

TABLE DES MATIERES

PRÉAMBULE.....	I
TITRE 1. LE SUIVI DES RECOMMANDATIONS PARLEMENTAIRES	1
TITRE 2. LES ENQUETES DE CONTRÔLE.....	9
A. ENQUETES A LA REQUETE DU PARLEMENT OU DES MINISTRES9 COMPETENTS	
CHAPITRE 1 : L'ENQUÊTE DE CONTRÔLE SUR LA MANIÈRE DONT LA FIRME EPSI A ÉVENTUELLEMENT ÉTÉ SUIVIE PAR LES SERVICES DE RENSEIGNEMENT DANS LE CADRE DE LA LUTTE CONTRE LA PROLIFÉRATION.....	11
1. Introduction	11
2. Les faits tels qu'exposés par la presse	11
3. L'intérêt parlementaire.....	12
4. La Procédure d'enquête.....	12
5. Le cadre législatif et réglementaire belge.....	14
5.1 La loi du 9 février 1981 et ses arrêtés royaux d'exécution	15
5.2 Les règles de l'Union européenne en vue du contrôle des exportations de biens et technologies à double usage et des équipements militaires	15
6. Constatations	16
6.1 Le rôle de La Sûreté de l'État	16
6.2 La façon dont l'Administration des douanes et accises a pris connaissance des faits...	17
6.3 Le traitement de l'information sur la firme EPSI par la Sûreté de l'État.....	18
6.4 Les commentaires de la Sûreté de l'État.....	23
7. Le problème de la communication d'informations classifiées aux fonctionnaires et aux membres de la CANPAN.....	24
8. Conclusions.....	25
9. Recommandations	28

CHAPITRE 2 :	L'ENQUETE DE CONTROLE RELATIVE A UN INCIDENT DE TIR LORS D'UNE GARDE DES LOCAUX DE LA SURETE DE L'ETAT	30
1.	Introduction	30
2.	Procédure.....	30
2.1	L'enquête de contrôle	30
2.2	L'enquête judiciaire	31
2.3	Application de l'article 38 § 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements	32
3.	Constatations	32
4.	Recommandations	33
5.	Avis de madame la ministre de la Justice	34
B.	ENQUETES MENEES A L'INITIATIVE DU COMITE PERMANENT R.....	37
CHAPITRE 1 :	ENQUÊTE DE CONTRÔLE SUR UN INCIDENT DE SÉCURITÉ SURVENU AU SGRS	39
1.	Procédure.....	39
2.	Application de l'article 69 §§ 1 à 5 (section 2) du règlement d'ordre intérieur du Comité permanent R.....	39
3.	Constatations	40
3.1	Les états de M. X au sein du SGRS	40
3.2	Les faits constatés entre le 26 et le 27 février 2004	40
3.3	Découverte et traitement de l'incident de sécurité.....	41
3.4	Suites données à l'incident.....	43
4.	Conclusions.....	44
5.	Avis du ministre de la Défense nationale	45
CHAPITRE 2 :	ENQUETE COMMUNE DES COMITES P ET R RELATIVE A LA COORDINATION ENTRE LES DIFFERENTS SERVICES DE RENSEIGNEMENT ET DE POLICE DANS LA LUTTE CONTRE LE TERRORISME.....	47
C.	PLAINTES DE PARTICULIERS ET DENONCIATIONS	48
CHAPITRE 1 :	PLAINTÉ D'UN PARTICULIER À L'ENCONTRE DE L'ADMINISTRATEUR GÉNÉRAL DE LA SURETÉ DE L'ÉTAT	49

<u>CHAPITRE 2</u> : ENQUÊTE SUR LES INFORMATIONS RECUEILLIES, TRAITÉES ET COMMUNIQUÉES PAR LA SÛRETÉ DE L'ÉTAT À PROPOS DE LA DEMANDE DE RÉGULARISATION DE SÉJOUR D'UN PLAIGNANT	50
<u>CHAPITRE 3</u> : ENQUÊTE DE CONTRÔLE SUITE À UNE PLAINTÉ D'UN PARTICULIER CONCERNANT LA TRANSMISSION D'INFORMATIONS PAR LA SURETÉ DE L'ÉTAT À L'OFFICE DE LA NAISSANCE ET DE L'ENFANCE	51
1. Introduction	51
2. Procédure.....	51
3. L'objet de la plainte	51
4. Les vérifications effectuées par le Comité permanent R.....	52
5. Constatations	53
6. La position de la Sûreté de l'Etat.....	55
7. Conclusions.....	56
8. Recommandations	57
9. Echange de vues entre la Ministre de la Justice, le Comité permanent R et la Sûreté de l'Etat.....	57
<u>CHAPITRE 4</u> : PLAINTÉ D'UN SOUS-OFFICIER À L'ENCONTRE DU SGRS	59
D. LES ENQUETES EN COURS.....	60
<u>CHAPITRE 1</u> : LE RÔLE DES SERVICES DE RENSEIGNEMENT EN MATIÈRE DE LUTTE CONTRE LA PROLIFÉRATION	61
<u>CHAPITRE 2</u> : DEPLACEMENTS DE PERSONNES VERS DES ZONES SENSIBLES.....	62
<u>CHAPITRE 3</u> : LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE : ENQUÊTE SUR LE SUIVI ÉVENTUEL D'UNE FIRME BELGE	62
<u>CHAPITRE 4</u> : SUIVI DE L'ENQUÊTE SUR L'ISLAMISME RADICAL.....	62

<u>CHAPITRE 5</u> : L'ENQUÊTE SUR LA MANIÈRE DONT LE SGRS ORGANISE LA CONSERVATION, LA GESTION ET L'EXPLOITATION (INFORMATIQUE) DES DONNÉES À CARACTÈRE PERSONNEL QU'IL RECUEILLE	63
TITRE 3. LE CONTROLE DES INTERCEPTIONS DE SECURITE	65
TITRE 4. LES ENQUETES JUDICIAIRES	69
TITRE 5. LES QUESTIONS POSÉES AUX SERVICES DE RENSEIGNEMENT	73
<u>CHAPITRE 1</u> : L'APPLICATION DES STATUTS SYNDICAUX DES MEMBRES DU PERSONNEL DU SGRS.....	76
<u>CHAPITRE 2</u> : L'APPLICATION DE L'ARTICLE 14 DE LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ - ACCORDS ÉVENTUELLEMENT PASSÉS ENTRE LA SÛRETÉ DE L'ÉTAT ET DES SERVICES PUBLICS	79
<u>CHAPITRE 3</u> : LA CONTRIBUTION APPORTÉE PAR LES SERVICES DE RENSEIGNEMENT À LA CONFECTION DES LISTES TERRORISMES	80
<u>CHAPITRE 4</u> : LA DIFFUSION D'IMAGES SATELLITAIRES SUR L'INTERNET.....	82
<u>CHAPITRE 5</u> : LE FONCTIONNEMENT DE LA SECTION « LÉGISLATION EN MATIÈRE D'ARMES » DE LA SÛRETÉ DE L'ÉTAT	86
TITRE 6. ETUDES ET ACTIVITES	93
<u>CHAPITRE 1</u> : L'ÉTUDE SUR LE POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE	95
1. La difficulté de définir le potentiel scientifique et économique d'un pays	96
2. Notions connexes : les matières d'intérêt économique stratégique, les besoins et les intérêts vitaux de la Nation, le potentiel socio-économique du pays	96
2.1 La loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques	97
2.2 L'arrêté royal du 18 avril 1988 portant création du Centre Gouvernemental de Coordination et de Crise	97

2.3	L'arrêté royal du 31 janvier 2003 portant fixation du plan d'urgence pour les événements et situations de crise nécessitant une coordination ou une gestion à l'échelon national.....	97
2.4	L'arrêté royal du 17 octobre 2003 portant fixation du plan d'urgence nucléaire et radiologique pour le territoire belge	98
2.5	La Banque de données CRIVISEN (points CRItiques, VItaux et SENSibles).....	98
3.	La consultation : questions et réponses	99
3.1	Les questions posées	100
3.2	Les réponses obtenues	101
4.	Le rapport d'expertise	109
5.	La protection du potentiel scientifique et économique à l'étranger	115
5.1	En France	115
5.2	Aux Pays Bas	117
5.3	En Allemagne	118
5.4	En Grande Bretagne	119
6.	Le contrôle des investissements étrangers	120
6.1	En Europe	120
6.2	La France	120
6.3	Aux États-Unis	123
7.	Synthèse des points de vue recueillis	123
7.1	Comment définir les éléments essentiels du potentiel scientifique ou économique d'un pays comme la Belgique ?	123
7.2	Qui sont les moteurs de ce potentiel scientifique et économique ?.....	125
7.3	Quelles menaces visent ce potentiel scientifique et économique ?	126
7.4	A quelles difficultés se heurte la protection du potentiel économique et scientifique de notre pays ?.....	128
7.5	Comment attribuer un caractère national au potentiel scientifique et économique du pays ?.....	129
7.6	Comment définir le secret en matière économique, scientifique et technologique et situer sa place dans une économie caractérisée par les mutations technologiques, la circulation de l'information et son ouverture internationale ?	130
7.7	Comment la Sûreté de l'État doit-elle prendre sa mission en charge dans cette matière ?	131
8.	Conclusions	134
8.1	Les conclusions du rapport d'expertise	134
8.2	Les conclusions du Comité permanent R	135
8.3	Quelques constatations	136
8.4	Une autre approche	137
 <u>CHAPITRE 2</u> : ASSISTANCE A LA REDACTION DU PROJET DE LOI RELATIF A L'ANALYSE DE LA MENACE		139
 <u>CHAPITRE 3</u> : LISTES TERRORISTES		140

1.	Aperçu et état des lieux des procédures judiciaires.....	140
1.1.	Liste 1267	141
1.2.	Liste 1373a	146
1.3.	Liste 1373b	148
2.	De la pertinence d'une liste belge	149
3.	Conclusion	150
<u>CHAPITRE 4</u> :	ETUDE JURIDIQUE COMPARÉE PORTANT SUR CERTAINS ASPECTS DE L'INTERACTION ENTRE LES SERVICES DE RENSEIGNEMENT ET LA JUSTICE	151
1.	Obligation ou possibilité de transmettre aux autorités judiciaires des informations relatives à un délit	151
2.	Possibilité de fournir une "assistance technique"	151
3.	Utilisation en justice de données que les services de renseignement ont obtenues légalement par des méthodes auxquelles la justice ne peut peut-être pas recourir	152
4.	Les données des services de renseignement comme moyen de preuve ou comme information de départ ou d'orientation	152
<u>CHAPITRE 5</u> :	LE CONTRÔLE DEMOCRATIQUE DES SERVICES DE RENSEIGNEMENT – SEMINAIRE	153
TITRE 7. LES ACTIVITÉS DU COMITÉ PERMANENT R EN TANT QU'ORGANE DE RECOURS.....		155
<u>CHAPITRE 1</u> :	MODIFICATIONS RELATIVES A LA MISSION ET A LA COMPOSITION DE L'ORGANE DE RECOURS	157
<u>CHAPITRE 2</u> :	ACTIVITES DE L'ANCIEN ORGANE DE RECOURS.....	158
<u>CHAPITRE 3</u> :	LA QUESTION PREJUDICIELLE ET L'ARRET DE LA COUR D'ARBITRAGE	160
TITRE 8. LA COMPOSITION ET LE FONCTIONNEMENT DU COMITE PERMANENT R		161
<u>CHAPITRE 1</u> :	LA COMPOSITION DU COMITE PERMANENT R.....	163

<u>CHAPITRE 2</u> :	LA COMMISSION PARLEMENTAIRE DE SUIVI	164
<u>CHAPITRE 3</u> :	LES ACTIVITÉS DE GESTION DU COMITE PERMANENT R.....	165
<u>CHAPITRE 4</u> :	LES MOYENS FINANCIERS	166
<u>CHAPITRE 5</u> :	LES RELATIONS AVEC DES ORGANES DE CONTRÔLE ETRANGERS.....	167
1.	La rencontre avec l'autorité de contrôle néerlandaise.....	167
2.	La Participation au colloque du « Comité canadien de Surveillance des Activités de Renseignement et de sécurité ».....	168
2.1	Le contrôle des services de renseignement et de sécurité	168
2.2	Le contrôle des services de renseignement à l'heure des menaces terroristes.....	170
2.3	Remarques finales.....	170
<u>CHAPITRE 6</u> :	PARTICIPATION DU COMITÉ PERMANENT R A DES SEMINAIRES, JOURNEES D'ETUDE ET COLLOQUES	172
1.	Journée d'étude sur le rôle des organisations internationales dans la lutte contre le terrorisme	172
2.	Rapport de la conférence sur « INFORMATION OPERATIONS »	172
2.1	Qu'entend-on par 'INFORMATION OPERATIONS' ?	172
2.2	Contexte historique.....	174
2.3	Les IO sur le plan politique et éthique	175
2.4	L'application des Information Opérations dans les zones actuellement en guerre ou en crise.....	176
2.5	Information Operations et renseignements	179
2.6	Conclusions	180
3.	Séminaire sur les « listes terrorismes »	181
4.	Le colloque 'Military satellites'.....	182
5.	Les rencontres pour l'Innovation, la Compétitivité et la Connaissance	183
6.	Séminaire EUROMED JUSTICE « Définition et incriminations pénales. Aspects transversaux du crime organisé »	190
7.	Séminaire sur le « terrorisme »	191

PREAMBULE

Considérations générales

Le rapport d'activités 2005 est le 13^{ème} rapport général d'activités remis par le Comité permanent R en application de l'article 35, 1^o de la loi organique de contrôle des services de police et de renseignement du 18 juillet 1991.

Ce type de rapport général « *qui comprend, s'il échet, des conclusions et des propositions d'ordre général couvrant la période allant du 1^{er} janvier au 31 décembre de l'année précédente* » est différent des deux autres formes de rapport prévues par le même article aux points 2^o et 3^o, à savoir : les rapports concernant des enquêtes confiées au Comité par la Chambre des représentants ou le Sénat et le rapport fait par le Comité « *lorsque au terme d'un délai qu'il estime raisonnable, il constate qu'aucune suite n'a été réservée à ses conclusions, ou que les mesures prises sont inappropriées ou insuffisantes* » et qu'il en fait rapport au parlement.

Ce rapport est aussi le dernier rapport du Comité permanent R dans sa composition actuelle telle qu'elle résulte des nominations faites par le Sénat en septembre 2001, pour une durée de cinq ans expirant le 19 septembre 2006.

Le rappel du début de cette période est également celle des événements tragiques du 11 septembre 2001, qui entre autres choses, ont focalisé une attention accrue sur les services publics de renseignement et sur la fonction essentielle que ceux-ci doivent remplir de manière primordiale aussi bien pour la protection des valeurs démocratiques que pour celle intimement liée aux droits et libertés fondamentales des personnes.

Ces principes sont clairement énoncés aussi bien dans la loi organique du contrôle des services de police et de renseignement, que dans la loi organique des services de renseignement et de sécurité du 30 novembre 1998.

En ne prenant comme exemples pour la période 2001 à 2006, que les rapports du Comité permanent R concernant « Echelon », « l' Islamisme Radical », « les vols CIA », on comprend que l'évaluation des différents aspects de l'efficacité du renseignement (le recueil de l'information, son traitement et son analyse, ainsi que sa communication aux destinataires légitimes) se doit toujours d'être confrontée en finale à l'aune de la protection des droits et libertés fondamentales.

Le contrôle du Comité permanent R est exercé pour le compte du pouvoir législatif et aussi dans une certaine mesure, pour le compte des ministres de tutelle des deux services de renseignement belges, la Sûreté de l'Etat et le Service Général du Renseignement et de la Sécurité des Forces armées (SGRS).

Ce contrôle reste toujours indissociablement liée, que cela soit explicite (par exemple dans le cas de plaintes de particuliers) ou implicite (comme dans le cadre d'enquêtes plus générales sur le fonctionnement des services dans le contexte de missions liées à la menace extrémiste ou à des menaces contre le potentiel scientifique et économique du pays) à la protection des droits et libertés démocratiques que les personnes sont en droit d'attendre non seulement de l'ordre juridique national, mais aussi des ordres juridiques européen et international.

La notion d'efficacité des services de renseignement, qui est une des facettes sur laquelle porte le contrôle légal du Comité permanent R, ne se conçoit donc uniquement que dans ce contexte.

Le second alinéa de l'article 2 de la loi du 30 novembre 1998, organique des services de renseignement et de sécurité, consacre cette philosophie dans son libellé : « *Dans l'exercice de leurs missions, ces services veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société* ».

Cette finalité, à l'exception de tout autre, est celle qui justifie la raison d'être des services publics de renseignement et leur confère une spécificité intrinsèque qui les distingue essentiellement de toutes les activités privées de renseignement.

