sphère des activités de la criminalité organisée, aurait fourni certaines informations récentes à un service étranger. Il aurait appris à cette occasion qu'il était présenté sous un jour négatif en Belgique. Il ne lui fut pas fourni davantage de précision.

Il dut toutefois constater que, quelques temps plus tard, les membres de la Sûreté avec lesquels il était normalement en contact l'avertissaient qu'il devait mettre un terme à leur relation, étant donné que l'intéressé ne jouissait pas d'une bonne réputation au siège de la Sûreté de l'Etat à Bruxelles.

Le plaignant supposait que cette décision était la conséquence d'informations qu'il avait communiquées et qui mettaient en lumière des relations suspectes entre diverses personnes dont certaines appartenant, d'après lui, au monde des affaires et au monde du renseignement.

Il avait pensé s'adresser à la presse, mais finalement avait décidé d'informer le Comité R s'agissant pour lui de faits qui montraient des dysfonctionnements au sein de la Sûreté de l'Etat.

Il précisait encore être en possession de nouvelles informations intéressantes pour ce service, mais ne pouvoir les transmettre à ses contacts habituels sous peine de leur faire courir le risque d'être sanctionnés ou même déplacés.

3. L' ENQUÊTE

3.1. Certaines règles générales concernant l'utilisation d'informateurs

Dans le cadre de cette enquête des échanges de vue ont eu lieu entre le Service d'enquêtes du Comité R, le Directeur des Opérations de la Sûreté de l'Etat, le responsable de la section locale de la Sûreté de l'Etat et les deux membres concernés de ce service.

A ces occasions, certaines règles générales concernant le recours à des informateurs ont été rappelées.

C'est ainsi qu'une personne ne peut être informateur répertorié *si elle a des antécédents judiciaires, si elle travaille pour un autre service de renseignements, s'il apparaît que les informations fournies par cette personne ne sont pas fiables.*

Ces trois critères ne se trouvent pas repris explicitement dans une note de service. Il faut souligner qu'ils datent d'une période où la Sûreté de l'Etat n'avait pas pour mission explicite de s'occuper de la criminalité organisée et n'était donc pas, par définition, en contact avec le milieu délinquant.

Cette situation est différente aujourd'hui, en ce sens que l'article 7 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité a attribué à la Sûreté de l'Etat la mission *«de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel…».*

L'article 8 de la même loi définit pour sa part *« l'activité qui menace ou pourrait menacer(...)»* comme étant notamment *«toute activité individuelle ou collective, déployée à l'intérieur du pays ou à partir de l'étranger, qui peut avoir un rapport avec (…) les organisations criminelles,(…)».*

Dans ce nouveau contexte, il apparaissait donc essentiel pour la hiérarchie de la Sûreté de l'Etat d'assouplir l'application du critère relatif aux antécédents judiciaires. Il est toutefois toujours proposé de ne pas inscrire officiellement comme informateur rémunéré les personnes ayant des antécédents judiciaires, mais d'admettre éventuellement, en fonction du cas, que ces personnes puissent fournir des informations occasionnelles.

Les critères d'appréciation et les modalités de traitement de ces informations occasionnelles de cette espèce feront l'objet d'une prochaine enquête.

3.2. L' application de ces critères au cas d'espèce

3.2.1 Le contexte

Les premiers contacts de la Sûreté de l'Etat avec l'informateur remontent au mois de mars 1998. Ces contacts ont été initiés suite à des informations communiquées à notre service de renseignement par le service d'un autre pays européen concernant des activités de trafic d'armes en relation avec un groupement terroriste.

A cette occasion, l'intéressé a fait état de ses nombreux contacts aussi bien avec des services de renseignement qu'avec des services de police, dans toute l'Europe et dans le reste du monde.

Il a révélé avoir également des contacts au sein du milieu criminel et connaître des problèmes sur le plan judiciaire à attribuer d'après lui, *« à ses activités de renseignement ».*

En rapport avec les faits précis de trafic, l'intervenant déclara avoir été sollicité pour servir d'intermédiaire. Pour cela, il devait disposer de moyens pour se rendre à l'étranger et rencontrer une personne de contact.

Vu ses problèmes judiciaires, il devait également disposer d'une nouvelle identité et d'un nouveau passeport. Il demandait donc l'aide de la Sûreté de l'Etat.

Il avait apparemment fait le même récit à d'autres services de renseignement, mais sans grand succès. Cela l'avait amené à s'adresser à l'ambassade du pays dont le service de renseignement avait averti la Sûreté de l'Etat.

3.2.2. Les premières vérifications faites par la Sûreté de l'Etat

Les antécédents judiciaires de l'intervenant ont montré qu'il avait encouru, de 1993 à 1998, de nombreuses condamnations principalement pour des faits de délinquance financière (faux en écritures, escroquerie, abus de confiance, …).

Des vérifications faites auprès de services de renseignement étrangers et auprès des services de police nationaux, il est apparu que les informations fournies par le plaignant étaient pour une grande partie inexactes et pour une autre partie déjà connues des autorités.

Dans un cas, ces informations devaient principalement permettre à l'intéressé d'obtenir un visa pour pouvoir revenir en Belgique[1].

Ces vérifications ont permis à la Sûreté de l'Etat d'adresser, le 12 mars 1998, un rapport circonstancié au Ministre de la Justice, ainsi qu'au magistrat national concernant cette affaire.

En conclusion de cette note la Sûreté de l'Etat mentionnait ce qui suit : ***« Vu les antécédents de E., nous pouvons conclure qu'à l'aide de plusieurs éléments il construit un récit. Au départ de ce dernier, il tente alors d'obtenir certaines choses : de l'argent, un véhicule et de faux documents d'identité. Ceux-ci devraient être mis à sa disposition par la Sûreté de l'Etat ou par un service de police.***

La Sûreté de l'Etat ne va pas s'engager plus avant dans cette affaire ; ce qui précède est communiqué à toutes fins utiles et restera sans aucune suite, sauf survenance d'éléments nouveaux ».

La Sûreté de l'Etat apprit par la suite que le service homologue étranger mentionné [2] avait finalement pu organiser le voyage de l'informateur, dans le but qu'il puisse rencontrer la personne de contact. Durant le séjour de l'intéressé, aucune rencontre ne se réalisa. Ce dossier ne fut donc pas davantage suivi par la Sûreté de l'Etat.

Le 16 avril 1998 l'interdiction d'entretenir le suivi des contacts avec le plaignant était signifiée à la section locale.

3.2.3. Les autres informations et le suivi de l'affaire par la hiérarchie de la Sûreté de l'Etat.

Le plaignant tenta cependant à plusieurs reprises de renouer les contacts avec la section locale de la Sûreté de l'Etat, en fournissant d'initiative et occasionnellement des informations concernant plusieurs affaires en relation avec la criminalité organisée. A chaque fois celles-ci se révélèrent déjà connues de la Sûreté ou bien sans fondement.

Le ministre de la Justice, le magistrat national, ainsi que le Procureur général territorialement compétent ont été mis au courant de ces nouveaux renseignements par un rapport de la Sûreté de l'Etat du 1er octobre 1999.

---

(1) Ces dernières informations faisaient état de trafic d'enfants et d'un certain « Marc » de Charleroi.

(2) Voir pt.3.2.1

En conclusion, ce rapport rappelle le caractère peu fiable de la source et souligne son caractère dangereux. On s'est en effet aperçu à ce moment que l'intéressé confirmait faussement des informations qui provenaient déjà indirectement de lui-même et qui avaient ainsi déjà été portées à la connaissance des agents de la Sûreté par une autre personne. Deux exemples concrets sont donnés pour illustrer le danger de telles manipulations.

La Sûreté de l'Etat confirme donc son intention de mettre définitivement un terme à tous les contacts avec Monsieur E.

Le 25 février 2000, une nouvelle note d'information fut toutefois adressée au Ministre de la Justice, au magistrat national ainsi qu'au Procureur général territorialement compétent concernant des informations communiquées en mai 1999 par le plaignant relativement à des faits de criminalité organisée. Une nouvelle fois, le peu de confiance que l'on pouvait accorder à l'informateur était souligné.