Cette finalité doit une fois de plus être soulignée. Qu'il soit clair que le rôle d'un organe comme le Comité permanent R est d'être critique et parfois sans complaisance. Cela ne signifie pourtant pas que dans son ensemble, le travail des services et de leurs agents doit être systématiquement mis en cause. Ce travail exercé dans des conditions souvent difficiles, peu connues ou comprises du public, mérite d'être pris en considération.

La logique du contrôle voulue par le législateur belge – qui aujourd'hui est soulignée d'une manière plus large par la Commission temporaire d'enquête du Parlement européen¹ concernant les vols présumés de la CIA en ces termes : « *... les règles régissant les activités des services secrets semblent inadéquates dans plusieurs États membres de l'Union, ce qui rend nécessaire la mise en place de meilleurs contrôles...* » - est essentiellement d'initier et de développer une dynamique d'intégration et de progrès de la fonction de renseignement nationale – et peut-être un jour européenne - adaptée à l'évolution d'un monde ouvert, conflictuel et multipolaire où les menaces sont multiples, diffuses et en continuelle mutation, dans lequel le modèle démocratique a beaucoup à gagner, tout en étant constamment menacé. Dans un État démocratique, cette logique commande de soutenir, comme le Comité permanent R n'a cessé de le faire, que les services de renseignement et de sécurité, demeurent distincts des services de police.

Cette logique se doit d'éviter l'écueil du « *politiquement correct* » souvent associée à une culture inappropriée du secret. Elle se doit aussi en sens inverse, d'éviter un autre écueil, celui de la transparence incorrecte qui n'alimente que le sensationnel au détriment des vrais débats et donc de la recherche des vraies solutions. Le renseignement n'est-ce pas également « l'Intelligence » ?

Mais si cette finalité doit aussi être soulignée, c'est parce qu'aujourd'hui, on se doit d'être conscient du fait que face aux menaces des organisations criminelles (dont le monde du renseignement belge ne semble pas toujours mesurer l'ampleur²) et de l'extrémisme (terreau du rejet de la démocratie avant d'être celui du terrorisme sous toutes ses formes), le recours

1 Parlement Européen, Commission temporaire sur l'utilisation alléguée de pays européens par la CIA pour le transport et la détention illégale des prisonniers, Projet de rapport intérimaire, 2006/2027, PE 372.179v01-00, 24 avril 2006.

2 Dans son rapport général d'activités 2004, le Comité permanent R notait ses premières constatations dans le cadre de l'enquête de contrôle sur « la manière dont les services de renseignement belges fonctionnent et collaborent dans le cadre de leur nouvelle mission légale concernant les menaces des organisations criminelles » : « Le Comité permanent R constate une attitude de retrait manifestée par les deux services par rapport à une analyse stratégique de la menace des organisations criminelles relativement à la sécurité nationale. Ce manque de vision stratégique pourrait avoir comme corollaire dans ce domaine un déficit en communication de renseignements pertinents aux autorités politiques. La Sûreté de l'État semble, comme cela a déjà été constaté par le Comité permanent R dans d'autres sphères de ses compétences, privilégier une action à court terme orientée vers des résultats judiciaires », dans Rapport général d'activités 2004, Bruxelles, 2005, pp. 13-19 (www.comiteri.be).

à des mesures d'exception, impliquant notamment le monde du renseignement à l'échelle internationale, constitue des restrictions aux droits et libertés fondamentales des personnes qui semblent s'imposer de plus en plus souvent comme seules réponses.

Sans aller au-delà de cette constatation, et donc sans entrer dans un débat qui n'est pas de sa compétence, le Comité permanent R, reconnaît certainement la nécessité de ce type de mesures pour lutter et éradiquer des menaces graves. Il désire pourtant attirer l'attention sur le fait que ces mesures sécuritaires doivent respecter non seulement les formes juridiques adéquates, mais qu'elles doivent également dans leur exécution rester sous le contrôle effectif des autorités démocratiques légitimes, à tous les niveaux.

Le contrôle mis en place dans notre pays par la loi du 18 juillet 1991, organique des services de police et de renseignement s'est penché de manière récurrente sur certaines des caractéristiques liées à l'aspect international de la communauté du renseignement, dont les moindres ne sont pas la culture du secret, la règle du tiers service et celle du « donnant-donnant ».

Ce faisant le Comité permanent R, n'a jamais remis en cause le bien fondé de ces spécificités. Il s'est cependant attaché, dans la logique pré-rappelée et au travers de dossiers concrets, à vérifier si, sans être autrement précisée, réglementée et contrôlée de manière indépendante, ces spécificités n'étaient pas susceptibles d'engendrer des dysfonctionnements contraires aux finalités légitimes poursuivies, notamment en regard de l'ordre juridique qui s'impose au niveau national à tous les services de sécurité.

Des recommandations sont nées de ces constats³, notamment celles qui, dans le rapport général d'activités du Comité permanent R de 2004 ont porté sur la coopération et la coordination du renseignement, principalement dans le cadre de la lutte contre le terrorisme⁴. Pour rappel, cette recommandation avait été adoptée le 16 juillet 2004 par les Commissions de la Chambre des représentants et du Sénat, chargées du suivi du Comité permanent R⁵.

En 2005, le Comité permanent R a été consulté comme expert technique par le Gouvernement pour participer à la préparation du projet de loi relatif à l'analyse de la menace, répondant ainsi à la recommandation du Parlement. Ce projet de loi vient d'être adopté par le Sénat le 15 juin 2006⁶, après que la Chambre des représentants l'ait également voté le 9 mars 2006.⁷

L'aboutissement de ce processus concrétise de manière exemplaire le mode de fonctionnement équilibré du processus de contrôle parlementaire externe des services de renseignement mis en place par le législateur belge.⁸

Le Comité permanent R estime également que cet exemple précis répond à la logique du contrôle telle qu'elle est soulignée ci-dessus.

3 Voir aussi le présent rapport, Titre 1 : « Le suivi des recommandations parlementaires » .

4 Comité permanent R, *Rapport général d'activités 2004*, Bruxelles, 2005, pp. 4-5 (www.comiteri.be).

5 Doc 3-725/1 (Sénat) DOC 51 1289/001 (Chambre) – Session 2003-2004- 16 juillet 2004 « *Rapport fait au nom de la commission du suivi du Comité permanent de contrôle des services de renseignement et de sécurité et de la commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de contrôle des services de police* » par MM H. Vandenberghe et de Donnéea.

6 Sénat, 2005-2006, 3-171, 15 juin 2006.

7 Chambre, DOC 51 2330/001, 9 mars 2006.

8 Comité permanent R, *Rapport général d'activités 2004*, Bruxelles, 2005, pp. 1-4 (www.comiteri.be).

Un autre exemple concerne la mission confiée au Comité permanent R par la Ministre de la Justice, le 3 décembre 2004, de travailler sur un projet de définition des éléments essentiels du potentiel scientifique et économique du pays à sauvegarder. L'état d'avancement de cette mission est présenté dans le présent rapport⁹.

Le Comité permanent R tient à souligner la coopération apportée à l'étude en cours par la Sûreté de l'État et plus particulièrement par les représentants des services concernés par cette problématique. Cette coopération qui s'est manifestée notamment dans le cadre d'échanges de vues très approfondis, caractérisés par une grande transparence, démontre d'une manière plus générale, que le contrôle peut évoluer autrement et se concrétiser dans ce type de processus, sans que les rôles et les missions légales de chacun ne se trouvent dénaturées. Le Comité permanent R pense être à même d'enrichir ainsi l'information qu'il doit soumettre aux commissions de suivi parlementaire et pallier ainsi, dans une certaine mesure, à l'impossibilité de communiquer en l'état actuel de la législation des informations classifiées aux termes de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, à des destinataires qui bien que pouvant justifier du « besoin d'en connaître » (ce qui est le cas des membres des commissions de suivi parlementaires du Comité permanent R) ne sont pas en possession de l'habilitation de sécurité requise¹⁰.

En partant de ces considérations générales, ce préambule tient à mettre en évidence certains problèmes particuliers à résoudre pour améliorer le contrôle et le fonctionnement des services de renseignement. Ces points sont abordés séparément ci-après.

L'application de l'article 33 de la loi du 18 juillet 1991 organique des services de police, de renseignement et de sécurité

Dans son rapport d'activités général de 2001, le Comité permanent R reprenait une série d'informations qu'il estimait indispensables pour accomplir sa mission plus efficacement, et cela nonobstant l'existence de l'article 33 de la loi du 18 juillet 1991 qui impose aux services de renseignement « *de transmettre d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services. Le Comité permanent R et son service d'enquêtes ont le droit de se faire communiquer les textes qu'ils estiment nécessaires à l'accomplissement de leur mission* »¹¹.

Le Comité permanent R rappelle donc les 15 points évoqués à ce sujet dans son rapport général d'activités 2001, pour lesquels aucune modification n'a été apportée à l'article 33 dont question.

Le Comité permanent R complète cette demande faite en 2001, par la constatation que l'article 33 dans sa formulation actuelle n'est pas correctement appliqué ou est appliqué avec retard ou de manière lacunaire, une interprétation littérale étroite des mots « *règlements et directives* » utilisés par la loi, étant privilégiée.

Cela vaut également pour les demandes de communication adressées par le Comité permanent R ou son service d'enquêtes. Au cours du dernier exercice de contrôle, ces communications n'ont pas toujours été sans poser de problèmes, notamment dans des dossiers délicats. Cet état de chose a parfois amené le Comité permanent R à recourir à des moyens plus intrusifs (saisies de documents) ou coercitifs (convocation par exploits d'huissier) prévus par la loi.

⁹ Voir aussi le présent rapport, Titre 6 « Études et activités du Comité permanent R ».

¹⁰ Comité permanent R, *Rapport général d'activités 2004*, Bruxelles, 2005, p. 3 : l'état de la question est inchangé à ce jour (www.comiteri.be).

¹¹ Comité permanent R, *Rapport général d'activités 2001*, Bruxelles, 2002, pp. 206-207 (www.comiteri.be).

Le Comité permanent R estime que ces situations portent préjudice à toutes les parties. Il conviendrait de trouver dans l'avenir d'autres solutions pour évoluer réciproquement vers une confiance accrue. Une réflexion devrait être entamée entre les différentes parties concernées par le contrôle des services de renseignement pour aboutir à des procédures acceptables.

Dans un certain nombre d'enquêtes, le Comité permanent R a dû en effet établir des rapports complémentaires parce que des informations pertinentes n'avaient pas été fournies dès le départ, à ses enquêteurs. Il est à signaler que dans des enquêtes récentes, des informations ont été fournies directement et d'initiative par le gouvernement pour permettre au Comité R de préciser les résultats de ses investigations. De telles situations sont de nature à porter préjudice au fonctionnement général des services de renseignement dans notre pays.

En parallèle à ce type de démarche, il conviendrait d'apporter une plus grande précision au libellé de l'article 33 associant, s'il échet, la prévision d'éventuelles sanctions en cas de non-respect des obligations imposées. Le Comité permanent R s'interroge en outre sur la nécessité de faire revoir et d'éventuellement faire préciser ou compléter les procédures internes de manière adéquate, afin non seulement de rendre le contrôle externe moins aléatoire, mais aussi de renforcer le contrôle interne de la hiérarchie et de favoriser ainsi la concertation préconisée ci-avant.

Le contrôle de la classification

Un des paradoxes lié au contrôle des services de renseignement est sans doute de concilier la nécessité du secret avec celle d'une transparence indispensable au bon fonctionnement démocratique des divers pouvoirs.

La nécessité du secret est consacrée par la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, attestations et avis de sécurité¹².

La transparence est quant à elle nécessaire pour l'exercice d'un contrôle parlementaire externe.

Les deux aspects peuvent sembler contradictoires et engendrer une méfiance réciproque. Celle-ci ne peut se résoudre que par un travail, sans doute de longue haleine. Ce travail a débuté en 1991 avec la loi organique du contrôle des services de police et de renseignement. Mais dans ce domaine, on peut parfois regretter que la subjectivité, les idées préconçues et les préjugés l'emportent encore sur l'objectivité.

Pour revenir à la transparence, il est certain qu'elle ne peut signifier la mise systématique sur la place publique de tous les dossiers et de tous les éléments qu'ils contiennent. Transparence n'est donc pas synonyme de publicité. La transparence n'est que la conséquence de la place et des missions des services de renseignement et de sécurité : d'une part informer les autorités politiques pour permettre des prises de décision adéquates et en temps utile et d'autre part, se soumettre au contrôle externe du Parlement.

Au-delà de cela, la publicité si elle est requise peut revêtir des formes différentes, être évaluées en fonction du moment et des impératifs de sécurité ou de l'importance des intérêts légitimes en jeu. Ceux-ci sont définis aussi bien dans la loi organique des services de renseignement que dans la loi sur la classification et les habilitations de sécurité.

¹² M.b., 7 mai 1999.

Une condition semble d'emblée essentielle : que la décision de communiquer qui pour le surplus reste de la compétence d'appréciation de chacun des pouvoirs constitutionnels, fasse le cas échéant l'objet d'une concertation. Si nécessaire, une réflexion pourrait être entamée sur ce sujet après étude comparative des procédures qui existent dans d'autres pays en la matière.

Après 13 années d'existence, le Comité permanent R peut affirmer que la plupart des sujets de ses enquêtes ont pu être valablement débattus en commissions parlementaires sans qu'il soit nécessaire de leur communiquer des informations classifiées. La classification couvre, dans la plupart des cas, des détails opérationnels ou l'identité de personnes dont la connaissance n'apporte aucun élément essentiel aux questions de principe soulevées par les débats.

En ce qui concerne la nécessité du secret ou d'une manière plus générale de la classification, le Comité permanent R a souligné à plusieurs reprises que notre système légal ne prévoyait en l'espèce aucun système de contrôle ou de recours en cas de classification abusive ou détournée de sa finalité. Le Comité permanent R souhaite que ce principe d'un organe de contrôle indépendant ou d'un recours soit dès à présent admis.

La notion de dossiers de renseignement

Le Comité permanent R a souvent du faire appel, lorsque ses enquêtes portaient sur des sujets thématiques, à l'exploitation des sources ouvertes, voire à des experts externes pour pouvoir exercer sa mission de contrôle en connaissance de cause.

Plus récemment, et notamment dans le cas de dossier concernant des plaignants, mais pas uniquement, le Comité permanent R a constaté qu'avant de commencer le moindre travail de contrôle à la Sûreté de l'État, il lui a fallu reconstituer lui-même un dossier, les pièces concernant l'affaire étant, soit à rechercher à différents endroits, soit manquantes, soit encore inexistantes en la forme ou lacunaires.

Dans un cas, il a été constaté que l'existence à la Sûreté de l'État de dossiers dits « réservés » n'était pas détectable par la consultation de la base de données informatisées ; que certains de ces dossiers étaient manquants, ou bien introuvables ; qu'il n'a pas été possible de déterminer si ces dossiers étaient complets, toujours en traitement ou s'il s'agissait d'archives.

Il est bien évident que sans pouvoir affirmer que ces constatations s'appliquent à tous « les dossiers » de la Sûreté de l'État, il n'en reste pas moins vrai qu'une telle situation pose problèmes dans les cas d'espèce, surtout lorsque des informations de nature personnelle sont transmises par la suite à d'autres autorités et sont susceptibles d'avoir des conséquences directes sur les plaignants concernés. Il faut préciser que ces cas ne tombent pas dans le champ d'application des recours en matière d'avis, d'attestation et d'habilitations.

Une constatation similaire a été faite au cours de l'année 2006 dans l'enquête de contrôle sur l'affaire « Erdal »¹³.

13 Le rapport de cette enquête est disponible sur le site du Comité permanent R : www.comiteri.be

Le Comité permanent R recommande particulièrement dans le contexte de la révision ou de la mise en place de procédures plus appropriées dont question ci-dessus, de tenir compte des présentes constatations en vue d'assurer une conservation rigoureuse et systématique des dossiers en cours et de leur contenu, ainsi que des archives.

L'application de l'article 38 de la loi organique du contrôle des services de renseignement

L'article 38 précité prévoit en substance, d'initiative ou sur demande, la communication des jugements, arrêts et informations relatifs aux crimes, délits et procédures pénales mettant en cause des membres des services de renseignements. L'autorisation du juge d'instruction est requise en cas d'instruction judiciaire en cours.

Cette disposition ne prévoit toutefois pas, la communication d'informations pertinentes en relation avec des sujets traités par les services de renseignement, contenues dans des dossiers judiciaires, lorsque leurs membres sont cités à titre de témoins, d'experts ou même de victimes d'infractions dans l'exercice de leurs fonctions.

Ces informations se révèlent parfois nécessaires dans le cadre d'enquêtes de contrôle notamment lorsque des données personnelles concernant des personnes impliquées dans des procédures judiciaires ont été transmises par des services de renseignements et que ces données sont contestées dans le cadre de plaintes déposées auprès du Comité R. Des documents de cette nature peuvent également avoir été saisis dans les locaux d'un service de renseignement dans le cadre d'une instruction judiciaire, il y a parfois quelques années et ces documents peuvent présenter un intérêt déterminant dans le déroulement d'une enquête de contrôle actuelle, alors même que le dossier judiciaire est définitivement clôturé.

Rien ne devrait empêcher dans ces cas, le Comité R de demander accès et copie des pièces utiles à son enquête. Aucune base légale n'impose toutefois aux autorités judiciaires de donner une suite positive à une telle demande. Cette lacune est susceptible de priver l'organe de contrôle d'un accès à des pièces, documents et déclarations qui seraient pertinentes pour son enquête administrative.

Le Comité permanent R recommande que l'article 38 soit étendu à ce type d'informations.

TITRE 1
LE SUIVI DES RECOMMANDATIONS
PARLEMENTAIRES

Les commissions de suivi du Sénat et de la Chambre des représentants ont examiné le rapport général d'activités 2004 du Comité permanent R au cours de leurs réunions des 6 et 13 juin 2005, du 21 février 2006 et du 9 mars 2006.

Au cours de cette dernière réunion, le rapport d'activités 2004 du Comité a été approuvé à l'unanimité des membres présents. Le Parlement s'est basé sur les conclusions et recommandations de ce rapport pour formuler ces propres recommandations.¹

Le Comité permanent R reprend ci-après ces recommandations parlementaires et décrit brièvement les actions entreprises par les différents acteurs en 2005 afin de concrétiser ces recommandations.

COORDINATION ET ÉCHANGE D'INFORMATIONS

« *L'échange des renseignements entre :*

- *la Sûreté de l'État et le SGRS;*
- *ces services de renseignements, les ministres et les autorités administratives;*
- *les autorités judiciaires,*

doit être optimisé.

L'échange insuffisant d'informations entre les services de renseignements, les autorités judiciaires et policières, trouvera dans le futur, pour ce qui est de la lutte contre le terrorisme, une solution à la suite de l'entrée en vigueur du projet de loi relatif à l'analyse de la menace.

En vertu de ce projet de loi, un « Organe de coordination pour l'analyse de la menace (OCAM) sera créé. Cet organe aura comme mission :

- *d'établir un échange d'informations systématique et structuré entre tous les partenaires impliqués dans la lutte contre le terrorisme et l'extrémisme;*
- *d'arriver à des analyses communes de la menace sur la base de cet échange d'informations.*
- *l'échange d'informations entre les services de renseignements et le Comité permanent R doit aussi être optimisé :*
- *le Comité permanent R n'est toujours pas mis au courant de l'ordre du jour et des directives du Comité ministériel du renseignement et de la sécurité; les commissions du suivi ont toutefois insisté déjà plusieurs fois sur ce point auprès du gouvernement;*
- *les commissions du suivi parlementaire appellent les services de renseignements à augmenter la transparence de leurs travaux en publiant un rapport annuel accessible au public. Le site internet de l'AIVD néerlandais peut servir d'exemple.*

Les commissions du suivi parlementaire soulignent qu'une lutte efficace contre la criminalité organisée implique une combinaison de prévention et répression. L'importance d'un échange d'informations rapide entre la Sûreté de l'État, qui travaille de façon préventive, et les autorités judiciaires et policières, qui travaillent de façon pro-active et répressive, paraît évidente.

Les commissions du suivi parlementaire attendent une collaboration concrète et plus étroite à la suite de l'entrée en vigueur de la Circulaire COL 12/2005 du 5 octobre 2005 du Collège des procureurs généraux et de la directive qui en découle du Comité ministériel du renseignement et de la sécurité.

¹ Ann. Parl., Sénat, 9 mars 2006, 2005–2006, 3-1150 et Ann. Parl., Chambre, 9 mars 2006, Doc 51 2336/001.

En ce qui concerne l'interaction entre les services de renseignements et les autorités judiciaires, les commissions du suivi ont demandé une étude au Comité permanent R. La première partie de cette étude est reprise au rapport annuel². La commission souligne que cette étude relève une série de questions de principe et recommande qu'elles soient examinées, par exemple dans le cadre de l'examen du projet de loi relatif à l'analyse de la menace.

Pour ce qui concerne cette sous-partie des recommandations, le Comité permanent R attire l'attention sur le fait que le protocole d'accord avec la police fédérale n'est toujours pas finalisé.³ Toutefois, en 2005, les travaux relatifs au projet de loi devant conduire à la création de l'OCAM ont été poursuivis. Le Comité permanent R a largement contribué à l'avancement des travaux.⁴

Dans le courant de l'année 2005, le Comité permanent R n'a pas été informé de l'agenda et des directives du Comité Ministériel du Renseignement et de la Sécurité. Dans la mesure où le Comité permanent R devra à l'avenir exercer un contrôle sur le fonctionnement de l'OCAM, ceci risque de poser problème.

Les services de renseignements n'ont pas encore rendu public leur rapport annuel concernant l'année 2005.

Pour ce qui concerne l'interaction entre les services de renseignements et le monde judiciaire, le Comité permanent R a demandé une étude juridique comparative approfondie qui devra déboucher en 2006 sur des recommandations consolidées.⁵

LES MÉTHODES SPÉCIALES DE RECHERCHE

Les commissions du suivi parlementaire partagent le souci du Comité permanent R concernant le risque de sécurité et les menaces que font peser les moyens technologiques d'interception des communications non seulement sur les intérêts du pays, mais aussi sur les libertés et droits fondamentaux des citoyens.

Les commissions du suivi parlementaire recommandent au gouvernement d'établir une politique générale et centralisée de la sécurité de l'information basée sur le principe de précaution. Il est également souhaitable de charger un service de résoudre le problème de la protection de l'information.

Les commissions du suivi parlementaire sont satisfaites que la loi du 27 décembre 2005 apportant des modifications diverses au Code d'instruction criminelle et au Code judiciaire en vue d'améliorer les modes d'investigation dans la lutte contre le terrorisme et la criminalité grave et organisée, ait créé un cadre équilibré pour ce qui est de l'utilisation, par les services policiers et judiciaires, des techniques spéciales de recherches de l'information.

Comme elles l'ont indiqué à plusieurs reprises dans le passé, les commissions du suivi parlementaire insistent sur le fait que le recours par les services de renseignements à des techniques spéciales doit être rendu possible sur le plan légal, prévoyant le respect des principes d'égalité, de subsidiarité et de proportionnalité.

² Comité permanent R, *Rapport d'activités 2004*, Bruxelles, 2005, pp. 103-142.

³ Voir Titre 5 Les questions posées aux services de renseignement, chapitre 2 l'application de l'art. 14 de la loi organique des services de renseignements et de sécurité – accord éventuellement passé entre la Sûreté de l'Etat et les services publics.

⁴ Voir Titre 6 Etudes et activités, chapitre 2 Assistance à la rédaction du projet de loi relatif à l'analyse de la menace.

⁵ Voir Titre 6 Etudes et activités, chapitre 4 Etude juridique comparée portant sur certains aspects de l'interaction entre les services de renseignement et la justice.

Il faut dès lors :

- *établir des normes légales;*
- *élaborer des directives précises;*
- *introduire une formation adéquate et des mises en place de procédures internes et externes de contrôle strict.*

Dans la mesure des vérifications opérées par le Comité permanent R, aucune action particulière n'a été entreprise pour ce qui concerne la recommandation visant à charger un service d'apporter une solution à la problématique de la protection de l'information.

Pour ce qui concerne le second aspect – la réglementation légale des “méthodes particulières de renseignements” – le gouvernement a déclaré à plusieurs reprises qu'il s'attellait à la rédaction d'un projet de loi. Le Comité permanent R n'est pas associé à ces travaux. Ce projet devrait être finalisé dans le courant de l'année 2006. Il va de soi que le Comité permanent R étudiera avec l'attention requise ce projet particulièrement important.

PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE

Les commissions du suivi parlementaire soulignent une fois de plus l'importance de la protection du potentiel scientifique et économique de notre pays et rappellent à ce sujet la recommandation du 16 juillet 2004 : « insistant pour que le gouvernement donne un contenu concret aux articles 7 et 10 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ». Par ordre de la ministre de la Justice, le Comité permanent R prépare une étude contribuant à la définition précise de la notion « des éléments essentiels du potentiel scientifique et économique du pays à sauvegarder ».

Les commissions du suivi parlementaire soulignent l'importance de cette étude.

Cette étude a été réalisée par le Comité permanent R dans le courant de l'année 2005. Les résultats de l'étude sont disponibles dans le chapitre 6 Etudes et activités, chapitre 1 l'étude sur le potentiel scientifique et économique.

RECRUTEMENT ET TRAITEMENT DES INFORMATEURS

Les commissions du suivi parlementaire recommandent que des directives écrites soient élaborées quant au recrutement des informateurs et au traitement à leur réserver, qu'ils soient occasionnels ou réguliers.

Se référant aux réponses du ministre de la Justice aux questions parlementaires posées dans le courant de 2005 et début 2006, le Comité permanent R peut déduire que la problématique des informateurs sera traitée dans un projet global qui règlera les méthodes particulières de renseignements.

HABILITATIONS DE SÉCURITÉ

Les commissions du suivi parlementaire recommandent au gouvernement de prévoir, comme condition de nomination pour l'administrateur général de la Sûreté de l'État et son adjoint, dans l'arrêté royal du 17 janvier 1994, qu'ils doivent être titulaires d'une habilitation de sécurité.

Les commissions du suivi parlementaire demandent au gouvernement de désigner une autorité collégiale particulière composée de personnes indépendantes des services de renseignements, pour délivrer ou retirer les habilitations de sécurité aux hauts fonctionnaires dirigeant ces services. Cette autorité serait également compétente pour les autorités qui exercent la tutelle ou le contrôle sur ces services.

La mise en oeuvre des lois du 11 décembre 1998 relatives à la classification et aux habilitations de sécurité semble avoir entraîné une augmentation globale des missions d'enquête et des vérifications de sécurité, surtout dans le domaine nucléaire.

Afin de pouvoir répondre de façon adéquate aux problèmes inhérents à l'augmentation de la charge de travail, les commissions du suivi parlementaire font les recommandations suivantes :

- *il faut que les autorités de sécurité et les services de renseignement tiennent des statistiques précises du nombre d'enquêtes et de vérifications de sécurité effectuées ainsi que du nombre de décisions ou avis négatifs;*
- *il y a lieu de tenir un échéancier afin de déterminer les délais dans lesquels les enquêtes et vérifications sont effectuées.*

Le gouvernement est invité à :

- *procéder à une évaluation objective de la charge de travail engendrée par ces missions;*
- *accorder des moyens humains et techniques suffisants aux services de renseignements pour l'exécution de ces missions.*

L'Arrêté royal du 5 mars 2006 a modifié l'Arrêté royal du 14 janvier 1994 relatif au statut de l'administrateur général et de l'administrateur général adjoint de la Sûreté de l'Etat. Aucune disposition relative à une habilitation de sécurité obligatoire n'y est reprise. Dans la mesure des vérifications opérées par le Comité permanent R, on ne s'est pas penché sur la création d'une autorité collégiale particulière, composée de personnes indépendantes des services de renseignements, qui veilleraient à délivrer ou à retirer des habilitations de sécurité aux hauts fonctionnaires de ces services.

En ce qui concerne la recommandation concrète du Parlement portant sur la mise en oeuvre des lois du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, le Comité permanent R organisera dans le courant de l'année 2006 un tour de table.

SUIVI DE L'AUDIT DE LA SÛRETÉ DE L'ÉTAT

Dans le rapport relatif à l'enquête sur « la transgression éventuelle par des membres de la Sûreté de l'État d'un ordre de cesser le contact avec un informateur » le Comité permanent R estime « que l'on pourrait se trouver devant des indices d'une action concertée trouvant une de ses composantes à l'intérieur même de la Sûreté de l'État en vue de s'opposer à la candidature d'un des postulants à la fonction d'administrateur général de cette administration ».

Ce rapport dénonce une fois de plus certains dysfonctionnements, manipulations et rivalités internes de ce service. Les dysfonctionnements constatés ne sont pas seulement nuisibles au bon fonctionnement du service mais permettent aussi d'échapper à tout contrôle effectif, aussi bien interne qu'externe.

Ces dysfonctionnements ont déjà été constatés dans l'audit que le Comité permanent R avait organisé.

Pour ces raisons, les commissions du suivi recommandent qu'une concertation soit mise en place pour établir un suivi des mesures prises à la suite des constatations de l'audit en ce qui concerne la concentration de certains pouvoirs à certains niveaux de la hiérarchie de la Sûreté de l'État qui rendent possibles des dysfonctionnements incompatibles avec la bonne marche d'un tel service dans un État de droit. »

Pour ce qui concerne cette dernière recommandation, la Sûreté de l'Etat a entrepris diverses actions en 2005. Ces actions n'ont pas fait l'objet d'une évaluation par le Comité permanent R. Toutefois, début 2006, une enquête particulière a été ouverte quant aux flux d'informations et prises de décision au sein des services de renseignements. La problématique soulevée par le Parlement sera examinée en marge de cette enquête.

TITRE 2

LES ENQUETES DE CONTROLE

A. ENQUETES A LA REQUETE DU PARLEMENT OU DES MINISTRES COMPETENTS

CHAPITRE 1 : L'ENQUÊTE DE CONTRÔLE SUR LA MANIÈRE DONT LA FIRME EPSI A ÉVENTUELLEMENT ÉTÉ SUIVIE PAR LES SERVICES DE RENSEIGNEMENT DANS LE CADRE DE LA LUTTE CONTRE LA PROLIFÉRATION

1. INTRODUCTION

Plusieurs articles parus dans les journaux "*Le Soir*" et « *De Gazet van Antwerpen* » les 29 et 30 avril ainsi que le 11 mai 2005 ont attiré l'attention de plusieurs parlementaires parmi lesquels des sénateurs membres de la Commission chargée du suivi parlementaire du Comité permanent R. Ces articles posaient la question de savoir si une firme belge avait exporté ou tenté d'exporter du matériel pouvant contribuer à la prolifération nucléaire en Iran¹.

2. LES FAITS TELS QU'EXPOSÉS PAR LA PRESSE

Les articles en question rapportent que la direction du SPF Finances a adressé le 22 décembre 2004 un message à l'ensemble des directions régionales des douanes. Selon le FOD Finances « *certaines sociétés belges tenteraient d'exporter des biens à double usage, sans licence communautaire d'exportation* ». Il s'agirait de presses et ou de parties de presse isostatiques destinées à l'Iran. Ce matériel pourrait être transformé en presse isostatique nucléaire ce qui pourrait justifier sa saisie, même si aucune licence d'exportation n'est requise. Les services de douane étaient donc priés de porter leur attention particulière à cette possibilité et d'exercer une surveillance renforcée sur l'exportation et le transit de marchandises similaires.

La seule firme capable de produire ce type de matériel dans notre pays serait la firme EPSI installée à Tamise, en région flamande. Sa direction aurait d'ailleurs reconnu avoir exporté par camion, et sans licence, au mois de janvier 2005, une petite presse isostatique, à Téhéran : cette presse à chaud de laboratoire, destinée à l'industrie aéronautique iranienne, devrait lui permettre d'opérer un traitement thermique, sous haute pression, d'aubes de turbines d'avion. Comme le four de la presse n'était pas supérieur à 152 mm de diamètre, le traité de non-prolifération (TNP) n'exigeait pas de licence d'exportation. Supérieur à cette norme, le four serait considéré comme un « bien à double usage » c'est-à-dire susceptible d'être utilisé à des fins nucléaires ou militaires. Le certificat d'utilisation finale produit par « *Iran Aircraft Industries* » indique d'ailleurs que ce matériel ne sera pas utilisé à des fins militaires, de défense ou nucléaire. Cette presse aurait été installée au siège de l'entreprise « *Iran Aircraft Industries* » à Téhéran.

« *Le Soir* » suggère cependant que le four isostatique fourni à cette entreprise iranienne pourrait servir à produire soit des pièces de missiles d'une portée de 2.000, voire 3.000 kilomètres, soit des drones, dont l'Iran a déjà équipé la milice du Hezbollah, soit des pièces détachées pour son aviation militaire.