Il faut noter à ce sujet que le chef de la section locale reçut une réprimande pour ne pas avoir tenu strictement compte du contenu de la note du 16 avril 1998 qui donnait comme instruction «de ne plus chercher à avoir de contacts avec Monsieur E. même dans le contexte d'informations occasionnelles ».

3.2.4 Le point de vue des agents sur le terrain

Ces agents furent entendus par le Service d'enquêtes du Comité R concernant leur impression personnelle au sujet de l'informateur.

Il confirmèrent certes que l'intéressé n'était pas fiable à 100 % tout en ajoutant cependant que le plaignant avait aussi apporté des informations utiles.

Il n'était pas impensable d'après eux que celles-ci aient d'ailleurs été à l'origine des résultats positifs enregistrés par d'autres services nationaux. Ils citent un exemple à ce sujet.

Ils continuent donc de penser que l'intéressé aurait pu démontrer à terme son utilité pour le service en matière de criminalité organisée, à condition qu'il ait été traité et suivi par des personnes expérimentées et que ses informations aient été soumises à un contrôle très approfondi.

Il est donc évident qu'une divergence de conception se manifeste au travers du cas d'espèce entre les agents du terrain et la direction des opérations.

4. CONCLUSIONS ET RECOMMANDATIONS

4.1 Il est apparu de l'enquête qu'en l'espèce les trois critères habituels pris en compte par la Sûreté de l'Etat pour mettre fin à tous les contacts avec l'informateur étaient rencontrés.

L'intéressé avait non seulement un passé judiciaire chargé, mais il travaillait de surcroît - d'après ses dires - pour d'autres services de renseignement et ses informations s'étaient révélées soit de peu de valeur parce que déjà connues, soit peu fiables et suspectes d'être utilisées à des fins de manipulation.

La décision de mettre fin à tout contact avec l'informateur a été prise principalement pour éviter des problèmes dans l'avenir. La matière concernant la criminalité organisée est neuve pour la Sûreté de l'Etat et l'on peut comprendre que la plus grande prudence en ce domaine se soit imposée.

Les risques liés au recrutement d'informateurs appartenant au milieu délinquant qui a déjà entraîné de très graves dysfonctionnements dans d'autres services spécialisés à l'occasion d'affaires récentes (entre autres des faits de corruption), renforcent bien certainement cette approche.

4.2. Il n'en reste pas moins vrai que face à la mission nouvelle que l'article 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité attribue à la Sûreté de l'Etat, la hiérarchie de ce service est consciente que l'application stricte du critère relatif à l'existence d'antécédents judiciaires pour exclure le travail avec un informateur doit être revue et assouplie.

Elle impose sans doute également dans le chef des agents chargés de recueillir l'information une grande capacité d'adaptation.

Sur le plan des principes, il est peu réaliste en effet d'envisager de répondre le plus efficacement possible à cette nouvelle mission en ne recherchant et en ne recueillant seulement que des informations provenant de personnes sans antécédent judiciaire. De tels renseignements ne pourraient concerner le plus souvent que des informations périphériques.

Par ailleurs, l'absence d'antécédent judiciaire ne constitue qu'une ébauche de garantie, eu égard à son caractère purement formel. Peut-on, par définition, considérer l'informateur dont le casier judiciaire est vierge comme une personne exempte de reproche ? Sa fiabilité est-elle totale ? Est-il par essence l'informateur idéal ? Il ne sera un informateur utile que par ses accointances avec le milieu.

Des critères basés exclusivement sur le principe de prudence ne peuvent donc être retenus sans prendre un autre risque qui est de se couper de sources importantes d'informations dans cette matière très sensible des organisations criminelles.

Il faut relever par ailleurs que dans d'autres domaines plus traditionnels de l'action des agents extérieurs de la Sûreté de l'Etat, le même type de dangers inhérents au recrutement d'informateurs existait déjà. Pensons notamment à la matière de l'extrémisme et à celle du terrorisme.

D'autre part, il n'est pas toujours facile de tracer une limite nette et précise entre les autres missions légales qui sont confiées aux services de renseignement et celle attribuée spécifiquement à la Sûreté de l'Etat concernant les menaces que font peser dans différents domaines les organisations criminelles.

L'article 8 f) de la loi organique des services de renseignement du 30 novembre 1998 vise spécialement à ce sujet « les conséquences déstabilisantes sur le plan politique ou socio-économique » susceptibles d'être causées par les organisations criminelles [3].

Il est un fait que les activités de celles-ci sont en effet multiples et diversifiées et qu'elles peuvent toucher des secteurs sensibles comme ceux relatifs au potentiel économique du pays *(citons e.a. à ce sujet la prise de participation dans des entreprises économiques via le blanchiment de capitaux d'origine criminelle, la corruption, les trafics d'êtres humains et ceux de la main d'œuvre clandestine)*, au terrorisme, à la prolifération, autant de matières concernées par les missions de la Sûreté de l'Etat.

4.3. La Sûreté de l'Etat doit aussi se positionner par rapport aux autres services qui participent à la lutte contre la criminalité organisée[4] et participer dans ce domaine à la meilleure collaboration possible avec les autres services administratifs, policiers et judiciaires[5].

Cette coopération est d'ailleurs visée par la loi organique des services de renseignement et de sécurité, comme d'ailleurs la possibilité reconnue par cette même loi aux services de renseignement de recourir à « des sources humaines » pour le recueil d'informations[6].

Selon le rapport 1999 des Ministres de la Justice et de l'intérieur sur le crime organisé en 1998 : *« Etant donné la finalité spécifique de la Sûreté de l'Etat et l'absence de compétences policières, ce service peut uniquement soumettre l'information qualifiée de «douce» (la Sûreté de l'Etat n'effectue aucune enquête judiciaire et ne rédige pas de procès-verbaux). De plus, la Sûreté de l'Etat ne mène aucune enquête sur des faits punissables isolés mais tente de dresser une carte des structures. Enfin, on vise à éviter ainsi des doubles comptages (une partie des informations provenant de la Sûreté de l'Etat est transformée par les services de police en information dure). Le fonctionnement de la Sûreté de l'Etat n'est pas axé sur la conversion de ce type de renseignements en données quantitatives. Par conséquent, elle donne une description qualitative du phénomène »*[7].

---

(3) L'article 8, f) définit d'autre part l'organisation criminelle comme "*(…) toute association structurée de plus de deux personnes, établies dans le temps, en vue de commettre de façon concertée des crimes et des délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions (…)».*

(4) Selon le rapport annuel 1999 sur le crime organisé la Sûreté de l'Etat est à concurrence de 1% à l'origine des informations qui ont permis de démarrer une enquête judiciaire (cf . rapport - p.71, pt. 9.2 - tableau n° 13).

(5) Une circulaire du Collège des procureurs généraux près les Cours d'appel de juin 1999, classifiée « confidentielle » règle la collaboration entre les services de renseignement et de sécurité, le ministère public et les juges d'instruction. Voir également « Le rapport sur la mise en application du protocole d'accord entre le ministre de la justice et le ministre de la défense nationale règlant la coopération et l'échange d'informations entre la Sûreté de l'Etat et le Service général du renseignement et de la sécurité » (Rapport d'activités 1999 du Comité R , p.p. 55 à 58)

(6) Cf . respectivement les articles 18 et 20 de la loi organique des services de renseignement et de sécurité dd. 30 novembre 1998

(7) Voir rapport - p. 36, cf. note de base n° 21

Dans le plan fédéral de sécurité et de politique pénitentiaire[8], à plusieurs reprises, le rôle de la Sûreté de l'Etat dans la chaîne de sécurité et plus particulièrement dans la lutte contre la criminalité organisée, est souligné, notamment dans l'établissement d'analyses stratégiques.

4.4. Selon l'ancien Administrateur général de la Sûreté de l'Etat, le recours à des informateurs reste également le moyen principal pour obtenir des renseignements (entretien du 2 février 1999 avec le Comité R).

4.5. En 1995, le Comité R avait déjà effectué une enquête théorique de contrôle sur l'utilisation d'informateurs par la Sûreté de l'Etat et le SGR. Les résultats de cette enquête ont été publiés dans le rapport général d'activités de 1997 *(voir pages 134 à 164*).

Cette enquête visait à identifier les problèmes qui peuvent se poser à l'occasion de l'utilisation d'informateurs et d'en dégager des premières recommandations.

Dans sa conclusion générale le Comité R soulignait que la matière méritait *«d'être traitée en ce qui concernait les services de renseignement»* et qu'il y avait un risque *«dans les domaines de la criminalité organisée et du terrorisme, que la différence entre informateur des services de police et de renseignement ne s'estompe et que les deux services aient à faire face à des problèmes comparables».*

Le Comité R avait recommandé à cette occasion qu'un texte légal soit édicté qui règlerait l'utilisation d'informateurs par les services de renseignement, selon les principes de subsidiarité, de proportionnalité et de protection externe de l'informateur, en ce compris sa protection physique.

4.6. Si la décision prise en l'espèce de mettre fin aux contacts avec l'informateur apparaît comme justifiée, la mise en perspective du cas particulier dans un contexte actuel plus élargi, ainsi que la divergence d'appréciation de la situation par les agents du terrain et par la direction du service montrent que l'on se trouve en présence d'une problématique suffisamment importante pour qu'elle soit réglée dans l'avenir et dans toutes ses composantes, de manière à établir le meilleur équilibre possible entre les exigences d'efficacité dans l'identification des menaces telles qu'elles sont définies par la loi organique des services de renseignement et celles de la protection des personnes, en ce compris les informateurs eux-mêmes et les agents des services concernés.

Le Comité R réitère donc sa recommandation de mettre en place une législation générale en la matière.

(8) Cf. Sénat et Chambre des représentants de Belgique – session 1999-2000 – Doc. n°. 2-461/ 1 Sénat et DOC n° 50 0716/001 Chambre dd. 13 juin 2000 - p.p. 44 à 45 – projet 27

A propos de cette recommandation, le ministre de la Justice se réfère, dans son courrier du 4 avril 2001 [9], à la remarque formulée par la Sûreté de l'Etat selon laquelle « *la loi organique (art. 18, 38, 39, 40, 41 et 43) contient les bases légales quant au recours aux informateurs pour le recueil du renseignement, la sécurité des données les concernant et les informations qu'elles communiquent, la protection des données classifiées (dont celles qui seraient confiées par ces sources) et la garantie de leur anonymat notamment par le biais de la sanction pénale en cas de révélation de l'identité d'une personne qui demande l'anonymat ou dans l'hypothèse de la divulgation par les agents de la Sûreté de l'Etat des secrets confiés dans l'exercice de leurs missions (en ce compris l'identité d'un informateur si celle-ci est confiée sous le sceau du secret).*

Compte tenu de ces textes, il ne paraît pas nécessaire de prévoir d'éventuelles autres règles relatives aux informateurs. Il convient en effet de se limiter à des règles très générales dans le cadre de la loi afin de ne pas compromettre le travail opérationnel du service. Par contre, les autres règles concernant les informateurs pourraient être reprises dans des directives internes avec un contrôle ».

(9) Voir infra p. 158

CHAPITRE 3 : ENQUETE DE CONTROLE SUITE A LA PLAINTE D'UN PARTICULIER

1. PROCEDURE

Le 13 mars 2000, le Comité R réceptionne un courrier d'une personne détenue, laquelle souhaite voir le Comité R initier une enquête à charge des services de renseignement belges (et étrangers) en raison des circonstances qu'il a constatées à l'encontre de sa personne et en rapport avec la franc-maçonnerie et dont il leur prête la responsabilité. Il signale par ailleurs avoir pris contact avec la « section politique » de l'ambassade américaine

Le 27 mars 2000, le Comité R fait donc parvenir au chef de son Service d'enquêtes une apostille par laquelle il invite ce dernier à entendre le plaignant en confirmation de sa plainte, tout en signalant qu'une réévaluation de cette plainte sera faite après prise de connaissance de cette audition.

En date du 28 mars 2000 le président du Comité R notifie l'ouverture de cette enquête au président du Sénat, en conformité avec l'article 32 de la loi organique du contrôle des services de police et de renseignements du 18 juillet 1991, sous l'intitulé « plainte d'un particulier au sujet d'activités supposées des services de renseignement ».

Par courriers du 30 mars 2000, le chef du Service d'enquêtes du Comité R avise à son tour de l'ouverture de cette enquête les ministres de la Défense nationale et de la Justice, en exécution de l'article 43.1 de la même loi organique.

Le Service d'enquêtes du Comité R dépose un rapport en date du 7 avril 2000.

Une apostille complémentaire lui est adressée le 7 juin 2000 et le rapport d'enquête final sera déposé le 20 juin 2000.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 26 mars 2001.

Le 4 avril 2001, le ministre de la Justice a fait savoir au Comité R qu'il n'avait aucune remarque quant à la publication de ce rapport.

Le 25 avril 2001, le ministre de la Défense nationale a fait savoir au Comité R qu'il n'avait pas d'objection à la publication de ce rapport.

2. CONSTATATIONS

Le Service d'enquêtes du Comité R s'est donc entretenu avec le plaignant en date du 5 avril 2000 et un procès-verbal a été dressé des propos recueillis. Celui-ci, quoique maintenant le contenu de son courrier précité, déclare en substance ne pouvoir y apporter d'éléments contributifs.

Aucun grief précis, aucun élément complémentaire ne seront ajoutés, nonobstant les insistances des enquêteurs.

Dès réception de l'apostille l'invitant à procéder à des vérifications supplémentaires, le chef du Service d'enquêtes s'est enquis des circonstances de la détention du plaignant.

Il est apparu de cette vérification que l'intéressé avait fait l'objet d'une ordonnance d'internement rendue par une chambre du conseil et confirmée peu après par une chambre des mises en accusation. Le requérant a en outre signalé avoir formé un pourvoi en cassation contre cette dernière décision.

Quelques jours plus tard les enquêteurs du Comité R ont interrogé la Sûreté de l'Etat sur l'éventualité d'informations disponibles au sein du service relativement à la personne du plaignant, mais il leur a été répondu que l'intéressé était inconnu de la Sûreté de l'Etat.

3. CONCLUSIONS

Les démarches préalables opérées par le Service d'enquêtes du Comité R n'ont pas permis d'apporter le moindre élément matériel susceptible de vérifications, mais ont révélé que le plaignant avait fait l'objet d'une mesure judiciaire d'internement psychiatrique, confirmée en degré d'appel.

En raison de cette double circonstance le Comité R a décidé de clôturer l'enquête en l'état.

CHAPITRE 4 : ENQUETE DE CONTROLE SUITE A LA PLAINTE D'UN PARTICULIER

1. PROCEDURE

Le 10 mai 2000, le Comité R réceptionne un courrier d'une personne qui souhaite faire part d'une agression dont il a fait l'objet de la part de deux individus dont l'un serait d'après le plaignant «un voyou notoirement à la solde d'un bureau régional d'un des services de renseignement». Cet acte constituerait en fait une intimidation.

Le plaignant joint à son courrier une copie d'un procès-verbal de dépôt de plainte du 6 mai 2000 et annonce son intention d'intenter toute action en justice qu'il estimera appropriée, de même qu'il se réserve la possibilité d'en référer à la presse. Pour le surplus, il se tient à la disposition du Comité R, s'il échet.

Le même jour, le Comité R fait donc parvenir au chef de son Service d'enquêtes une apostille par laquelle il invite ce dernier à entendre le plaignant en confirmation de sa plainte, tout en signalant qu'une réévaluation de cette plainte sera opérée après prise de connaissance de cette audition.

Le service d'enquêtes du Comité R dépose un rapport d'évaluation en date du 25 mai 2000.