¹ SCHOONE, C. 'Du "nucléaire" belge en Iran ?', *Le Soir*, 29 avril 2005 ; HUISMAN, R., 'Vlaams bedrijf leverde verdachte pers aan Iran', *Gazet van Antwerpen*, 30 avril 2005 en SCHOONE, C., 'Il fallait arrêter ce matériel ...', *Le Soir*, 11 mai 2005.

Les journaux indiquent que le service des douanes aurait rédigé un procès-verbal de six pages sur la firme EPSI, ceci après une inspection effectuée sur place en février 2005 : au total, quatre presses, non soumises à licence d'exportation, auraient été vendues par cette société à l'Iran. Au moment de la mise en garde adressée aux douanes, la firme EPSI se serait vue refuser l'octroi d'une licence pour la fourniture à l'Iran d'une presse isostatique de plus grande taille que celles qui ont été livrées.

Les journaux précisent enfin que ce seraient les services de renseignement américains (la CIA en l'occurrence) qui auraient alerté la Belgique. Le fait que de telles exportations aient pu échapper au contrôle des autorités belges, pourrait provoquer des difficultés avec le gouvernement des États-Unis.

Dans son édition du mercredi 11 mai 2005, le journal *Le Soir* relate le commentaire d'une « source américaine » selon laquelle « *il fallait arrêter ce matériel* » et pour qui « *la situation internationale devrait inciter les autorités belges à un contrôle plus sérieux* ». La direction de la firme EPSI dément être associée à tout programme atomique ou nucléaire iranien. Selon elle, l'intervention américaine relèverait d'une forme de « protectionnisme commercial ».

3. L'INTÉRÊT PARLEMENTAIRE

Le 29 avril 2005, Madame la députée fédérale GERKENS a posé une question parlementaire au vice-première ministre et ministre de la Justice ONKELINX sur « *le matériel nucléaire produit en Belgique et exporté vers l'Iran* ». Dans cette question, la députée s'est notamment demandée si une enquête se justifiait sur cette affaire.

La ministre a répondu à cette question le 3 mai 2005² sur base d'une note que la Sûreté de l'État lui a communiquée le 2 mai. Le contenu de cette note sera examiné sous le point 6.3. du présent rapport.

4. LA PROCÉDURE D'ENQUÊTE

Les informations parues dans la presse le 29 avril 2005 ont été commentées au cours de la réunion tenue le mardi 3 mai 2005 par la Commission du Sénat chargée du suivi parlementaire du Comité permanent R.

Le Comité permanent R a rappelé aux membres de la commission qu'il avait déjà ouvert une enquête de contrôle sur le rôle des services de renseignement en matière de lutte contre la prolifération d'armements non conventionnels ou très avancés.

Les membres de cette commission ont annoncé leur intention d'entendre les responsables de l'administration des douanes à propos du cas de la firme EPSI. Ils ont chargé le Comité permanent R de recueillir l'information nécessaire auprès des services de renseignement.

Le jour même, le Comité permanent R a décidé d'ouvrir une enquête spécifique sur la manière dont la firme EPSI avait éventuellement été suivie par les services de renseignement dans le cadre de la lutte contre la prolifération.

Les services et les ministres compétents en ont été avertis le 4 mai 2005.

² Questions et Réponses, Chambre n° 6763 – 3ème session CRABV 51 COM 586.

Le 12 mai 2005, la Commission sénatoriale a confirmé sa demande d'enquête au Comité permanent R.

Pour la première fois dans ses douze années d'existence, le Comité permanent a estimé nécessaire de recourir à deux moyens de contrainte que lui confère la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements :

- Il a fait procéder à la saisie de certains documents en application de l'article 51 de la loi précitée ;
- le Président du Comité permanent R a fait citer à comparaître par huissier de justice, trois membres du personnel de la Sûreté de l'État en application de l'article 48 § 2 de la même loi.

L'application de la règle du Tiers service³ a motivé deux initiatives de l'administrateur général de la Sûreté de l'État en vue de restreindre l'accès du Comité permanent R à certains documents et de lui en limiter l'utilisation.

Ainsi l'administrateur général de la Sûreté de l'État estimait que la saisie des certains documents classifiés était de nature à constituer une menace pour l'exécution des missions de la Sûreté de l'État visées aux articles 7 et 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. La sûreté de l'État a pris contact avec l'autorité d'origine des documents concernés pour avoir sa position en ce qui concerne l'application de l'opposition auprès du Président du Comité permanent R prévue à l'article 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Les documents saisis étaient classifiés « secret » au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité en raison d'informations communiquées par des services de renseignement étrangers.

L'administrateur général de la Sûreté de l'État ne s'étant toutefois pas opposé formellement à la saisie, la question ne fut pas soumise au Président du Comité permanent R comme le prévoit l'article 51, alinéa 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

Le 30 mai 2005, l'administrateur général de la Sûreté de l'État a justifié ses réticences à communiquer les documents saisis et a fait part au Comité permanent R de la position du service émetteur dans les termes suivants :

³ La '**règle du tiers service**' : il s'agit d'une règle (parfois écrite, parfois orale) appliquée dans le monde des services de renseignements. Elle implique qu'un renseignement transmis d'un service officiel d'un Etat à un autre service officiel étranger reste la « propriété » du service émetteur. Cela signifie que le renseignement :
– doit garder dans le service receveur le même degré de classification que celui que le service émetteur lui a donné ;
– ne peut être communiqué et traité que dans le respect des conditions de sécurité adéquates (protection du secret, habilitations de sécurité, etc ...) ;
– ne peut être utilisé que dans le but pour lequel le renseignement a été fourni ;
– ne peut pas être communiqué à des tiers non habilités sans l'accord du service émetteur.
Le Comité permanent R a déjà consacré une étude à cette règle (Voir *Doc. Parl.*, Chambre 1997-98, 1139/5,55).

« Les documents saisis étaient classifiés « secret » par le service émetteur afin de protéger un de ses intérêts. L'acte de saisie, même si elle est fondée sur une loi, est de nature à porter atteinte à ces intérêts. Dans ce contexte, le service émetteur attend du service receveur d'être mis au courant de tout événement qui pourrait mettre en péril un de ses intérêts. Une omission de ces obligations porterait atteinte à la confiance entre les services et dès lors au bon fonctionnement du receveur qui ne recevra plus d'information. La réponse du service émetteur du 18 mai 2005 confirme qu'une prudence de notre part était tout à fait justifiée. Par un message secret, ce service nous envoie un texte non classifié utilisable en dehors du contexte pur de renseignement. »

Ce texte non classifié provenant du service américain émetteur est mentionné plus loin dans ce rapport d'activité.

Outre l'invocation de l'article 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, l'Administrateur général de la Sûreté de l'État a également averti le Comité permanent R via le service d'enquêtes. Aux termes de cet avertissement, le Comité devrait se montrer extrêmement circonspect dans l'utilisation de certains documents et ne pas mettre la ministre en difficulté vis-à-vis du Parlement.

Cet avertissement oral a été confirmé le 2 juin 2005 par une lettre adressée au chef du Service d'enquêtes R. Le Comité permanent R estime devoir prendre la responsabilité de n'écarter aucun document de son dossier d'enquête. Le Comité permanent R a pour mission légale d'examiner l'action et l'efficacité des services de renseignement. Il ne peut être empêché d'en tirer les conclusions qui s'imposent, quelle que soit l'exploitation politique que certains seraient tentés d'en tirer.

Un rapport, classifié « SECRET » a été approuvé le 14 juin 2005. La classification de ce rapport se justifie par le fait qu'il mentionne un certain nombre d'informations classifiées « SECRET » qu'un service américain a communiquées à la Sûreté de l'État. La présente version déclassifiée de ce rapport a été approuvée le 14 juin 2005.

Le 29 septembre 2005, le Ministre de la Justice transmettait au Comité permanent R, la réponse faite par la Sûreté de l'État suite au rapport d'enquête du 15 juin 2005. Cette réponse porte la classification « SECRET – LOI DU 11.12.1998 ». Le Comité permanent R a adressé sa réponse à la Ministre de la Justice par courrier du 6 octobre 2005.

5. LE CADRE LÉGISLATIF ET RÉGLEMENTAIRE

La presse a indiqué que le matériel exporté par EPSI pourrait être transformé en presse isostatique nucléaire ce qui pourrait justifier sa saisie même si aucune licence d'exportation n'était requise. Il a également été suggéré que la presse isostatique pourrait servir à produire soit des pièces de missiles, soit des drones, soit des pièces détachées pour son aviation militaire. Plusieurs législations sont susceptibles d'être appliquées à l'exportation de ces deux types de matériel.

5.1. La loi du 9 février 1981 et ses arrêtés royaux

Cette loi du 9 février 1981 relative aux conditions d'exportation des matières et équipements nucléaires, ainsi que des données technologiques nucléaires, prise en application du Traité de non-prolifération (TNP), interdit de transférer, à destination de pays non dotés d'armes nucléaires, des matières et équipements nucléaires, ainsi que des données technologiques nucléaires et leurs dérivés, pour des fins d'utilisation autres que pacifiques et moyennant les contrôles requis. Pour garantir le respect de ces conditions, chaque transfert est soumis à une autorisation préalable, délivrée par le Ministre ou le Secrétaire d'État qui a l'énergie dans ses attributions. Depuis l'année 2004, l'autorisation est accordée par le ministre régional en charge de l'économie de la Région où est située l'entreprise concernée.

Cette autorisation est donnée après avis de la "*Commission d'avis pour la non-prolifération des armes nucléaires*" (CANPAN).

Les matières, équipements et données technologiques dont l'exportation est soumise à autorisation ministérielle sont aussi précisés par le Roi, compte tenu des accords internationaux régissant le domaine nucléaire et auxquels la Belgique est partie contractante. A la demande du Ministre, la CANPAN lui donne également son avis sur tout projet de modification de la liste de matériels et technologies jointe à l'arrêté royal.

Cette loi du 9 février 1981 est mise en œuvre par l'arrêté royal du 12 mai 1989 « *relatif au transfert à destination de pays non dotés d'armes nucléaires, des matières nucléaires, des équipements nucléaires, des données technologiques nucléaires et leurs dérivés* »⁴.

Selon les annexes de cet arrêté royal, doivent être soumises à l'avis de la CANPAN les « *Presses isostatiques capables d'atteindre une pression de régime maximale égale ou supérieure à 69 MPa et possédant une chambre dont le diamètre intérieur de la cavité est supérieur à 152 mm ainsi que des matrices et des moules spécialement conçus et des dispositifs de contrôle et un " logiciel spécialement conçu à cet effet. »*

5.2. Les règles de l'Union européenne en vue du contrôle des exportations de biens et technologies à double usage et des équipements militaires

Le règlement (CE) n° 1334/2000 du Conseil européen du 22 juin 2000⁵ institue un régime communautaire de contrôle des exportations de biens et technologies à double usage. Il s'agit de tous les biens qui sont ou qui peuvent être destinés à un usage lié aux armes de destruction massive, ainsi qu'aux armes conventionnelles si celles-ci sont destinées à l'exportation vers des destinations soumises à un embargo sur les armes.

L'Iran n'est soumis à aucun embargo multilatéral sur les armes conventionnelles. Seuls les États-Unis et l'Angleterre ont imposé un embargo de manière unilatérale.

L'exportation des biens énumérés à l'annexe I du dit règlement est soumise à autorisation. Il s'agit d'équipements visés par le Groupe des fournisseurs nucléaires (Nuclear Suppliers Group (GFN/NSG))⁶, l'Arrangement de Wassenaar sur les biens à double usage⁷ et par le Régime de Contrôle de la Technologie des Missiles (*Missile Technology Control Regime* ou MTCR)⁸.

⁴ M.B., 15 juin 1989.

⁵ Modifié par le règlement (CE) n° 149/2003 du Conseil le 27 janvier 2003.

⁶ Nommé 'Club de Londres' à son commencement.

⁷ <http://www.wassenaar.org>

⁸ www.mtcr.info

Dans cette annexe figurent plusieurs modèles de presses isostatiques.

L'exportation de biens non énumérés dans cette annexe du règlement peut aussi être soumise à autorisation « *si les autorités compétentes de l'État membre où l'exportateur est établi ont informé celui-ci que les produits en question sont ou peuvent être destinés, entièrement ou en partie, à contribuer au développement, à la production, au maniement, au fonctionnement, à l'entretien, au stockage, à la détection, à l'identification ou à la dissémination d'armes chimiques, biologiques ou nucléaires ou d'autres dispositifs nucléaires explosifs, ou au développement, à la production, à l'entretien ou au stockage de missiles pouvant servir de vecteur à de telles armes.* »

Deux arrêtés ministériels du 28 septembre 2000 réglementant l'exportation et le transit des biens à double usage consacrent l'application de ce règlement européen n° 1334/2000 pour la Belgique.

6. CONSTATATIONS

6.1. Le rôle de La Sûreté de l'État

L'article 8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité charge de manière explicite la Sûreté de l'État de s'occuper des menaces liées à la prolifération, à savoir « *le trafic ou les transactions relatifs aux matériaux, produits, bien ou know-how pouvant contribuer à la production ou au développement de systèmes d'armements non conventionnels ou très avancés.* » Et l'article 8 d'ajouter : « *Sont notamment visés dans ce cadre le développement de programmes d'armement nucléaire, chimique et biologique, les systèmes de transmission qui s'y rapportent, ainsi que les personnes, structures ou pays qui y sont impliqués* ».

La manière dont la Sûreté de l'État traite cette matière est décrite dans un manuel de formation des agents des services extérieurs : « *Les activités de la Sûreté de l'État visent surtout à prévenir l'exportation de connaissances et de produits qui peuvent être utilisés afin de constituer des arsenaux et des systèmes d'armes nucléaires, biologiques et/ou chimiques. Son apport en la matière se situe sur le plan purement informatif. Le service ne dispose en effet d'aucune compétence décisionnelle en matière de non-prolifération* ». Et la Sûreté de l'État de décrire ainsi ses tâches en la matière :

- fournir de l'information aux autorités compétentes : « Il s'agit aussi bien d'informations à caractère général concernant l'évolution du domaine de la prolifération que d'informations spécifiques destinées à empêcher des transactions non souhaitées », par exemple, des informations relatives à des pays « proliférant », à des acheteurs ou à des fournisseurs suspects ;
- informer ces autorités « de manière à empêcher des participations indésirables à la réalisation de programmes d'armements non conventionnels » ;
- informer les milieux du commerce, de l'industrie et les laboratoires spécialisés ;
- effectuer sur le territoire national le suivi opérationnel (c'est-à-dire recueillir des renseignements) des situations où l'on suspecte une violation des dispositions contre la prolifération, ceci en collaboration éventuelle avec d'autres services compétents ;

- contribuer à mettre en œuvre concrètement et à adapter la politique belge de non-prolifération ;
- participer à des réunions nationales et internationales de coordination ou à toute autre initiative en matière de non-prolifération.

Parmi les membres de la "*Commission d'avis pour la non-prolifération des armes nucléaires*".

6.2. La façon dont l'Administration des douanes et accises a pris connaissance des faits

Au cours de leur audition par la Commission du Sénat chargée du suivi parlementaire du Comité permanent R, trois représentants de l'Administration des douanes et accises du SPF Finances ont relaté la manière dont leur service a été mis au courant des faits qui nous intéressent, à savoir l'exportation d'une presse isostatique de la firme EPSI vers l'Iran et comment ils ont traité cette affaire.

Cette relation fait l'objet d'une note écrite rédigée par le directeur général des douanes et accises. Ce document a été remis aux membres de la Commission et aux membres du Comité permanent R. La manière dont l'Administration des douanes et accises a été informée de cette affaire peut être résumée comme suit.

- Le 28 septembre 2004, les douanes ont reçu un message électronique de la CANPAN en vue d'appliquer la procédure d'alarme. L'information secrète était ainsi rédigée : « *Op de vergadering van de CANVEK heeft een lid informatie verspreid – met classificatie « geheim » - over de mogelijkheid tot omzeilen van het Belgisch nucleaire exportregime, waarbij een Belgisch bedrijf is genoemd. De bron van deze informatie is een buitenlandse inlichtingendienst.* » Le message se termine en annonçant une réunion de la CANPAN qui doit se tenir le jour même.
- Le 1^{er} octobre 2004, la CANPAN établit un projet de circulaire concernant l'exportation possible d'une presse isostatique vers l'Iran.
- Le 5 octobre 2004, ce projet de circulaire est adressé pour avis aux autorités régionales compétentes pour l'octroi des licences d'exportation. Les douanes obtiennent l'accord de la Région flamande mais aucune réponse de la part de la Région wallonne.
- Le 28 octobre 2004, l'administration des douanes et accises belges reçoit la visite de l'attaché des douanes américaines auprès de l'ambassade U.S. à Bruxelles. L'attaché américain remet à son homologue belge une brève note secrète. Selon ce document, la firme EPSI était sur le point d'expédier ce jour même une presse isostatique à froid à la firme vers l'Iran. Le transport devrait se faire par camion.
- Suite à cette information, les cinq bureaux des douanes et accises auxquels la firme EPSI avait l'habitude de s'adresser pour déclarer ses exportations (Sint Niklaas, Anvers, Zaventem, Meer et Malines) furent alertés avec demande de stopper le convoi.
- Le 3 novembre 2004, la firme EPSI procède à l'exportation par camion d'une presse isostatique en passant par le bureau de douane d'Eynatten. Le destinataire déclaré de l'expédition est la firme iranienne *Iran Aircraft Industry*. L'expédition était accompagnée d'une lettre de la Région flamande indiquant que le matériel exporté n'était pas à double usage et qu'il n'était dès lors pas soumis à licence d'exportation.

- Le 19 novembre 2004, l'administration des douanes adresse un message électronique à la CANPAN. Se référant au message du 28 septembre 2004, les douanes demandent à la CANPAN si la firme concernée est bien du Waasland. Le 22 novembre 2004, la CANPAN répond de manière affirmative.

Au terme de l'enquête qu'elle a menée auprès de la firme EPSI, l'Administration des douanes et accises conclut qu'il n'y a aucune trace de fraude. La procédure du catch all ne devait pas s'appliquer. Le matériel a été commandé, transporté et exporté de manière tout à fait régulière. Aucune licence d'exportation n'était nécessaire puisqu'il ne s'agissait pas d'un bien à double usage.

6.3. Le traitement de l'information sur la firme EPSI par la Sûreté de l'État

Les documents que la Sûreté de l'État a fourni au Comité permanent R ainsi que les déclarations sous serment des membres de son personnel permettent de retracer le traitement du cas EPSI par ce service comme suit :

La firme EPSI est connue du service depuis 1994

EPSI a son siège social situé à Tamise. L'entreprise est spécialisée dans la recherche, la mise au point et la production d'applications à haute pression : presses isostatiques à chaud, à froid, pompes à haute pression, outillage pour réacteurs, etc. Ses produits sont notamment utilisés dans l'industrie aérospatiale.

EPSI était autrefois une filiale de *NATIONAL FORGE USA* faisant partie du groupe américain *RCR Group Incorporated*, une entreprise américaine ayant son siège en Pennsylvanie. Elle s'appelait alors *NATIONAL FORGE EUROPE NV*, et avait son siège à Sint-Niklaas. En 1996, la firme prit son indépendance par rapport au groupe américain et devint EPSI (*Engineered Pressures Systems International NV*). Son siège social fut transféré à Temse tandis qu'elle conserve une filiale dans l'État du Massachusetts aux États-Unis.

Le premier avertissement du service américain (15 juillet 2004)

Le 15 juillet 2004, la Sûreté de l'État reçoit une note de l'ambassade américaine à Bruxelles. Il s'agit d'un document classifié « SECRET » saisi par le Service d'enquêtes R le 12 mai 2005. Faisant suite à l'invocation de la règle du tiers lors de la saisie du document précité le 12 mai 2005, le service émetteur a permis la déclassification du contenu suivant :

- *« In the spirit of our close missile nonproliferation partnership, we would like to alert you to a matter of potential proliferation concern and request your government's assistance in investigating this activity.*
- *The U.S. has information that an Iranian company is attempting to purchase a hot isostatic press from the Belgium firm Engineered Pressure Systems International N.V. (EPSI).*
- *Hot isostatic presses can be used in making nose tips for reentry vehicles and nozzle inserts for rocket motors. They also can be used to form metal laminates and improving the quality of metal castings and forgings.*

- *Some isostatic presses are controlled under category II items 6 of the MTCR annex.*
- *We hope you will be able to use this information to investigate this activity and disrupt Iran's ability to procure sensitive equipment for its missile programs from Belgium.*
- *In particular, we urge your government to employ all appropriate measures, including catch-all controls, to ensure that Belgian entities do not contribute, even inadvertently, to missile programs in Iran".*

L'administrateur général de la Sûreté de l'État commente le contenu de cette note de la manière suivante :

« La première chose à faire était d'évaluer la valeur de l'information. Cela pouvait être une simple alerte dans le cadre de la non-prolifération mais d'autre part, cela pouvait être une tentative de nuisance économique. Nonobstant cela, le service a favorisé la thèse non prolifération étant donné que l'Iran est vu par les Américains comme un pays faisant partie de l'axe du Mal ».

La section « prolifération » ainsi que la section locale de Gand ont donc été chargés le 16 juillet 2005 d'effectuer une enquête à propos de la firme belge *EPSI* et sur ses activités d'exportation vers l'Iran.

Participation à la réunion de la CANPAN (le 6 septembre 2004)

Un commissaire divisionnaire représentait la Sûreté de l'Etat à cette réunion-CANPAN. Il n'y avait pas de représentant de l'Administration des douanes et accises présent.

Le représentant de la Sûreté de l'État fit savoir qu'il disposait d'informations, couvertes par le secret professionnel, selon lesquelles un exportateur chercherait à esquiver le régime du contrôle sur l'exportation de matériel nucléaire. Le procès-verbal de cette réunion ne mentionne ni le nom de l'exportateur concerné, ni le pays destinataire.

L'enquête du Comité permanent R a pourtant fait apparaître que la firme *EPSI* et l'Iran ont bien été cités oralement comme étant les protagonistes de cette transaction douteuse.

La hiérarchie de la Sûreté de l'État a marqué son accord sur cette communication. Bien que les membres de la CANPAN ne soient pas tous titulaires d'une habilitation de sécurité, il paraissait nécessaire de leur communiquer cette information classifiée sans laquelle il leur était impossible de prendre les mesures adéquates. L'intention du service américain n'était certainement pas d'en empêcher la communication puisqu'il demandait aux autorités belges d'empêcher l'exportation.

Le procès-verbal de la réunion mentionne que le secrétariat de la CANPAN chargerait le service des douanes de renforcer le contrôle des biens nucléaires à double usage, « *dès que le secret de l'information sera supprimé et à condition de la coopération des Régions.* »

Participation à la réunion de la CANPAN (le 28 septembre 2004)

Un analyste du service d'études « prolifération » représentait la Sûreté de l'État à cette réunion. Pas plus que le 6 septembre précédant, aucun représentant de l'administration des douanes et accises ne participait à cette réunion.

Deux dossiers furent discutés au cours de cette réunion :

- Un premier dossier d'exportation d'une presse isostatique de la firme EPSI vers l'Iran : Les membres présents de la CANPAN émirent un avis négatif estimant qu'il existait « *un risque inacceptable que l'équipement soit impliqué dans des activités liées aux armes nucléaires ou une activité d'explosion nucléaire* ».
- Le cas évoqué le 6 septembre 2004 de la société belge suspectée de vouloir contourner le régime d'exportation nucléaire : Ni le nom de l'intervenant, ni le nom de la firme en question ne sont indiqués dans le procès-verbal.

Le PV de la réunion mentionne seulement que le secrétariat de la CANPAN a eu un contact avec les services des douanes. Ceux-ci élaborent une circulaire en vue de renforcer le contrôle de l'équipement visé lors de la dernière réunion.

Le 5 octobre 2004, le ministre de l'Économie a confirmé le refus d'accorder la licence d'exportation d'une presse isostatique vers l'Iran demandée par la firme EPSI.

Le premier rapport interne de la Sûreté de l'État suite aux informations américaines (le 5 octobre 2004)

L'enquête a été menée durant la seconde moitié du mois de septembre et le début du mois d'octobre 2004.

L'hypothèse selon laquelle la firme EPSI tenterait de contourner les contrôles douaniers en diminuant temporairement le diamètre de la presse est peu vraisemblable. Une telle adaptation serait un travail lourd et difficile à réaliser. Une telle adaptation ferait échapper l'équipement aux normes qui figurent en annexe de l'arrêté royal du 12 mai 1989 relatif aux transferts nucléaires, mais pas aux normes de l'Arrangement de Wassenaar.

Le rapport remarque que l'Iran est parfaitement au courant des règles applicables en Europe aux exportations sensibles destinées aux pays à risques. Les firmes iraniennes exploitent les différences de réglementation entre pays européens pour contourner les contrôles douaniers et les refus de licences d'exportations.

Le deuxième avertissement américain (28 et 29 octobre 2004)

Le 29 octobre 2004, la Sûreté de l'État reçoit un nouvel avertissement américain daté du 28 octobre 2004. Ce document informe le service que la firme EPSI est sur le point de fournir une presse isostatique à froid à une firme iranienne.

Le transport devrait se faire par camion. L'apparence du matériel exporté pourrait être modifiée afin de contourner la réglementation belge en matière de douanes. Il est aussi signalé que les douanes belges ont reçu le même avertissement.

La Sûreté de l'État n'a jamais communiqué la moindre réponse au service américain concernant ses avertissements des 15 juillet et 28 octobre 2004.

Le 3 novembre 2004, la firme EPSI procède à l'exportation par camion d'une presse isostatique en passant par le bureau de douane d'Eynatten.

Le deuxième rapport interne de la Sûreté de l'État (25 novembre 2004)

Ce rapport classifié « SECRET » daté du 25 novembre 2004 indique que la société EPSI a effectivement livré une « petite » presse isostatique à l'Iran à la fin du mois d'octobre. Selon les documents officiels, l'utilisateur final de la presse serait « *Iran Aircraft Industries* » qui l'utiliserait pour traiter des ailettes de turbines. Selon le rapporteur, cette explication est plausible.

L'hypothèse selon laquelle l'Iran pourrait modifier augmenter le diamètre intérieur de la presse après sa livraison n'est pas sérieuse. Une telle adaptation technique n'est pas exclue en théorie, elle est cependant très difficile à réaliser et peu sûre quant à ses effets.

Il est donc très peu probable qu'un pays comme l'Iran qui ne dispose pas des capacités techniques pour produire une presse isostatique puisse en modifier les caractères.

Le rapport signale en outre que la société EPSI se plaint d'une lacune dans la réglementation des exportations. Lorsqu'elles sont accordées, les licences sont valables pour un an alors que le délai qui s'écoule entre l'octroi de la licence et la livraison effective du matériel est souvent supérieur à une année.

Cela signifie qu'au moment où la commande est prête à être livrée, il faut recommencer la procédure. Cette situation cause un handicap commercial à nos sociétés exportatrices. Le rapporteur suggère de procéder comme dans certains pays avoisinants : délivrer un avis préalable au moment de la commande.

Participation à la réunion de la CANPAN (le 1^{er} mars 2005)

Un analyste du service d'études « prolifération » représentait la Sûreté de l'État à cette réunion. Un représentant de l'Administration des douanes et accises y participait aussi.

La firme EPSI fut évoquée à propos de plusieurs dossiers d'exportation de presses isostatiques vers l'étranger.

La commission se pencha ensuite sur « *l'information concernant l'esquive potentielle du régime d'exportation nucléaire, affaire dans laquelle une société belge serait impliquée* ».

Le représentant de l'Administration des douanes et accises fut invité à donner « *des explications quant aux actions entreprises et à entreprendre qui pourront servir d'éléments de réponse* ».

Selon ces explications, la société EPSI (ici désignée par son nom) a été placée sous surveillance permanente par les services des douanes. Les douanes devaient encore examiner si oui ou non la presse exportée relevait du contrôle de l'exportation.

La réponse à une question parlementaire du 29 avril 2005

Le 2 mai 2005, la Sûreté de l'État fut priée de fournir à la vice-première ministre et ministre de la Justice ONKELINX des éléments de réponse à la question parlementaire posée par Madame la députée fédérale GERKENS sur « *le matériel nucléaire produit en Belgique et exporté vers l'Iran* »⁹.

⁹ Question n° 6763, Chambre – 3ème session CRABV 51 COM 586.

Se basant sur les informations parues dans le journal « Le Soir » du 29 janvier 2005, la députée demandait notamment si les services de renseignement belges étaient au courant de l'exportation de matériel nucléaire vers l'Iran à partir d'entreprises belges.

Le même jour, la Sûreté de l'État a répondu à Madame la ministre de la Justice en ces termes :

« La Sûreté de l'État est consciente que du matériel pouvant être utilisé dans le cadre d'un programme nucléaire est susceptible d'un export depuis la Belgique vers des pays tels que l'Iran. C'est la raison pour laquelle dans le cadre de notre mission de lutte contre la prolifération d'armes chimiques, biologiques et nucléaires nous essayons autant que possible et en collaboration avec les autres autorités belges compétentes de suivre ce type de transactions et de les empêcher le cas échéant.

Cependant en tant que service de renseignement nous ne sommes pas en mesure de suivre la totalité des exportations belges. En juillet 2004, des informations venant d'un service étranger nous indiquaient la possibilité d'une exportation d'une HIP vers l'Iran. Cet élément a été évoqué lors d'une réunion de la Commission d'avis pour la non-prolifération des armes nucléaires (CANPAN). Ces réunions confidentielles visent à examiner les dossiers soumis à licence.

Toutefois, dans le cas présent des informations parues dans « Le Soir », l'exportation de cette presse isostatique à chaud n'était pas connue de la Sûreté de l'État même si elle était au courant des activités générales de la firme EPSI notamment via les nombreux dossiers qu'elle soumet régulièrement auprès de la CANPAN.

Selon les informations du journal « Le Soir », il semble que cette HIP tombait en dessous des critères nécessitant la soumission du dossier auprès de la CANPAN.

Il reste toujours la possibilité que les autorités américaines, via leurs agents de liaisons près les douanes, transmettent directement des informations dont la Sûreté n'est pas destinataires.

Concernant les informations parues dans la presse, notre service n'en avait pas été informé préalablement par le Ministère des Finances.

De façon générale, le dispositif classique d'échange d'informations en matière de lutte contre la prolifération nucléaire est la CANPAN dont la Sûreté est membre.

A côté de cela, les mécanismes habituels d'échange et de contact avec les autres entités belges s'appliquent bien évidemment aussi en matière nucléaire.

Il est évident que les mécanismes actuels de lutte contre la prolifération en Belgique pourrait être améliorés bien que ceux-ci fournissent déjà des résultats non négligeables. Il faut garder à l'esprit que les moyens humains et logistiques alloués dans le cadre de la lutte contre la prolifération en Belgique ne permettent pas d'assurer un suivi total et systématique des exportations sensibles et ne le permettront sans doute jamais à 100%.

Quant à se prononcer sur la nécessité d'une enquête, il conviendrait à tout le moins d'identifier ce qui n'a pas fonctionné pour permettre l'application de la clause catch-all. »

Faisant suite à ce courrier, Madame la ministre de la Justice a répondu que les informations parues dans Le Soir n'étaient pas connues de la Sûreté de l'État, « même si elle était au courant des activités générales de la firme EPSI, notamment via les nombreux dossiers qu'elle soumet régulièrement auprès la commission d'avis ».

Dans sa lettre adressée au Comité permanent R le 18 mai 2005, l'administrateur général de la Sûreté de l'État affirme également que la Sûreté de l'État n'a pas reçu d'information concernant la presse isostatique HIP mentionnée dans le journal « Le Soir » le 29 avril 2005.

Commentaire du Comité permanent R

L'article du Soir en question mentionne une presse isostatique qui aurait été exportée à Téhéran par camion, et sans licence, au mois de janvier 2005.

Effectivement, la présente enquête n'a relevé aucune trace d'une telle exportation qui aurait été effectuée en janvier 2005. Le contexte et les circonstances exposées par l'article semblent pourtant se référer à l'exportation effectuée par EPSI le 3 novembre 2004.

Le Comité permanent R estime dès lors abusif d'affirmer ne rien connaître de l'opération vu les avertissements précis reçus du service de renseignement américaine (CIA) et le rapport rédigé le 25 novembre 2004.