Une apostille complémentaire lui est adressée le 7 juin 2000, l'invitant à poursuivre les investigations dans le cadre d'une enquête de contrôle.

Par courrier du même jour, le chef du Service d'enquêtes du Comité R avise le ministre de la Justice de l'ouverture de cette enquête, en exécution de l'article 43.1 de la même loi organique.

En date du 8 juin 2000, le président du Comité R notifie l'ouverture de cette enquête au président du Sénat, en conformité avec l'article 32 de la loi organique de contrôle des services de police et de renseignement du 18 juillet 1991, sous l'intitulé « enquête de contrôle suite à la plainte d'un particulier concernant la Sûreté de l'Etat ».

Le rapport d'enquête final sera déposé le 19 juillet 2000.

Le plaignant a ultérieurement adressé au chef du Service d'enquêtes du Comité R les copies respectivement datées des 20 décembre 2000 et 16 janvier 2001 de nouvelles doléances qu'il a adressées à l'administrateur général de la Sûreté de l'Etat en relation avec le harcèlement dont il se plaint.

Le présent rapport de contrôle a été approuvé par le Comité R en date du 26 mars 2001.

Le 4 avril 2001, le ministre de la Justice a fait savoir au Comité R qu'il n'avait pas de remarque à formuler au sujet de la publication de ce rapport.

2. CONSTATATIONS

Le Service d'enquêtes du Comité R s'est donc entretenu avec le plaignant en date du 23 mai 2000 et un procès-verbal a été dressé des propos recueillis.

Il ressort de la déclaration que l'incident dénoncé serait en fait la « énième » péripétie d'une série qui aurait débuté en 1993-1994, à l'issue d'un malentendu banal, le plaignant ayant à cette époque été vu en compagnie de membres de la PJ.

Il aurait eu le tort de laisser circuler - par amusement - la rumeur selon laquelle il travaillait pour le ministère de la Justice, ce qui aurait fini par provoquer des filatures répétées et des interpellations dans les débits de boissons qu'il fréquente.

Basque par son père, il relate avoir fait l'objet d'une surveillance spécifique lors de la visite du roi d'Espagne, et notamment par un hélicoptère « Puma » de la gendarmerie qui aurait effectué un vol stationnaire devant la fenêtre de son living, « *pour l'observer avec sa grosse caméra* ». Ses comptes bancaires auraient aussi été vérifiés par la gendarmerie.

Il ne connaît aucun membre de services de renseignement et le harcèlement est toujours effectué par l'entremise de « petits voyous » mandatés à cette fin.

Il a travaillé en France, en Afrique du Sud et en Israël et son hypothèse est qu'il serait - à tort - pris pour « *un gros poisson* ».

Il ne souhaite qu'une chose : récupérer sa tranquillité.

Interrogé à son propos le 26 juin 2000, un commissaire de la PJ a déclaré le connaître et le considérer comme un érudit, puis l'avoir perdu de vue à la suite de son départ à l'étranger. Il n'est pas connu défavorablement des services de police.

Interrogé à son tour en date du 4 juillet 2000, un commissaire de la Sûreté de l'Etat a déclaré que l'intéressé n'était pas connu de son service, ni même à titre personnel par ses collaborateurs. Il n'exclut toutefois pas l'éventualité d'une rencontre, sans identification de l'intéressé, au hasard de la fréquentation de débits de boissons par des agents de la Sûreté de l'Etat.

3. CONCLUSIONS

L'audition préalable du plaignant n'a pas permis au Comité R de se faire une opinion immédiate. Il a donc entamé une enquête de contrôle. Celle-ci n'a révélé aucune circonstance susceptible d'intéresser la Sûreté de l'Etat, a fortiori de provoquer le comportement de harcèlement dénoncé.

Il en est par contre apparu que le plaignant fréquente assidûment les débits de boissons et y a laissé s'installer un hâlo de mystère autour de ses activités, tant en raison de sa fréquentation de policiers que de ses origines ou de ses occupations professionnelles à l'étranger.

Sans mettre en doute l'agression que le plaignant invoque à l'appui de sa thèse, le Comité R estime cependant à la lecture du contenu de son enquête et à défaut de la moindre indication contraire, que celle-ci serait plutôt imputable à des mauvais garçons fréquentant les mêmes établissements, sans la moindre liaison avec la Sûreté de l'Etat.

En raison de cette absence actuelle d'éléments de conviction allant dans le sens de la plainte, le Comité R a décidé de clôturer l'enquête en l'état.

E. SUIVI DES ENQUETES DES ANNEES PRECEDENTES

RAPPORT FINAL CONCERNANT L'ENQUETE COMMUNE SUR LES MESURES DE SECURITE PRISES AU SEIN DU SERVICE GENERAL D'APPUI POLICIER[1] (SGAP) EN VUE D'ASSURER LE SUCCES DES ENQUETES JUDICIAIRES ET DE MANIERE PLUS GENERALE SUR L'EFFICACITE DE CE SERVICE

1. PREAMBULE

1.1. **La première partie de cette enquête de contrôle** a été ouverte par le Comité R le 18 décembre 1997, suite à une dénonciation faite par un membre de la «Commission Sirène » du SGAP, relative au fait que la Sûreté de l'Etat avait accordé un certificat de sécurité à un membre du personnel de cette commission, ultérieurement poursuivi dans le cadre d'une instruction judiciaire pour avoir fourni des renseignements au milieu criminel. Ce dossier judiciaire est toujours en cours au moment de la rédaction du présent rapport.

1.2. **L'intérêt parlementaire pour la question était manifeste**, comme en témoignent les diverses interpellations relevées à l'époque (voir les pages 4 et 5 du rapport intermédiaire du 10 août 1998 dont question au point 1. 4 ci-dessous).

1.3. Le 3 février 1998, en application des articles 52 et suivants de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, **l'enquête de contrôle a été élargie à une investigation commune** avec le Comité P. Les devoirs à exécuter par le Service d'enquêtes commun consistaient à relever les normes et directives applicables à la problématique pour ensuite en décrire les structures, la composition, la procédure d'engagement des membres du SGAP, et enfin le concept de sécurité en vigueur dans ce service dans lequel était incorporée la section « Sirène », chargée de l'application de la Convention d'Application de l'Accord de Schengen.

1.4. **Un premier rapport intermédiaire** retraçant les grandes tendances du fonctionnement du SGAP « en ce qui concerne les mesures de sécurité prises au sein de ce service en vue d'assurer le succès des enquêtes judiciaires et de manière plus générale sur l'efficacité de ce service » a été transmis, le 10 août 1998, respectivement aux présidents du Sénat, de la Chambre des représentants, et de la Commission spéciale chargée de l'accompagnement parlementaire des Comités P et R, ainsi qu'aux ministres de la Justice et de l'Intérieur.

Un des buts de ce rapport était notamment de répondre à la question de savoir qui était responsable de la conception et de la mise en œuvre des mesures de sécurité au niveau de la division coopération policière internationale du SGAP (en abrégé C.P.I.), le chef de cette division ayant acquis progressivement dans les faits le contrôle réel de la « Commission Sirène », au détriment du Directeur et ensuite du Directeur a.i. de celle-ci.

[1] Depuis le 1er janvier 2001 et suite à la réforme des polices, le SGAP n'existe plus en tant que tel. Ses missions ont été reprises par la direction générale de l'appui opérationnel, « la direction générale III »

Le rapport intermédiaire rendait compte des nombreuses difficultés rencontrées dans la recherche de la réponse à cette question.

Des problèmes d'antagonismes personnels, de rivalité entre personnes provenant de différents corps de police semblaient en effet s'être concrétisés au niveau du fonctionnement de la commission « Sirène ».

Ces difficultés de fonctionnement avaient rendu stériles des échanges d'informations concernant la protection des données et la garantie du maintien du niveau de sécurité dont l'absence était dénoncée depuis 1995 par le directeur de la « Commission Sirène ». Ces difficultés avaient provoqué également une dilution dans la détermination des responsabilités en cas de « fuites d'informations ».

L'affaire judiciaire (voir 1.1) fut le révélateur de ces problèmes auxquels était confronté le Service Général d'Appui Policier depuis 1995.

Après avoir ainsi mis en exergue une série de dysfonctionnements illustrant un climat avéré de guerre des polices, dont l'enjeu était la gestion de l'information, le rapport intermédiaire recommandait en substance de résoudre les problèmes de sécurité en respectant concrètement et scrupuleusement les règles prévues à l'article 118-1°, 2°, 3° et 4° de la Convention d'Application de l'Accord de Schengen[2] destinées à assurer la protection de la vie privée dans ce système.

---

[2] Article 118

1. Chacune des Parties Contractantes s'engage à prendre, pour la partie nationale du Système d'Information Schengen, les mesures qui sont propres :
   a. à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations) ;
   b. à empêcher que des supports de données ne puissent être lus, copiés, modifiés ou éloignés par une personne non autorisée (contrôle des supports de données) ;
   c. à empêcher l'introduction non autorisée dans le fichier ainsi que toute prise de connaissance, modification ou effacement non autorisés de données à caractère personnel intégrées (contrôle de l'intégration) ;
   d. à empêcher que des systèmes de traitement automatisé de données ne puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation) ;
   e. à garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès) ;
   f. à garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission) ;
   g. à garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction) ;
   h. à empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données ne puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport).
2. Chaque Partie Contractante doit prendre des mesures particulières en vue d'assurer la sécurité des données lors de la transmission de données à des services situés en-dehors des territoires des Parties Contractantes. Ces mesures doivent être communiquées à l'autorité de contrôle commune.
3. Chaque Partie Contractante ne peut désigner pour le traitement de données de sa partie nationale du Système d'Information Schengen que des personnes spécialement qualifiées et soumises à un contrôle de sécurité.
4. La Partie Contractante responsable de la fonction de support technique du Système d'Information Schengen prend pour ce dernier les mesures prévues aux paragraphes 1 à 3.

Par courrier du 24 août 1998, le ministre de la Justice faisait part de ses réserves concernant l'opportunité de publier le rapport d'enquête commune dans les rapports annuels 1998 des Comités permanents P et R.

Pour expliquer sa position, le ministre de la Justice faisait état de la réforme des polices en cours et, dans ce contexte, du projet d'intégrer le SGAP dans la direction générale chargée du soutien opérationnel au sein de la future police fédérale. Il faisait mention d'autre part des modifications qui venaient d'intervenir[3] dans la structure et le fonctionnement des organes de gestion du SGAP pour remédier aux problèmes survenus dans le passé au niveau du processus décisionnel qui avaient empêché le bon fonctionnement du service. Il signalait également que d'autres remarques pertinentes du rapport d'enquête commune avaient déjà été prises en compte. Il attirait enfin l'attention sur le fait que la publication du rapport pouvait porter préjudice au bon déroulement de la procédure judiciaire en cours qui, au travers du cas de la personne incriminée, concernait également le fonctionnement du SGAP, de la section C.P.I. et celui du service SIRENE en particulier.

Par courrier du 7 septembre 1998, le ministre de l'Intérieur adoptait une approche similaire à celle de son collègue de la Justice.[4]

La partie de l'enquête relative uniquement *« aux conditions d'octroi du certificat de sécurité à la personne inculpée de vol de documents »* a toutefois été publiée dans le rapport annuel d'activités 1998 du Comité R (pages 217 à 226) en application de l'article 37 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

2. LES SUITES DE L'ENQUETE

2.1. Une seconde partie de l'enquête commune a été initiée le 1er février 1999. Elle avait pour but de poursuivre le contrôle relatif aux enquêtes de sécurité concernant le personnel ainsi que celui relatif à la sécurité d'une manière plus générale (les locaux, la fonction d'officier de sécurité, l'informatique, les photocopieuses, la mise à disposition de matériel d'écoute).

Il faut souligner d'emblée que cette seconde partie de l'enquête de contrôle a connu de nombreux retards liés aux difficultés internes de fonctionnement de l'ancien Comité P et à la démission successive de plusieurs de ses membres.

Le rapport final de ce complément d'enquête a été transmis aux deux Comités le 15 octobre 1999.

Les nouveaux membres du Comité permanent P ont été nommés le 18 novembre 1999 et sont entrés en fonction le 26 novembre 1999. Ce n'est qu'à partir de cette date que ces derniers, confrontés par ailleurs à de multiples priorités, ont pu également s'atteler au réexamen de l'ensemble du dossier.

---

3 Voir à ce sujet les considérants de l' AR du 11 juin 1998, modifiant l'AR du 11 juillet 1994 concernant le SGAP (M.B. du 2 juillet 1998 prévoyant l'élargissement du conseil d'administration à deux nouveaux membres, à savoir un représentant des autorités administratives et un représentant des autorités judiciaires, le remplacement de la règle du consensus pour les décisions par celle de la majorité et enfin le remplacement du comité de direction tricéphale par un directeur.

4 Voir au sujet du rapport intermédiaire les interpellations parlementaires dans Chambre des représentants de Belgique, 49e Législature -SO 1998-1999- Compte rendu analytique –COM 14.12.98.

2.2. Nonobstant ces éléments et principalement le fait qu'aujourd'hui, dans le cadre de l'organisation de la nouvelle police fédérale, la division « Coopération policière internationale » - comprenant « Sirène » - est intégrée dans la direction générale III, en charge de l'appui opérationnel[5], les deux Comités permanents P et R estiment indispensable, en application de l'article 53 de la loi du 18 juillet précitée, de clôturer cette enquête commune et de faire rapport au Parlement et au ministre de la justice en leur communiquant la substance des conclusions de l'enquête complémentaire.

Celles-ci constituent une suite aux constatations du rapport intermédiaire et montrent surtout à ce sujet l'évolution en matière de sécurité qui a suivi ce premier rapport. Elles mettent d'autre part en évidence la nécessité du développement, du maintien et de l'application de règles de sécurité adéquates, notamment dans le domaine informatique, ainsi que celle de fournir les moyens indispensables pour garantir notamment le résultat exigé par « la Convention d'Application de l'Accord de Schengen » ou par « la Convention Europol » auxquelles la Belgique a souscrit.

C'est ainsi que le Service d'enquêtes commun a pu constater que le problème de la sécurité au sein de la division Coopération policière internationale (CPI) était en pleine évolution et ce de manière positive.

L'histoire de la division CPI a démontré que, d'une manière générale, le danger ne vient pas toujours de l'extérieur, mais bien de l'intérieur. Une prise de conscience à ce niveau était nécessaire et semble être devenue réalité, comme cela a été constaté à l'occasion des nouvelles visites sur place des enquêteurs.

Les instructions de sécurité sont très précises et l'officier de sécurité travaille maintenant à plein temps pour obtenir une amélioration du niveau de sécurité.

La division CPI s'est dotée d'autre part des moyens techniques de contrôle adéquats. La gestion administrative et l'archivage des dossiers répondent également à des critères précis de sécurité.

Une amélioration sensible au niveau des enquêtes de sécurité effectuées lors de l'engagement du personnel, tant policier que civil, a été constatée. Des demandes d'enquêtes de sécurité sont adressées à l'Autorité Nationale de Sécurité, qui délivre une habilitation de niveau « très secret » après avoir fait procéder aux enquêtes d'usage.

Les Comités permanents P et R se demandent comment cette procédure va continuer à être appliquée suite à l'entrée en vigueur le 1er juin 2000 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

En effet, les articles 8 et 10 de cette loi établissent une exception à l'obligation de détenir une habilitation de sécurité en ce qui concerne les autorités judiciaires dans le cadre de leurs compétences propres et, d'autre part, l'article 24 § 4 de l' arrêté royal du 24 mars 2000 portant exécution de la loi, prévoit qu' « aucune demande d'habilitation de sécurité ne pourra être adressée au président de l'Autorité nationale de sécurité pour les membres de la gendarmerie ou d'autres services de police ».