6.4. Les commentaires de la Sûreté de l'État

Dans sa lettre du 18 mai 2005, l'administrateur général commente la manière dont son service a traité la problématique de la façon suivante :

- *“Contrairement à l’abus de langage qui a parfois était fait, une presse isostatique à chaud est un bien à double usage pouvant éventuellement trouver une application dans le cadre d’un programme nucléaire, mais n’est en rien comme certains le disent un matériel nucléaire.*
- *D’autre part, concernant la possibilité de modifier les spécificités techniques de ce type de presse en vue d’éviter certains contrôles à l’exportation, de l’avis de spécialistes en la matière, cette démarche semble peu probable, très difficile à réaliser et risquerait d’altérer les performances de ce matériel voire même provoquer la perte totale de celui-ci.*
- *Par rapport aux dispositifs belges pour lutter contre la prolifération de matériel nucléaire, il faut savoir que les moyens humains et logistiques alloués à la lutte contre la Prolifération aux différentes entités compétentes sont largement insuffisants pour assurer un contrôle optimal et systématique des entreprises belges et des exportations depuis et via notre pays.*
- *Si nous prenons l’exemple des Douanes, même avec la meilleure volonté du monde, leurs agents ne seraient, paraît-il, en mesure de contrôler que 4 à 5 % maximum des exportations. Du côté de la Sûreté de l’État, les ressources humaines et logistiques ne permettent également qu’un suivi très partiel et bien souvent ponctuel.*
- *Il est certain que des moyens ont été dégagés depuis septembre 2001 pour renforcer la lutte contre le terrorisme, mais il est regrettable que dans le même temps la lutte contre la Prolifération soit restée dans l’ombre alors que cette problématique est plus que jamais présente sur l’échiquier mondial depuis 2001.*
- *En résumé, tous les acteurs de terrain concernés sont d’accord pour affirmer que la Belgique n’a actuellement pas les moyens d’une Politique de non-prolifération forte car même si des initiatives se sont mises en place depuis 2001, les moyens de les concrétiser ne suivent malheureusement pas.*

- *Quels que soient les moyens consacrés à la lutte contre la Prolifération, un contrôle à 100% restera cependant toujours illusoire.*
- *Concernant le rôle de la Sûreté, même si on a un rôle indéniable, nous tenons à rappeler que nous ne sommes en aucun cas compétents en la matière de contrôle « matériel » des exportations, ni en matière d'interception.*
- *Dans le cas évoqué par le journal « Le Soir » et sans plus de précisions, il semble que seules les autorités régionales compétentes pour délivrer une autorisation d'exportation et/ou l'administration des Douanes auraient pu agir pour empêcher l'exportation de cette HIP vers l'Iran.*
- *Lorsque l'on parle d'exportation d'une HIP par la firme EPSI sans en mentionner toutes les spécifications techniques de ce matériel ni les modalités précises de l'exportation, il est toujours difficile de déterminer si l'on parle tous de la même HIP, étant donné que nous disposons pour l'instant de peu d'éléments de comparaison."*

7. LE PROBLÈME DE LA COMMUNICATION D'INFORMATIONS CLASSIFIÉES AUX FONCTIONNAIRES ET AUX MEMBRES DE LA CANPAN

Tous les membres de la CANPAN ne disposent pas encore d'une habilitation de sécurité leur permettant de pouvoir prendre connaissance d'informations classifiées.

Aucune directive n'a été donnée aux représentants de la Sûreté de l'État auprès de cette commission quant à la manière d'y communiquer certaines informations.

Ce problème a été posé à l'administrateur général par un commissaire divisionnaire dans les termes suivants :

« Deuxièmement, un problème important se pose à propos de la législation sur la classification et les habilitations de sécurité. A savoir, sous quelle forme (orale ou écrite ?) la Sûreté de l'État peut-elle communiquer de « l'Intelligence » (NDR : du Renseignement) aux autres fonctionnaires compétents. Le degré de véracité joue ici aussi un rôle puisque les autorités compétentes doivent s'appuyer sur les avis obtenus, notamment ceux auxquels la Sûreté de l'État contribue, pour prendre leurs décisions ».

Le commissaire propose à l'administrateur général d'examiner ce problème par rapport à une série de dossiers concrets qui ont été discutés à la CANPAN. A ce jour, aucune réponse ne semble avoir été apportée à ce problème.

8. CONCLUSIONS

L'objectif de la présente enquête n'était pas de déterminer si la firme EPSI a exporté un équipement vers l'Iran en violation d'un régime international de contrôle des exportations auquel la Belgique a adhéré. Le Comité permanent R n'a pas cette compétence légale. L'enquête du Comité permanent R s'est limitée à vérifier :

- la compétence des services de renseignement belges par rapport à cette problématique ;
- la manière dont ceux-ci ont traité l'information qu'ils ont reçue d'un service étranger sur cette exportation douteuse.

Il est apparu d'emblée que le SGRS n'a pas été avisé ni concerné par cette affaire.

L'information que la Sûreté de l'État a reçue du service américain le 14 juillet 2004 était de nature à alerter les autorités compétentes sur le caractère douteux de l'exportation. L'éventualité qu'une telle exportation ait lieu vers l'Iran en violation d'un régime de contrôle international des exportations devait être examinée.

S'il n'appartenait pas à la Sûreté de l'État d'en juger par elle-même, il lui appartenait du moins d'enquêter en temps voulu, d'analyser la situation et de transmettre l'information par écrit aux autorités compétentes, à savoir l'Administration des douanes et accises, le SFP Économie, la CANPAN et le service étranger dont émanait l'information initiale.

- L'enquête fut rapidement demandée au service extérieur chargé de la prolifération (le 16 juillet 2004); il a fallu cependant attendre le 5 octobre 2004 pour qu'un rapport soit rédigé. Ce rapport ne contient pas de conclusions définitives mais relève un certain nombre d'éléments et de questions sur lesquels il conviendrait d'investiguer davantage.
- L'analyse : ce même rapport contient une analyse sommaire quant à la possibilité de transformer ou non la presse isostatique en vue de contourner les contrôles douaniers. Aucun rapport d'analyse ne semble avoir été effectué par le service d'étude sur cette affaire. L'hypothèse d'une tentative de nuisance économique à l'égard de l'entreprise EPSI a été évoquée oralement mais aucune analyse écrite ne la conforte.
- L'information aux autorités : la seule information transmise par la Sûreté de l'État fut une communication orale de son délégué lors de la réunion de la CANPAN tenue le 6 septembre 2004. L'information transcrite sur le PV de cette réunion est vague et ne permet pas à l'administration des douanes de prendre les mesures nécessaires à l'égard de la firme EPSI. Il y eut aussi des contacts informels entre le service A 7 et des membres de l'administration de l'énergie du SPF Économie pendant l'enquête.

Il a donc fallu attendre le 28 octobre 2004 pour que l'information complète parvienne à la connaissance des douanes belges via les douanes américaines. A partir de ce moment seulement les douanes belges étaient en mesure d'entamer une action ciblée à l'égard d'EPSI. A ce moment aussi, la firme était sur le point de procéder à l'expédition suspecte.

Il est interpellant de constater que la firme EPSI a procédé à cette expédition via un bureau de douane par lequel elle ne passait habituellement pas. Cette circonstance particulière aurait mérité d'être examinée.

La Sûreté de l'État n'a pas informé le service étranger des suites données à son message du 14 juillet 2004.

Les présentes constatations illustrent une nouvelle fois de manière exemplaire le problème de l'application sans discernement de la règle du tiers service.

Cette problématique a déjà été exposée à plusieurs reprises par le Comité permanent R, notamment dans ses rapports d'activités des années 2003 et 2004.¹⁰

*« En ce qui concerne la collaboration internationale, le Comité permanent R a dressé durant la période d'activités 2003 « un rapport intermédiaire relatif à l'enquête sur la manière dont la Sûreté de l'État répond aux demandes des services de renseignement étrangers ayant un représentant dans le royaume » Ce rapport souligne des difficultés certaines dont la moindre n'est sans doute pas celle qui résulte en la matière d'une culture extrême et sans nuance du secret. Le Comité permanent R estime que la Règle du Tiers appliquée sans aucun contrôle ne peut constituer un automatisme qui aurait comme implication de déplacer de manière quasi exclusive et peut-être même parfois dangereuse, le pouvoir politique d'un État vers un service de cet État. Le Comité permanent R a déjà signalé que l'interprétation stricte de cette règle coutumière à son égard notamment, dresse un obstacle à un contrôle efficace ».*¹¹

Dans le cas d'espèce, l'application de la règle du tiers a eu pour effet :

- que le nom de la firme EPSI n'a pas été mentionné dans le PV de la réunion CANPAN au cours de laquelle le délégué de la Sûreté de l'État a attiré l'attention de cette autorité sur la problématique d'une livraison douteuse à l'Iran ;
- que la CANPAN n'a alerté l'Administration des douanes de cette problématique que dans des termes généraux ne lui permettant pas de cibler la firme concernée ;
- que ce sont les autorités américaines qui ont finalement pris l'initiative de prévenir directement les douanes belges ;
- que le nom de la firme EPSI n'a dès lors pas été communiqué à l'Administration des douanes dans un délai suffisant pour lui permettre d'organiser un contrôle préventif ;
- qu'une presse isostatique de la firme EPSI a pu être exportée vers l'Iran sans licence d'exportation et sans contrôle approfondi de la conformité de cette opération envers les règles internationales d'exportation d'équipements à double usage.

Le Comité permanent R estime en outre que les explications données début mai 2005 au ministre par la Sûreté de l'État sont incomplètes et donc peu conformes à la vérité. Ainsi, il n'était pas exact de lui dire que :

- *« dans le cas présent des informations parues dans « Le Soir », l'exportation de cette presse isostatique à chaud n'était pas connue de la Sûreté de l'État » ;*

¹⁰ Comité permanent R, *Rapport d'activités 2003 et 2004*, Bruxelles (www.comiteri.be).

¹¹ Comité permanent R, *Rapport d'activités 2003*, la collaboration internationale avec les services étrangers, pages 17 et 18.

- *« Il reste toujours la possibilité que les autorités américaines, via leurs agents de liaisons près les douanes, transmettent directement des informations dont la Sûreté n'est pas destinataire ».*

Bien que « Le Soir » se réfère à une exportation qui se serait passée en janvier 2005, la présente enquête a fait apparaître que :

- le 15 juillet 2004, la Sûreté de l'État avait reçu une note de la CIA lui indiquant qu'une firme iranienne tentait d'acquérir une presse isostatique à chaud auprès de la firme belge EPSI ;
- cette même information fut communiquée aux douanes le 28 octobre 2004 et rappelée à la Sûreté de l'État par le même service américain ;
- un rapport interne du 25 novembre 2004 constate que la société EPSI a effectivement livré, sans licence d'exportation, une « petite » presse isostatique à une firme iranienne à la fin du mois d'octobre 2004. L'utilisateur final de la presse l'utiliserait pour traiter des ailettes de turbines.

Le Comité permanent R estime dès lors qu'il est abusif d'affirmer ne rien connaître des faits révélés par le journal « Le Soir » le 29 avril 2005.

L'application de la règle du Tiers a également motivé les tentatives de l'Administrateur général de la Sûreté de l'État de restreindre l'accès du Comité permanent R à certains documents. Outre l'invocation de l'article 51 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, l'Administrateur général de la Sûreté de l'État a également adressé une mise en garde orale au service d'enquêtes du Comité permanent R.

Aux termes de cet avertissement, le Comité permanent R devrait se montrer extrêmement circonspect dans l'utilisation de certains documents et ne pas mettre la ministre en difficulté vis-à-vis du Parlement.

Cette mise en garde a été confirmée dans un courrier adressé le 2 juin 2005 au chef du Service d'enquêtes :

« Suite à votre appel téléphonique, je vous ai transmis mardi le 31/05 les documents demandés.

Pour le bon ordre, je vous réaffirme mon point de vue formulé lors de notre entretien, à savoir que seul le Ministre de la Justice peut décider si les informations que nous lui avons transmises afin de préparer une réponse à une question parlementaire peuvent être rendues publiques par le Comité. Le Ministre est seul maître des informations qu'il veut transmettre au parlement dans le cadre des questions parlementaires, ce qui entraîne dès lors sa responsabilité politique.

Aucune administration n'a le droit d'apporter des informations qui contribuent à une évaluation politique externe.

Étant donné que jusqu'à présent, le service a toujours refusé – à juste titre – de communiquer des informations données au Ministre, j'ai souhaité attirer à nouveau votre attention sur ce principe. Dans le cas où vous trouveriez absolument nécessaire de dévoiler le contenu de nos informations délivrées au Ministre, il me semble absolument nécessaire que vous obteniez son accord explicite.

Dans ce but, je transmets copie de la présente à la Cellule stratégique de Madame la Ministre Onkelinx.”

Le Comité permanent R estime devoir prendre la responsabilité de n'écarter aucun document de son dossier d'enquête et d'en tirer la conclusion qui en ressort, quelle que soit l'exploitation politique que certains seraient tentés d'en tirer. à savoir que la Sûreté de l'État n'a pas dit toute la vérité à son ministre sur cette affaire.

Ce faisant, c'est à ce service qu'il incombera d'assumer sa responsabilité si la ministre est mise en difficulté devant le Parlement, non au Comité permanent R dont la mission légale est en l'occurrence de veiller à l'efficacité des services de renseignement.

N'ayant pas correctement informé les autorités compétentes ni son ministre de tutelle, la Sûreté de l'État a assurément manqué à sa mission d'information des autorités et s'est dès lors montrée inefficace dans cette affaire.

9. RECOMMANDATIONS

La commission du Sénat chargé du suivi du Comité permanent R a examiné le présent rapport le lundi 30 janvier 2006. Elle a adopté les recommandations suivantes qui lui ont été proposées par le Comité permanent R.

Après discussion la commission du suivi recommande au gouvernement ce qui suit:

1. De charger la Commission d'avis pour la non-prolifération des armes nucléaires (CANPAN) d'émettre des avis,
 - non seulement sur les exportations de biens et équipements visés par la loi du 9 février 1981 relative aux conditions d'exportation des matières et équipements nucléaires, ainsi que des données technologiques nucléaires,
 - mais aussi sur toute exportation de biens et équipements susceptibles de contribuer à la prolifération de systèmes d'armements non conventionnels ou très avancés, notamment:
 - les biens et équipement à double usage visés par l'Arrangement de Wassenaar et autres règlements européens en la matière;
 - ceux visés par le Régime de Contrôle de la Technologie des Missiles (*Missile Technology Control Regime* ou MTCR);
 - les armes chimiques et bactériologiques visées par la Convention sur les armes chimiques (CAC), signée à Paris le 14 janvier 1993.
2. De renforcer la coopération entre les services de renseignement et l'administration des douanes et accises en matière de lutte contre la prolifération.
3. D'associer de manière plus étroite et permanente les représentants de l'Administration des douanes et accises aux travaux de la CANPAN.
4. De veiller, autant que cela soit possible, à ce que les mêmes personnes assurent la continuité de la représentation des services auprès de cette commission; qu'en cas d'absence du délégué attitré, son remplaçant soit informé des dossiers et avis traités par le titulaire.

5. De permettre aux services de renseignement et aux administrations représentées au sein de la CANPAN d'échanger des informations classifiées relatives à la prolifération. Ceci devrait se concrétiser:
- en faisant conclure entre ces services un accord conformément à l'article 14 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;
 - en engageant le processus d'octroi d'une habilitation de sécurité aux membres de la CANPAN, à son personnel et à ses correspondants de l'Administration des Douanes et des Accises, ceci en application de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

Le présent rapport ainsi que ses recommandations ont été adoptées par la commission du suivi du Sénat le 30 janvier 2006 et présentées à la presse le 31 janvier 2006. Le contenu de présent rapport est répercuté et commenté par la presse au cours des jours qui ont suivi.

Compte-tenu de l'importance que la presse a accordé au rapport et à ses recommandations, la commission du suivi a aussi organisé un débat en séance plénière du Sénat le jeudi 2 février 2006¹². Un débat a également eu lieu à la Chambre des représentants le même jour¹³. Au cours de ces débats Vice-première ministre et ministre de la Justice ONKELINX a pu exprimer son point de vue sur cette affaire.

Elle a déclaré soutenir complètement les constatations et les conclusions du Comité permanent R telles qu'elles ont été rendues publiques par la commission du suivi le 31 janvier.

Madame la ministre a reconnu l'existence de dysfonctionnements à la Sûreté de l'État dans l'analyse, l'information, la communication et les relations avec le ministre de tutelle. Elle a annoncé une réorganisation de ce service.

Les recommandations adoptées par le Sénat feront l'objet de discussions entre la ministre et les principaux responsables présents et futurs de la Sûreté de l'État. Ce qui devrait déboucher sur une série d'instructions qui tiennent compte de l'enquête réalisée par le Comité permanent R.