---

5 Cette direction générale a également pour mission la gestion de la banque de données générale nationale visée à l'article 44/4 de la loi sur la fonction de police du 5 août 1992. (article 5 de l'AR portant détermination des directions générales de la police fédérale et répartition entre elles des missions de la police fédérale)

Au niveau informatique, les outils de contrôle existent et certaines techniques de gestion de l'information ont été mises en place pour prévenir dans l'avenir tout abus dans le cadre de l'accès non autorisé à des informations.[6]

Tous ces éléments cités à titre exemplatif n'existaient pas lors des constatations qui donnèrent lieu à la rédaction du rapport intermédiaire. Les problèmes rencontrés restent cependant de ceux pour lesquels, à tout niveau, une évaluation permanente et rigoureuse est indispensable pour garantir l'efficacité des enquêtes judiciaires aussi bien sur le plan national qu'international, tout en garantissant également le respect de la vie privée et la protection des personnes.

L'insertion d'un article 257 bis dans la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (Moniteur belge du 29 décembre 2000) permet de concrétiser temporairement, dès le 1er janvier 2001, le contrôle et la surveillance des services de police qui seront deux des missions du futur parquet fédéral.

Les Comités permanents P et R, dans le cadre de leurs missions légales, resteront attentifs pour leur part à l'évolution dans le nouvel environnement policier, des problèmes de sécurité qui ont été soulevés à l'occasion de la présente enquête.

Le présent rapport a été approuvé par les Comités P et R lors de leur réunion commune du 9 février 2001.

Par courrier du 19 mars 2001, le ministre de la Justice a fait savoir qu'il n'avait pas d'objection à la publication de ce rapport.

6 L'article 18 de l'arrêté royal précité du 24 mars 2000 prévoit que « Les mesures techniques de protection des systèmes et réseaux de télécommunication de données classifiées et des systèmes et réseaux informatiques dans lesquels des données classifiées sont stockées, traitées ou transmises, sont déterminées par le Comité ministériel du renseignement et de la sécurité ».

TITRE III : CONTACTS DU COMITE

RAPPORT DE LA PARTICIPATION D'UN MEMBRE DU COMITE R AU SEMINAIRE INTITULE « MAITRISEZ LES OUTILS DE LA VEILLE ET DE L'INTELLIGENCE ECONOMIQUE » ORGANISE A PARIS LES 16 ET 17 MAI 2000 PAR L'« INSTITUTE FOR INTERNATIONAL RESEARCH »

Ayant décidé le 26 janvier 2000 d'ouvrir une enquête sur la manière dont la Sûreté de l'Etat s'acquittait de sa nouvelle mission de protection du potentiel scientifique ou économique, le Comité permanent R s'est intéressé au programme d'une série de séminaires organisés à Paris par l'« Institute for International Research » I.I.R. se présente comme « le plus important organisateur de conférences dans le monde ». Ses conférences concernent les domaines les plus récents du management et notamment le renseignement économique, domaine susceptible de concerner le patrimoine scientifique et économique d'un pays.

Pour se familiariser avec les pratiques du renseignement (ou intelligence) économique, le Comité R a donc décidé d'envoyer un de ses membres à Paris pour assister au séminaire intitulé « Maîtriser les outils de la veille et de l'Intelligence économique » et qui a eu lieu les 16 et 17 mai 2000. Ce séminaire était animé par François Jakobiak, ancien ingénieur chimiste au sein de la « Société Nationale Elf Aquitaine », actuellement consultant en information stratégique au sein d'une société qu'il a créé en 1994. Spécialisé dans les actions de conseils aux entreprises pour proposer des outils de veille technologique ou concurentielle, M. Jakobiak est aussi conférencier international et chargé de cours dans plusieurs universités et grandes écoles, parmi lesquelles l'Université Libre de Bruxelles. Il a publié cinq ouvrages d'information scientifique, technique et stratégique.

Le Comité permanent R résume ici le contenu du séminaire auquel un de ses membres a assisté.

De l'information scientifique et technique à la veille technologique.

C'est dans les années 70 que le ministère français de la Recherche a donné une première impulsion à la politique française d'information scientifique et technique. Au sein de ce ministère, le Centre de Prospective et d'Evaluation (C.P.E.) opérait la surveillance systématique des secteurs techniques majeurs.

L'information professionnelle peut être considérée selon trois approches différentes :

1) Dans une approche marchande, l'information est considérée comme un bien ou un service créateur de valeur ajoutée ou d'emploi.

2) Dans une approche fonctionnelle, l'information est importante parce qu'elle a des effets sur l'économie, la formation et la culture : elle est importante pour l'innovation, le développement économique, la productivité des secteurs industriels et le niveau culturel d'un pays.

3) Enfin, l'approche stratégique fait considérer l'information comme un bien stratégique, d'où la nécessité de préserver en toute circonstance l'accès du pays aux sources d'information indispensables, de diversifier les sources d'approvisionnement, de constituer sur le territoire national des « stocks stratégiques » d'informations.

La France accorde une priorité à l'approche stratégique de l'information. Cette priorité explique les actions de promotion de la veille technologique engagées par les pouvoirs publics français à partir de 1987 et qui ont conduit, en 1994, à l'éclosion officielle de l'intelligence économique.

En économie, il faut en effet innover pour survivre. Pour innover, il est non seulement indispensable d'être créatif, mais aussi de savoir ce que font les autres. Innovation et veille technologique sont donc liées.

En 1988, le ministre français de la Recherche constitue le « Comité d'Orientation Stratégique de la Veille Technologique » comprenant des experts industriels et des représentants d'organismes de l'Etat. Ce Comité a défini les grandes lignes d'une politique de veille technologique par les entreprises, résolument tournée vers la surveillance scientifique et technique.

Cette surveillance, quelle que soit la taille de l'entreprise, comprend les opérations successives de recherche, de collecte et de diffusion de l'information. Cette phase de surveillance est réalisée, le plus souvent, par des spécialistes de l'information documentaire. L'exploitation est réalisée par des experts du domaine d'activité de l'entreprise et comporte des opérations de traitement, d'analyse, de validation et de synthèse. Divers types d'informations sont pris en compte : scientifique, technique (avec une importance considérable de l'information contenue dans les brevets), technologique et économique. Il doit en ressortir des outils d'aide à la prise de décisions stratégiques. Trois types d'acteurs interviennent donc dans cette structure : les observateurs et collecteurs d'informations, les analystes (ou experts) et les décideurs.

La veille concurrentielle consiste quant à elle à observer et analyser le marché, l'environnement économique, commercial et financier de manière à détecter les menaces et à saisir les opportunités de développement.

C'est le rapport du Xième plan publié en février 1994 et intitulé « Intelligence Economique et stratégique des entreprises » (aussi connu sous le nom de « rapport Martre » du nom de son rapporteur) qui officialise cette dénomination et lui donne tout son sens : « L'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques ». Il s'agit donc à présent d'une initiative au niveau national, et non plus au niveau de l'entreprise. Le concept d'intelligence économique dépasse celui de veille technologique ou concurrentielle car il y a intention stratégique et tactique avec interaction entre les acteurs de tous les niveaux (privés, publics, …).

On lit aussi dans le rapport précité : « Le recueil, le traitement et la diffusion de l'information utile déterminent désormais la compétitivité des entreprises comme la puissance économique des Etats. En France, la question reste traitée de façon trop exclusivement défensive, si bien que notre système est moins efficace que ceux développés par certains Etats concurrents. Changer d'approche appelle une volonté claire de la puissance publique : elle seule pourra, en concertation étroite avec l'ensemble des acteurs concernés, donner l'impulsion nécessaire à une gestion collective de l'information » C'est donc bien au niveau de l'usage offensif de l'information que l'intelligence économique diffère de la veille stratégique. Cet usage offensif de l'information comprend par exemple l'influence et le lobbying.

L'intelligence économique concerne cinq niveaux d'acteurs entre lesquels il y a interaction :

- le niveau de base : l'entreprise;

- le niveau intermédiaire : un secteur professionnel, une branche d'activités;

- le niveau national : les ministères et les administrations où se prennent les décisions stratégiques; en France, les services de renseignement (DST, DGSE, DRM) sont concernés;

- le niveau transnational : les groupes multinationaux;

- le niveau international où les Etats se livrent à des stratégies d'influence.

Actuellement, de nombreux grands groupes économiques se contentent encore de pratiquer la veille technologique et concurrentielle, ainsi que le « benchmarking » c'est-à-dire la recherche, chez les concurrents, des méthodes les plus performantes pour une activité donnée, afin de s'assurer une supériorité. Mais l'intelligence économique commence aussi à se développer dans les entreprises.

Certaines universités et grandes écoles françaises dispensent des formations spécifiques à la veille technologique et à l'intelligence économique. Ces formations aboutissent à la délivrance de Diplômes d'Etudes Approfondies (DEA). Les étudiants de ce DEA sont en majorité des scientifiques, titulaires d'une maîtrise ou d'un diplôme d'ingénieur.

LES SOURCES D'INFORMATION

En intelligence économique, la variété des sources d'information est extrême, allant de l'information scientifique à l'information économique, politique et financière. La consultation des « sources ouvertes » externes est ici essentielles. On peut notamment citer :

- les bases informatiques de données de plus en plus accessibles via l'internet;

- la consultation de revues, journaux, publications périodiques diverses dés la parution de manière à capter l'information plus rapidement que sur les bases de données;

- les revues spécialisées, les ouvrages, les encyclopédies, les thèses universitaires;

- les brevets dont le contenu informatif peut être exploité pour la détection de technologies nouvelles, la surveillance globale de secteurs techniques et de la concurrence;

- les rapports des conseillers d'ambassades;

- les sites internet des entreprises; il existe aussi des sites d'intelligence économique ;

- les rapports annuels d'activité des entreprises;

- les normes juridiques présentes et en projet : une politique active de lobbying ne se conçoit pas sans participer activement à l'élaboration des normes;

- les congrès et les colloques;

- les forums de discussion sur l'internet;

- les expositions et les foires où il est intéressant de récolter les prospectus et les échantillons de la concurrence;

- les études multi-clients réalisées sur commande par des firmes spécialisées.

Pour une entreprise, la consultation de ses rapports et notes internes est une source très importante d'information technologique qui ne doit pas être négligée. Un certain nombre de grands groupes ont constitué des banques de données internes aisément interrogeables où se trouve archivé le savoir-faire de la société. Ces banques de données internes constituent naturellement la cible privilégiée de l'espionnage économique.
La recherche et la collecte de renseignements informels, sont aussi des opérations capitales en intelligence économique. Il s'agit d'une information non structurée, délicate ou très difficile à obtenir et qui ne peut être recueillie que par des réseaux de « correspondants spécialisés » auprès des clients, des sous-traitants, des concepteurs d'installations industrielles, des délégués commerciaux, etc. ... Cette information concerne essentiellement les besoins de la clientèle, le remplacement prévisible d'un produit, son évolution, les projets des concurrents.

La recherche de ce type d'information, qui n'a aucune chance d'être obtenu sur les bases de données traditionnelle, doit faire l'objet d'un plan de renseignement.

INTELLIGENCE ECONOMIQUE OU ESPIONNAGE ECONOMIQUE ?

Selon François Jakobiak, tout spécialiste de l'intelligence économique a intérêt à étudier ce que les spécialistes de la Défense Nationale ont réalisé ou écrit dans ce domaine pour en tirer de profitables leçons. Et le conférencier de préconiser aux entreprises l'établissement de plans de renseignement semblables à ceux des services de renseignement français. On retrouve en effet dans les modèles de plans proposés les opérations typiques du cycle du renseignement militaire (acquisition, appréciation, interprétation, communication du renseignement).

François Jakobiak insiste néanmoins sur le fait que l'intelligence économique doit s'attacher à utiliser l'information ouverte, ce qui n'est pas nécessairement le cas des services de renseignement, « habitués, quant à eux, à opérer dans la clandestinité au profit du Gouvernement ». En France, beaucoup de chef d'entreprises se méfient d'ailleurs du terme « intelligence économique », car il évoque pour eux les activités d'espionnage de l' « Intelligence Service" britannique ou de la « Central Intelligence Agency » américaine.

Conscient que l'on se trouve ici à la frontière de l'information ouverte et de l'information fermée (celle qui n'est pas donnée de plein gré), François Jakobiak rappelle pourtant qu'il ne faut pas faire d'amalgame entre l'espionnage industriel et l'intelligence économique. Il est donc impératif de bien définir l'éthique et la déontologie de l'entreprise en cette matière. Quelles sont les limites à ne pas franchir ? Et François Jakobiak de proposer la mise en oeuvre des quelques préceptes suivants :

- seule l'information ouverte est prise en compte;

- la discrétion est de mise mais il faut savoir que l'on obtient souvent des renseignements en en fournissant soi-même en échange;

- il appartient à chaque correspondant de juger de ce qu'il peut dire ou ne pas dire;

- il est vivement recommandé de faire preuve de fair-play.

LES PRATICIENS DE L'INTELLIGENCE ECONOMIQUE.

Les praticiens de l'intelligence économique proviennent de quatre « écoles » différentes :

- les spécialistes de la veille technologique constituent la première école et sont le plus souvent des ingénieurs qui ont fort bien compris la nécessité d'évoluer vers l'intelligence économique;

- la seconde école, d'inspiration plus commerciale, est celle des spécialistes du marketing ou de l'analyse concurrentielle;

- la troisième école est constituée par des spécialistes du renseignement militaire reconvertis dans l'intelligence économique;

- une quatrième école provient de fonctionnaires de police qui apportent leur connaissance des techniques d'enquêtes et de collecte de renseignements.

INFLUENCE ET LOBBYING

Le rapport Martre ne mentionne pas l'influence et le lobbying dans ses propositions relatives au développement de l'intelligence économique dans les entreprises françaises. L'influence serait donc plutôt une des composantes de l'intelligence économique d'Etat. Les possibilités d'influence et de lobbying des entreprises étant plus limitées que celles de l'Etat, il arrive donc que celles-ci s'adressent à des organismes officiels, à des ministères ou à des organismes

internationaux pour défendre leurs intérêts, notamment au niveau de l'élaboration des normes. Le Japon s'en est d'ailleurs fait une spécialité.

Aux Etats-Unis, on voit émerger un savoir-faire de type nouveau, celui de l' « InfoWar". Il s'agit pour une nation, de défendre ses industries en mobilisant ses ressources informationnelles (dont les structures électroniques comme l'internet) pour mettre en oeuvre des politiques d'influence fondées sur des guerres de l'information, c'est-à-dire la diffusion aux acteurs décisifs d'informations déstabilisatrices.

La guerre de l'information est donc l'utilisation offensive de l'information afin d'affaiblir, de déstabiliser, ou de détruire un adversaire. Les techniques utilisées peuvent être la désinformation, la manipulation d'information, les rumeurs ou la propagande. On ne peut prévenir et lutter contre ces méthodes qu'en maîtrisant soi-même les techniques offensives de la guerre de l'information.

CONCLUSIONS DU COMITE R.

L'intelligence économique, exploitation systématique de l'information pour des décisions stratégiques dans le domaine économique, résulte de la mondialisation des échanges et la vigueur de la compétition qui règne dans ce secteur. Comme dans le domaine militaire, il s'agit d'abord d'être bien informé, de bien interpréter, d'agir en conséquence et de faire, si nécessaire, un usage offensif de l'information. Cette pratique s'intègre de plus en plus au management et à la stratégie des grandes entreprises. L'Etat est lui-même appelé à jouer un rôle important dans l'intelligence économique.

En Belgique, un premier pas vient d'être franchi dans ce sens puisque la Sûreté de l'Etat a reçu la mission de participer à la protection du potentiel scientifique et économique du pays. Il ne s'agit encore que d'une démarche de nature défensive.