La ministre a ajouté le commentaire suivant, auquel se rallie pleinement le Comité permanent R :

« De nombreux agents (de la Sûreté de l'État) sont sensibles à nos propos. Surtout, que l'on ne jette pas un voile noir sur toute l'activité de la Sûreté de l'État ! Elle ne le mérite pas. Énormément d'agents et la Sûreté dans son ensemble effectuent un travail tout à fait remarquable. Ce travail n'est pas visible. Mais, ce que nous voyons, ce sont les dysfonctionnements parce que nous avons voulu un système de contrôle qui s'est montré efficace. Permettez-moi de souligner tout le travail qui est réalisé pour la sécurité de notre pays en dehors de ces dysfonctionnements ! »

¹² Sénat, 2 février 2006, 3-149 / p. 37

¹³ Chambre des représentants, 2 février 2006, CRIV 51 PLEN 191, p. 6

CHAPITRE 2 : L'ENQUETE DE CONTROLE RELATIVE A UN INCIDENT DE TIR LORS D'UNE GARDE DES LOCAUX DE LA SURETE DE L'ETAT

1. INTRODUCTION

Le 12 mars 2005, le Comité permanent R a pris connaissance d'un article intitulé « *Grogne à la Sûreté de l'État* » paru dans l'édition du samedi 12 et dimanche 13 mars 2005 du journal « *La Libre Belgique* ». Une partie de cet article était sous-intitulée « *Quand un inspecteur tire vers un autre, il ... ne se passe rien* ». Selon le journaliste, une lettre anonyme lui aurait été adressée révélant un incident grave au sein du service. Au cours d'une nuit de novembre 2004, pendant un service de garde, un inspecteur de la Sûreté de l'État aurait tiré une balle de revolver en direction de son collègue sans l'atteindre. La découverte de cet incident, non autrement expliqué que par une erreur de manipulation, n'aurait entraîné aucune réaction particulière de la hiérarchie du service.

Lorsque l'article précité est paru, les faits y relatés n'avaient pas encore été portés à la connaissance du Comité permanent R par la direction de la Sûreté de l'État.

2. PROCÉDURE

2.1. L'enquête de contrôle

Dès le samedi 12 mars 2005, la Vice-Première Ministre et Ministre de la Justice ONKELINX a, par communication téléphonique faite à son Président, chargé le Comité permanent R de mener une enquête de contrôle sur l'incident relaté par l'article de presse précité.

Une délégation du Comité permanent R, composée de son Président, d'un conseiller et du greffier, s'est rendue le lundi 14 mars 2005 à la Sûreté de l'État pour y entendre les premières explications de l'Administrateur général.

La Vice-Première Ministre et Ministre de la Justice a confirmé sa demande orale d'enquête par un courrier que le Comité permanent R a reçu le 16 mars 2005.

« J'ai été informée, ce samedi par la presse, qu'un incident se serait déroulé au sein de la Sûreté de l'État à l'occasion d'une garde de nuit mettant en présence deux inspecteurs divisionnaires. Les faits se seraient déroulés dans le courant du mois de novembre 2004. D'après les informations relatées dans la presse, l'un des inspecteurs aurait tiré un coup de feu en direction de son collègue sans toutefois l'atteindre.

Cet incident n'a, à aucun moment, été porté à ma connaissance par l'Administrateur Général de la Sûreté de l'État, ni par aucun autre dirigeant au sein de la Sûreté de l'État. Je souhaiterais que le Comité permanent de contrôle des services de renseignement puisse me fournir un rapport rapidement sur les circonstances de cet incident et m'informer des suites à y réserver. »

La présidente du Sénat a été avertie de l'ouverture de l'enquête de contrôle par courrier du 16 mars 2005.

Au cours de son enquête, le Service d'enquêtes R a entendu :

- le directeur des opérations,
- la victime du coup de feu,
- l'administrateur général adjoint de la Sûreté de l'Etat,
- l'auteur du tir litigieux .

A la suite de l'audition de l'auteur du tir litigieux, le chef du Service d'enquêtes du Comité R a estimé qu'il devait dresser procès-verbal sur-le-champ et transmettre celui-ci au Procureur du Roi de Bruxelles, en application des articles 40 alinéa 3 et 46 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement.

Un rapport a été adressé à la Vice-Première Ministre et Ministre de la Justice ONKELINX le 30 mars 2005.

2.2. L'enquête judiciaire

Compte tenu du fait qu'une enquête judiciaire a également été menée au sujet des faits examinés dans le présent rapport, le Comité permanent R a fait application de l'article 69 §§ 1 à 5 (section 2) de son règlement d'ordre intérieur qui dispose ce qui suit :

« Lorsqu'à l'occasion d'une enquête de contrôle, un membre du Service d'enquêtes constate un crime ou un délit commis par un membre des services de renseignements, l'instruction judiciaire relative à ces faits prend la priorité sur l'enquête de contrôle.

L'enquête de contrôle se poursuit le cas échéant, en se limitant aux éléments qui sont nécessaires à l'accomplissement des missions du Comité R. Le chef du Service d'enquêtes en avise alors le magistrat responsable de l'enquête judiciaire.

Le rapport sur l'enquête de contrôle ne peut mentionner ni le détail des infractions, ni l'identité des personnes impliquées comme prévenu, témoin ou victime dans les faits qui font l'objet de l'enquête judiciaire.

Le rapport ne peut contenir aucune copie d'une quelconque pièce de la procédure pénale; il s'abstient de toute conclusion sur d'éventuelles responsabilités pénales de personnes ou de groupes de personnes.

En cas de doute sur l'un de ces points, le chef du Service d'enquêtes soumet ce point au magistrat en charge de l'enquête. Le chef du Service d'enquêtes se conforme aux instructions du magistrat sur le point douteux. »

Au cours de cette enquête, l'auteur du tir incriminé a été provisoirement privé de sa liberté et mis à la disposition de la Justice.

Le 31 mai 2006, le Comité permanent R n'a pas encore connaissance de l'issue de cette procédure judiciaire.

2.3. L'application de l'article 38 § 2 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements

Le 30 novembre 2005, le Comité permanent R a demandé au Procureur général près la Cour d'appel de Bruxelles d'autoriser le Service d'enquêtes à prendre connaissance du dossier de cette enquête.

Le procureur général a donné son accord le 28 décembre 2005.

3. CONSTATATIONS

Les premières conclusions de l'enquête de contrôle

L'incident qui s'est déroulé lors de la garde des 12 et 13 novembre 2004 dans les locaux de la Sûreté de l'État est très grave dans la mesure où la vie d'un agent participant à cette garde a été sérieusement mise en danger par son collègue.

Les articles 4 et 7 de l'arrêté ministériel du 6 mai 2003 « *déterminant les armes et les munitions faisant partie de l'équipement réglementaire des agents des services extérieurs de la Sûreté de l'État et fixant les dispositions particulières relatives à la détention, à la garde et au port de ces armes* » n'ont pas été appliqués.

L'article 4 prévoit : « *Peuvent seuls se voir confier pour l'exercice de leurs missions, l'une des armes visées à l'article 1^{er}, les agents qui (...) et qui sont jugés aptes par l'Administrateur général ou en son absence par l'Administrateur général adjoint à la Sûreté de l'État sur avis du directeur des opérations ainsi que des moniteurs de tir à détenir et à porter de telles armes ainsi qu'à en faire au besoin usage* ».

En l'occurrence, l'aptitude de l'auteur du coup de feu à détenir une arme n'a pas été reconsidérée par la direction de la Sûreté de l'État alors qu'un rapport interne récent signalait des problèmes de comportement de l'intéressé.

L'article 7 mentionne quant à lui que : « *Tout tir au moyen d'une arme à feu en dehors des exercices de tir, doit immédiatement être signalé à l'administrateur général ou en son absence à l'administrateur général adjoint de la Sûreté de l'État sous la forme d'un rapport circonstancié* ».

Aucune mesure n'a été prise immédiatement pour déterminer les causes de l'incident et notamment déterminer si on se trouvait en présence soit d'un accident, soit d'un geste volontaire prémédité ou non. Les autorités judiciaires n'ont pas été prévenues.

A aucun niveau, les réactions de la hiérarchie n'ont été adéquates par rapport à la nature et à la gravité de l'incident. Dès le départ celle-ci a accredité une version minimaliste et accidentelle des faits sans aucune remise en cause, vérification ni mesure conservatoire.

Une telle attitude est contraire au principe de bonne administration et au sens des responsabilités que l'on est en droit d'attendre de la part de la hiérarchie d'un service de l'État dont les agents peuvent détenir et utiliser des armes pour l'exercice de certaines missions.

En effet, au-delà des faits eux-mêmes, les conséquences d'une telle attitude sont aussi à stigmatiser, comme :

- Le sentiment « d'étouffement » ou « l'étouffement de l'incident » ;
- Le malaise interne que ce « sentiment » ou cette manière d'agir a provoqué ;
- La dénonciation des faits via la presse aux autorités de tutelle et au Comité permanent R, qui en est résultée, plutôt qu'une information directe de ceux-ci par la hiérarchie de la Sûreté de l'État ;

A plusieurs reprises le Comité permanent R a signalé ce type de dysfonctionnement interne particulièrement inquiétant qui résulte dans le chef de certains au sein de la Sûreté de l'État de la mise en œuvre d'une culture dévoyée du secret consistant à vivre dans un système clos et à garantir ce cloisonnement par tous les moyens, même en cachant un incident comme celui-ci et en tentant d'en faire disparaître les traces. La prise de mesure ou d'initiatives, après la divulgation des faits via la presse, ne peut en aucun cas, atténuer ce constat.

En l'occurrence, le Comité permanent R relève les éléments graves suivants :

- La rétention de l'information relative à l'existence même de l'incident à l'égard de la Ministre de tutelle, des autorités judiciaires et du Comité permanent R ;
- Le peu de rapports internes concernant l'incident de tir et leur inconsistance avant la divulgation des faits par la presse;
- La présentation par le tireur et l'acceptation par sa hiérarchie d'une version aseptisée des faits dès le départ, sans aucune remise en question ni vérification sérieuse ;
- La mise à l'écart ou la disparition volontaire des traces visibles de l'incident et du projectile ; l'absence de mesure conservatoire concernant l'arme utilisée, de son expertise, de contrôle des munitions restantes (l'intéressé s'est servi de son arme à trois reprises après les faits pour des exercices de tir en 2004) de même que l'absence d'une reconstitution des faits.

4. RECOMMANDATIONS

Concernant la problématique des armes de service, le Comité permanent R recommande :

- d'évaluer la nécessité de gardes armées des bâtiments de la Sûreté de l'État ;
- de mettre en place :
 - o une procédure basée sur des dispositions claires et précises sanctionnées disciplinairement ;
 - o un contrôle interne effectif ;
 - o une obligation d'informer les autorités responsables (Ministre de la Justice, autorités judiciaires, Comité permanent R) de tout incident relatif à la détention et à l'utilisation d'armes et de munitions ;

- d'appréhender d'une manière générale, dans le cadre du suivi de l'audit le problème lié à l'utilisation abusive du caractère protégé des missions de la Sûreté de l'Etat et des moyens qui y sont associés à des fins non légitimes.

En ce qui concerne les affectations, les promotions, les transferts et les réaffectations des membres des services extérieurs de la Sûreté de l'État, le Comité R s'interroge sur la portée du principe de « barrière » repris à l'article 3 de l'arrêté royal du 29 avril 1966. Cette « barrière » s'oppose au principe général de la mobilité du personnel de l'État.

Le Comité permanent R recommande également de reprendre, à propos de la détention et de l'usage des armes par le personnel de la Sûreté de l'État, la définition des aptitudes et des qualités de caractère requises telle qu'elle est définie dans l'arrêté ministériel du 2 septembre 1976, à savoir :

« Avoir une constitution neuropsychique bien équilibrée, un sens moral et un jugement suffisants permettant aux candidats de garder leur sang-froid dans toutes les circonstances et d'avoir au moment opportun, des réactions adéquates ».

Ces recommandations avaient été particulièrement formulées en 1996 dans le rapport général d'activités 1996 du Comité permanent R à propos de l'enquête « *Statuts des agents des services de renseignements* ». ¹⁴

5. AVIS DU MINISTRE DE LA JUSTICE

Le 12 mai 2006, madame ONKELINX fait parvenir au Comité permanent R la réponse suivante :

« J'ai bien reçu votre courrier du 2 mai dernier me demandant mes réactions par rapport aux recommandations que vous avez formulées dans le rapport établi à la suite de l'enquête menée à propos d'un incident de tir intervenu lors d'une garde des locaux de la Sûreté de l'Etat.

Dès que j'ai été informée de cet incident, soit quelques mois après sa survenance, j'ai immédiatement demandé à l'Administrateur général de l'époque, Monsieur Koenraad Dassen, de bien vouloir me faire un rapport précis de la situation, notamment quant à l'utilisation des armes lors de ces services de garde et d'une manière générale au sein des services de la Sûreté de l'Etat.

Cette demande a été suivie par la création d'un groupe de travail au sein même de la Sûreté de l'Etat, chargé de faire le point sur l'ensemble des questions soulevées à propos de cet incident.

Parmi les mesures qui ont été prises, il a notamment été question de revoir fondamentalement l'arrêté ministériel déterminant les armes et les munitions faisant partie de l'équipement réglementaire des agents des services extérieurs de la Sûreté de l'Etat et fixant les dispositions particulières relatives à la détention, à la garde et au port de ces armes.

Un projet d'arrêté ministériel m'a été récemment transmis et je compte rapidement l'adopter. Il tente de clarifier quels sont les agents de la Sûreté de l'Etat qui peuvent être porteurs d'une arme pendant les heures de service et dans quelles conditions. Par ailleurs, des mesures de sécurité ont été renforcées quant à la conservation de ces armes.

¹⁴ Comité permanent R, *Rapport d'activités*, 1996, Bruxelles, 1997, pp. 138-194 (www.comiteri.be).

Comme vous le savez, nous avons également entamé une vaste réforme du statut des agents des services extérieurs de la Sûreté de l'Etat et, dans ce contexte, nous avons plus particulièrement travaillé sur les aptitudes physiques et psychologiques de ces agents par le biais de contrôles médicaux. Nous envisageons également la création d'une « Stress Team » composée de deux psychologues, qui devraient au sein-même de la Sûreté de l'Etat, pouvoir aider les agents confrontés à des missions particulièrement délicates, notamment au niveau de la protection et de la filature.

Toutes ces dispositions seront insérées dans le futur statut des agents des services extérieurs de la Sûreté de l'Etat.

Enfin, il est également prévu des possibilités de réaffectation au sein-même de la Sûreté lorsqu'un agent n'est plus à même de remplir certaines missions, notamment, en raison de son état psychologique ou de son état de santé. Le statut devrait également permettre à certaines conditions la mobilité vers d'autres services. Mais les discussions sont toujours en cours sur ce point. »

TITRE 2

LES ENQUETES DE CONTROLE

B. ENQUETES MENEES A L'INITIATIVE DU COMITE PERMANENT R

CHAPITRE 1 : ENQUÊTE DE CONTRÔLE SUR UN INCIDENT DE SÉCURITÉ SURVENU AU SGRS

1. PROCÉDURE

Le 14 avril 2004, le chef du SGRS a informé le Comité permanent R de la survenance d'un grave incident de sécurité au SGRS dans la nuit du 26 au 27 février 2004. Le SGRS a également communiqué au Parquet fédéral un rapport sur cet incident provoqué par un ancien membre du SGRS. Le 19 avril 2004, le Comité a décidé d'ouvrir une enquête de contrôle sur la manière dont le SGRS avait traité cet incident de sécurité. Une apostille a été adressée au Service d'enquêtes R le 30 avril 2004. Le parlement et le ministre de la Défense nationale en ont été avertis respectivement le 3 et le 5 mai 2004.

Par note datée du 20 septembre 2004, le chef du Service d'enquêtes a fait savoir au Comité que le parquet fédéral l'avait chargé d'effectuer une enquête judiciaire sur les faits dénoncés par le SGRS.

Faisant suite à cette information, le Comité permanent R a décidé de suspendre son enquête de contrôle et d'attendre le résultat de l'enquête judiciaire à laquelle le Service d'enquêtes prêtait son concours (application de l'article 69, section 2 du règlement d'ordre intérieur du Comité).

Le 4 mai 2005, l'auteur des faits incriminés a introduit auprès du Comité permanent R un recours contre la décision prise par le SGRS de lui retirer son habilitation de sécurité. À cette date, le Comité avait encore la qualité d'organe de recours en matière d'habilitation de sécurité (article 3 de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité telle qu'elle était encore en vigueur à cette date). Le Comité permanent R a rendu une décision négative sur ce recours le 31 août 2005.

Le 13 septembre 2005, le Comité permanent R a demandé au magistrat fédéral l'autorisation de consulter les procès-verbaux rédigés par le Service d'enquêtes R dans le cadre de l'enquête judiciaire. Le 21 septembre 2005, le magistrat fédéral a transmis au Comité permanent R la copie de ces procès-verbaux.

Le 27 octobre 2005, le Comité a décidé de poursuivre son enquête de contrôle et de l'étendre aux circonstances dans lesquelles l'incident de sécurité est survenu au SGRS. Une nouvelle apostille a été adressée au Service d'enquêtes R le 3 novembre 2005. Le Service d'enquêtes a remis son rapport complémentaire le 10 mars 2006. Le présent rapport a été approuvé le 30 mars 2006.