La Sûreté de l'Etat de l'Etat ne sera pourtant en mesure de s'acquitter de sa nouvelle mission que si :

- elle reçoit des moyens humains et matériels nécessaires;

- elle s'imprègne de cette nouvelle culture qu'est l'intelligence économique.

Il lui sera nécessaire à cet effet de tisser des liens étroits avec les acteurs économiques du pays.

LA PARTICIPATION AU COURS DE L'ANNEE 2000 DU COMITE R A DES REUNIONS DE TRAVAIL, SEMINAIRES, CONFERENCES ET COLLOQUES

- Conférence organisée le mercredi 1er mars 2000 par *« L'institut Supérieur de Défense (IRSD)* » sur le thème : *« Où va la Russie ?»*

- Conférence de R. Steele organisée par les Comités P et R sur le thème : « The recent developments in the field of open source intelligence in North-America » le 14 avril 2000.

- Participation au séminaire *« Maîtriser les outils de la veille économique* » organisé à Paris les 16 et 17 mai 2000 par *« L'institute for International Research* ».

- Participation à la Conférence organisée par le « *Haut Comité Français pour la Défense Civile »* à Lyon les 17, 18 et 19 mai 2000 par « sur le thème : « *Le risque biologique ».*

- Le 2 août 2000, les Comités P et R ont reçu la visite de deux membres des commissions parlementaires de suivi.

- Le 18 septembre 2000, les membres du Comité R ont participé à une séance d'information des stagiaires de la Sûreté de l'Etat. Divers exposés ont été présentés à cette occasion concernant la législation organique du contrôle et le rôle du Comité R.

- Le 3 octobre 2000, conférence du soir de l'IRSD *« Les relations internationales. Le rôle de la diplomatie et les possibilités de coopération avec les militaires ».*

- Le 23 octobre 2000, le Comité R a organisé un échange de vues avec un responsable du Groupe-Interforces anti-terroristes (GIA) au sein duquel la Sûreté de l'Etat et le SGR sont représentés.

- Le 27 octobre 2000, les Comités P et R ont participé à une séance d'information sur le réseau de communication A.S.T.R.I.D.

- Le 7 novembre 2000, conférence du soir de l'IRSD « Les tribunaux internationaux ».

- Participation au séminaire «*Eufis* » organisé à Bruxelles les 19 et 20 octobre 2000 sur le thème : « *Open Source Workshop ».*

- Le 29 novembre 2000 conférence de l'IRSD organisée sur le thème *« Des opérations humanitaires de soutien de la paix et la coopération civilo-militaire »*

- Le 1er décembre 2000 échange de vues organisé par le Sénat avec Duncan Campbell concernant le système d'écoutes *« Echelon »*

- Conférence organisée à Paris les 7 et 8 décembre 2000 par le Haut Comité français pour la défense civile sur le thème «*La défense civile de la France à l'aube du XXIème siècle – constat et avenir ».*

TITRE IV : COMPOSITION ET FONCTIONNEMENT DU COMITE R

COMPOSITION ET FONCTIONNEMENT DU COMITE R

COMPOSITION

Depuis la nomination, le 26 novembre 1999, comme membre du Comité permanent de contrôle des services de police (Comité P), de madame Danielle Cailloux qui faisait partie jusqu'à cette date du Comité R, les trois membres restant ont poursuivi l'exercice de leur mandat.

La loi du 1er avril 1999 (moniteur belge du 3 avril 1999) modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements avait réduit la composition du Comité R à un seul membre effectif permanent, le président, et à deux membres effectifs non permanents.

La loi du 20 juillet 2000 (moniteur belge du 1er août 2000) a modifié à nouveau la composition du Comité R. Celui-ci comportera trois membres à temps plein parmi lesquels un président. Un suppléant sera nommé pour chacun d'eux.

A la date d'approbation du présent rapport général d'activités, la nomination des trois nouveaux membres du Comité R n'est pas encore intervenue, de sorte que, les trois membres encore en fonction sont :

Monsieur Jean-Claude Delepière, président
Monsieur Gérald Vande Walle, membre
Monsieur Jean-Louis Prignon, membre

Ceux-ci continuent à exercer leurs fonctions jusqu'à la nomination de leurs remplaçants.

LE GREFFIER

Le Comité R est assisté d'un greffier, lui aussi nommé par le Sénat. Il assure le secrétariat des réunions du Comité R, en dresse les procès-verbaux et veille à l'expédition des pièces et à la conservation des archives. Le greffier est également responsable de la protection du secret de la documentation et des archives. Sa fonction est d'une durée indéterminée. Comme les membres du Comité R, il doit être titulaire d'une habilitation de sécurité du niveau "très secret".

Le greffier actuel du Comité R est monsieur Wouter De Ridder.

LE SERVICE D'ENQUETES

Le cadre actuel du Service d'enquêtes est de cinq personnes.

Le chef du Service d'enquêtes est nommé par le Comité R pour un terme de cinq ans renouvelable une fois. Il doit être une personne d'expérience choisie parmi des magistrats, des membres ou des fonctionnaires des services de renseignements ou de police. Il doit connaître les langues française et néerlandaise. Le chef actuel du Service d'enquêtes est monsieur Paul vander Straeten, premier substitut du procureur du Roi au parquet de Bruxelles.

Les membres du Service d'enquêtes sont nommés par le Comité R sur proposition du chef du Service d'enquêtes. Pour pouvoir être nommés, le chef et les membres du Service d'enquêtes doivent également être titulaires d'une habilitation de sécurité du niveau "très secret".

Les quatre membres actuels du Service d'enquêtes ont été nommés pour un terme renouvelable de cinq ans par détachement d'un service de police ou de renseignement.

C'est ainsi qu'au cours de l'exercice écoulé, les mandats de deux membres du Service d'enquêtes ont été renouvelés pour un nouveau terme.

LE PERSONNEL ADMINISTRATIF

Au cours de l'année 2000, le recrutement d'une collaboratrice-documentaliste de niveau 1 a été concrétisé.

A la parution du présent rapport d'activités, le cadre administratif du Comité R se compose donc des collaborateurs suivants :

- une documentaliste ;
- un comptable à titre statutaire;
- une secrétaire à titre statutaire;
- une employée à titre statutaire;
- un huissier à titre statutaire;
- une réceptionniste à titre statutaire;
- un chauffeur-technicien mis à disposition par les forces armées.

LES ACTIVITES

Le Comité R s'est réuni du 1er janvier 2000 au 31 décembre 2000, cinquante fois. Lors de ces réunions, des décisions ont été prises concernant les enquêtes, les textes du rapport d'activités et la logistique.

Les membres du Comité R se sont réunis 12 fois avec les Commissions de suivi parlementaire.

Outre ce qui est repris au chapitre I, le Comité R a également établi un projet d'arrêté royal permettant à ses membres ainsi qu'aux membres de son Service d'enquêtes d'accéder au Registre national des personnes physiques.
Ce projet a été transmis aux ministres de l'Intérieur et de la Justice par courrier du 6 décembre 2000.

LES MOYENS FINANCIERS

Les moyens du Comité R proviennent d'une dotation qui lui est accordée annuellement par le Parlement.

Depuis la loi du 1er avril 1999, le greffier est responsable des comptes du Comité R. Le règlement interne du Comité R prévoit un contrôle interne des dépenses. Celui-ci est effectué par un des membres du Comité R.

L'exécution du budget est contrôlée par la Cour des Comptes, qui établit chaque année un rapport à la demande de la Chambre des Représentants.

La dotation de l'année budgétaire 2000 se montait à 72.450.000 FB.

Un budget de 73.480.000 FB a été demandé pour l'année 2001.

ACTIVITES CONJOINTES AVEC LE COMITE P

Pendant la période de référence, les deux Comités P et R ont tenu 4 réunions conjointes.

De plus un groupe de travail, composé de membres des deux Comités, des greffiers ainsi que des représentants du personnel administratif, s'est réuni 15 fois au courant de l'exercice 2000 pour élaborer un projet de statut commun du personnel administratif.
Ce projet a été finalisé. Il a été communiqué le 7 juillet 2000 au président de la Chambre des Représentants.