2. APPLICATION DE L'ARTICLE 69 §§ 1 À 5 DU RÈGLEMENT D'ORDRE INTÉRIEUR

Compte tenu du fait qu'une enquête judiciaire a également été menée au sujet des faits examinés dans le présent rapport, le Comité permanent R a fait application de l'article 69 §§ 1 à 5 (section 2) de son règlement d'ordre intérieur (voir supra).

L'auteur des faits incriminés sera désigné comme étant M. X

3. CONSTATATIONS

3.1. Les états de M. X au sein du SGRS.

- M. X a été engagé en qualité d'employé civil de la section informatique du SGRS en juillet 1999 en qualité d'administrateur gestionnaire du système. D'abord engagé sous contrat de travail temporaire, M. X a été nommé en octobre 2000. M. X a été titulaire d'une habilitation de sécurité du niveau TRES SECRET ;
- La section informatique du SGRS gère les ordinateurs, les liaisons téléphoniques, GSM et satellites de ce service. La fonction initiale de M. X consistait à administrer ce réseau informatique, à y installer des programmes antivirus et à en assurer la maintenance ;
- Conformément aux règles en vigueur dans le service, M. X a été mis au courant des mesures de sécurité applicables au SGRS. L'intéressé a suivi des briefings internes lors de son entrée en service et a signé les documents par lesquels il reconnaît avoir été informé des mesures de sécurité en vigueur et être conscient de sa responsabilité particulière (notamment pénale) dans le respect de ces mesures ;
- En 2001, M. X, est muté au service INFOSEC ;
- La section INFOSEC est chargée de la sécurité du système informatique de l'ensemble des forces armées mais aussi d'autres autorités publiques. Cette section apporte son soutien à d'autres services fédéraux et internationaux. La Belgique ne dispose d'aucun autre service officiel chargé de la sécurité des systèmes d'information du gouvernement ;
- Au service INFOSEC, M. X effectue des études sur la sécurité de systèmes informatiques mais il n'est pas mêlé aux enquêtes ou aux activités de renseignement du SGRS ;
- Dans ces fonctions, M. X avait pourtant un accès illimité à toutes les données contenues tant dans le réseau sécurisé que non sécurisé du SGRS ;
- Tous les six mois, M. X signait le « *registre permanent* » au moyen duquel les consignes de sécurité étaient rappelées ;
- Au cours de l'année 2003, M. X se présente à un concours de recrutement organisé par une organisation internationale. Il réussit ce concours et est appelé à entrer au service de cette organisation début mars 2004.

3.2. Les faits constatés entre le 26 et le 27 février 2004

Le 26 février 2004, M. X signe les formulaires d'usage par lesquels l'attention du signataire est attirée sur son obligation de garder le secret après son départ du service.

M. X obtient l'autorisation de conserver son badge d'accès aux locaux de son service jusqu'au 27 février 2004, date à laquelle il sera tenu de le remettre au service de garde. Il passe la nuit du 26 au 27 février 2004 dans les locaux du service INFOSEC où il effectue de nombreuses photocopies. Il quitte les lieux le 27 vers 7h00 du matin en emportant des caisses en carton après avoir remis son badge d'accès au service de garde.

3.3. Découverte et traitement de l'incident de sécurité

Ce n'est qu'au cours d'une réunion tenue le lundi 1er mars 2004, qu'un commandant, signale que M. X a passé la nuit du 26 au 27 février 2004 dans les locaux du service INFOSEC. Cette présence parut anormale.

Le 2 mars 2004, un officier de sécurité se charge de mener une première enquête interne sur la présence de M. X dans les locaux du SGRS la nuit du 26 au 27 février 2004. Il interroge le caporal-chef qui était de garde au cours de cette nuit. Il demande aux supérieurs hiérarchiques de M. X si l'autorisation lui a été accordée de prendre des photocopies. Il questionne aussi de manière informelle d'autres membres du service INFOSEC. Plusieurs témoins déclarent avoir aperçu M. X occupé à faire des photocopies dans les locaux de SGRS entre le 26 et le 27 février.

Le premier rapport sur cette affaire est daté du 2 mars 2004 ; il consigne notamment ce qui suit :

- Le rapport du service de garde pour la nuit du 26 au 27 février ne contient aucune mention de ce fait ;
- Le caporal-chef de garde au cours de cette nuit confirme cependant la présence de M. X dans les locaux du service INFOSEC au cours de cette nuit. Il l'a vu employer la photocopieuse du service et emporter avec lui plusieurs boîtes de carton dont le contenu n'a pas été contrôlé ;
- Selon les premières constatations, M. X n'a – en principe - pas pu emporter avec lui des documents hautement classifiés ;
- Le rapport en conclut cependant que ces faits constituent un incident de sécurité de même qu'une infraction à la loi et aux règlements de sécurité avec compromission possible de documents classifiés ;
- Le rapport ajoute que ces faits sont susceptibles de constituer des actes d'espionnage ou de sabotage et qu'ils justifient un retrait de l'habilitation de sécurité de l'intéressé.

Le rapport prescrit des mesures complémentaires de vérification, notamment la convocation de M. X en vue de lui demander des explications.

Lors de son audition par le Service d'enquêtes R, le caporal-chef de garde au cours de cette nuit du 26 au 27 février 2004 déclare ne pas avoir interpellé M. X sur les motifs de sa présence dans les locaux. Sa mission n'était pas de contrôler les personnes présentes dans les locaux, seulement de fermer la porte du local vers 20 heures. Il affirme qu'il n'a pas considéré cette situation comme suspecte avant d'être interrogé par l'officier de sécurité.

Le 4 mars 2004, sur demande du SGRS, M. X adresse un courrier électronique à l'officier de sécurité du SGRS indiquant quels documents et cours techniques ont été copiés. M. X déclare n'avoir pris copie que de fichiers trouvés sur INTERNET ainsi que de quelques documents techniques, fichiers personnels et brouillons de programmes dont il était l'auteur.

Le second rapport daté du 5 mars 2004 communique la déclaration de M. X à sa hiérarchie. Il indique qu'aucune anomalie n'a été constatée au niveau des fichiers consultés par l'intéressé.

Le rapporteur tire cependant quelques leçons de cet incident qu'il qualifie de « sérieux » :

- plusieurs personnes étaient au courant des faits mais ont tardé à les signaler;
- le personnel de garde n'est pas intervenu lorsque M. X a quitté le SGRS le matin du 27 février 2004 en emportant des boîtes de documents.

L'officier de sécurité propose donc :

- d'organiser une campagne de sensibilisation du personnel aux règles de sécurité;
- de donner la compétence au personnel de garde de retenir quelqu'un à la sortie des installations du SGRS et de lui permettre de fouiller des personnes ;
- à défaut de pouvoir conférer de telles compétences au personnel de garde, de leur faire suivre une formation de MP (military police).

Le 9 mars 2004, un officier supérieur du SGRS rédige une note estimant que les faits ne constituent pas un vrai incident de sécurité, mais plutôt un usage illicite de moyens publics à des fins personnelles.

Le 12 mars 2004, M. X est entendu par quatre officiers et membres du SGRS sur son comportement. Il fut prié de rapporter tous les documents qu'il avait emportés avec lui ainsi que les fichiers qu'il avait gravés sur CD-Rom. L'inventaire des pièces écrites et fichiers électroniques rapportés par M. X est établi et contresigné par les membres du SGRS présents à l'audition.

Le 19 mars 2004, l'officier de sécurité adresse à sa hiérarchie le compte-rendu de l'audition de M. X. Ce rapport peut être résumé comme suit :

- L'intéressé confirme qu'il a choisi de passer la nuit à faire des photocopies personnelles pour ne pas bloquer la photocopieuse du service. Des problèmes techniques à la machine auraient retardé la prise de copies. M. X aurait aussi passé du temps à transmettre des courriers électroniques à un de ses collègues.
- Le supérieur hiérarchique de M. X reconnaît lui avoir donné l'autorisation de prendre des copies de quelques documents non classifiés mais pas de passer la nuit au secrétariat INFOSEC pour y photocopier un grand nombre de documents.
- Parmi les nombreuses photocopies remises par l'intéressé, ne se trouvait aucun document classifié.
- Par contre, un grand nombre de fichiers enregistrés sur CD portaient la classification « CONFIDENTIEL ». Certains d'entre eux étant particulièrement sensibles.

- M. X n'avait aucun « *need to know* » l'autorisant à prendre connaissance des documents classifiés qu'il avait enregistrés.
- L'officier de sécurité fait aussi remarquer qu'il n'existe aucune garantie que les documents et fichiers effectivement rapportés par M. X l'aient été dans leur totalité et leur intégralité.
- Le rapport conclut notamment que les faits suivants sont établis :
 - appropriation de documents appartenant à la Défense nationale,
 - reproduction et détention non justifiée de documents classifiés,
 - violation des règles de sécurité dans la gestion de documents classifiés n'ayant pas nécessairement pour conséquence une compromission de ceux-ci.
- Ces faits peuvent constituer des infractions pénales et justifient un retrait de l'habilitation de sécurité.
- Lors de son audition par le Service d'enquêtes R le 06/12/2004, M. X confirme les déclarations qu'il a faites le 12 mars 2004 au SGRS. Il n'a rien photocopié qui aurait trait aux missions de renseignement du SGRS, seulement les documents techniques. A cette occasion, il est possible qu'il ait transféré sans le vouloir des données sensibles et/ou classifiées qu'il détenait en sa qualité d'administrateur du réseau. Sa volonté n'a jamais été d'emporter ce type d'informations qui ne l'intéressaient pas, seulement celle de conserver l'expertise technique acquise au cours de son expérience professionnelle au SGRS.

3.4. Suites données à l'incident

3.4.1. Plainte judiciaire

Le 14 avril 2004, le SGRS adresse un rapport au Parquet fédéral ainsi qu'au Comité permanent R. Ce rapport impute à M. X la violation de règles de sécurité ainsi que plusieurs infractions pénales, parmi lesquelles une violation de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (appropriation et usage inapproprié de données classifiées).

Le rapport indique qu'il n'est pas certain que l'intéressé avait l'intention de transmettre à des tiers les informations qu'il avait recueillies. Le rapport ne se prononce donc pas sur une violation possible de l'article 119 du code pénal ¹⁵.

Le 17 septembre 2004, le Parquet fédéral ouvre une enquête judiciaire dont l'exécution est confiée au Service d'enquêtes R. Le 11 octobre 2005, le Parquet fédéral a fait savoir au Comité permanent R que ce dossier a été classé sans suite.

¹⁵ Loi du 19 juillet 1934, art. 1er. - Quiconque aura sciemment livré ou communiqué, en tout ou en partie, en original ou en reproduction, à toute personne non-qualifiée pour en prendre livraison ou connaissance, des objets, plans, écrits, documents ou renseignements visés à l'article 118, sera puni d'un emprisonnement de six mois à cinq ans et d'une amende de 500 francs à 5.000 francs. Sera puni des mêmes peines, quiconque, sans autorisation de l'autorité compétente, aura reproduit, publié ou divulgué, en tout ou en partie, par un procédé quelconque des objets, plans, écrits, documents ou renseignements visés à l'article 118.]

3.4.2. Retrait de l'habilitation de sécurité

Le SGRS a d'abord indiqué au Comité permanent R que l'intéressé ayant quitté le service depuis le 29 février 2004, il avait été décidé provisoirement de ne pas lui retirer son habilitation de sécurité. Le 14 avril 2005, le SGRS a retiré l'habilitation de sécurité dont M. X était titulaire.

Le 31 août 2005, le Comité permanent R, agissant en qualité d'organe de recours en matière d'habilitations de sécurité a rejeté le recours introduit par M. X contre la décision du SGRS lui retirant son habilitation de sécurité.

Le 20 décembre 2005, le Comité permanent R, agissant en qualité d'organe de recours en matière d'habilitations de sécurité, s'est déclaré incompétent pour connaître du recours introduit par M. X contre l'avis négatif exprimé par l'Autorité Nationale de sécurité au Chef de la sécurité d'une organisation internationale.

3.4.3. Les leçons tirées de cet incident de sécurité

Pour le SGRS, cette affaire démontre une fois de plus que le maillon le plus faible dans tout système de sécurité est l'élément humain. Il est donc d'une importance capitale que le personnel soit correctement et complètement informé des mesures de sécurité lors de son entrée en service. Ces mesures doivent être rappelées régulièrement. Le SGRS estime que les procédures actuellement en vigueur répondent à suffisance à cet impératif. Des audits de sécurité sont réalisés régulièrement (tous les trois mois), ce qui donne lieu, le cas échéant, à des adaptations et à des améliorations du contrôle, voire même à des sanctions disciplinaires en cas de faute.

3.4.4. Mesures prises dans le service

Le Comité permanent R a demandé si les mesures préconisées par l'officier de sécurité avaient été mises en oeuvre (rapport du 5 mars 2004).

Mise à part la poursuite de quelques démarches de sensibilisation à la sécurité via des affichettes apposées dans les locaux du SGRS, les recommandations précitées n'ont pas été suivies d'effet. L'élargissement des compétences du personnel de garde avec imposition de rondes de garde supplémentaires n'a pas été jugé opportun. De telles mesures ne sont appliquées qu'exceptionnellement, seulement lorsque le niveau de vigilance est augmenté. Seules les procédures d'accès au réseau informatique sécurisé ont été renforcées, notamment par l'instauration d'une accréditation.

4. CONCLUSIONS

Sur papier, les mesures de sécurité en vigueur au SGRS semblent appropriées et suffisantes, notamment en ce qui concerne l'information et les briefings de sécurité donnés aux membres du personnel.

Ces mesures semblent avoir été correctement appliquées à M. X aussi bien au moment de son entrée en service que pendant ses états de service. La responsabilité personnelle de M. X dans cet incident paraît évidente et justifie le retrait de son habilitation de sécurité. Le Comité permanent R ne se prononce pas sur la responsabilité pénale de l'intéressé.

Le Comité permanent R partage l'avis du SGRS que le maillon le plus faible dans tout système de sécurité est l'élément humain.

Par ailleurs, le Comité permanent R se demande pourquoi, entre le 27 février et le 1^{er} mars 2004, personne au SGRS n'a eu le réflexe de prévenir un officier de sécurité de la présence inhabituelle de M. X dans les locaux du SGRS la nuit du 26 au 27 février et de ses travaux de photocopies. Des directives commandent pourtant que chaque incident de sécurité soit immédiatement porté à la connaissance de l'officier de sécurité ou de la hiérarchie. Ceux qui ont constaté le comportement inhabituel de M. X ne semblent pas l'avoir perçu immédiatement comme un incident de sécurité. Le Comité permanent R s'interroge aussi sur la passivité de l'agent de garde face au comportement de M. X.

Cette attitude pose le problème du rôle et des missions attribuées au personnel de garde. Les consignes en vigueur pour l'établissement des rapports de garde indiquent que toute irrégularité doit être indiquée. La présence de M. X dans les bâtiments du SGRS la nuit n'a pas été considérée comme une irrégularité.

Le Comité permanent R se demande donc pourquoi le personnel de garde (la police militaire ?) ne pourrait recevoir quelques pouvoirs de police administrative, notamment celui de contrôler le comportement et les agissements suspects des personnes présentes dans les locaux à des moments inhabituels.

Le Comité permanent R estime que des mesures particulières devraient être prises en ce qui concerne la présence de personnes dans les bâtiments en dehors des heures habituelles de service :

- justification et autorisation préalable d'un chef de corps,
- avertissement de la hiérarchie,
- avertissement au corps de garde,
- la présence d'une seule personne ne devrait, en principe, pas être autorisée

Compte-tenu des conclusions présentées par l'officier de sécurité dès le 2 mars 2004 (incident de sécurité, suspicion d'acte d'espionnage ou de sabotage, compromission de documents classifiés, etc.), le Comité permanent R se demande pourquoi le SGRS a attendu le 14 avril 2004 pour porter les faits à la connaissance des autorités judiciaires. Une plainte immédiate avec demande de perquisition à domicile, de saisie, aurait permis d'apprécier plus rapidement la réalité et l'étendue de l'incident.

Le rapport de cette enquête de contrôle a été transmis le 4 avril 2006 ainsi que le 26 juin 2006 à l'attention du ministre de la Défense nationale FLAHAUT.

5. AVIS DU MINISTRE DE LA DEFENSE NATIONALE

Le 22 août 2006 le ministre de la Défense nationale a fait connaître son avis sur le présent rapport :

“En ce qui concerne l’enquête “sur un incident de sécurité au SGRS”, le rapport conclut que les mesures de sécurité existantes au SGRS sont suffisantes sur papier. Comme vous le soulignez à juste titre, relayant en cela le SGRS, dans tout système de sécurité, l’élément humain reste cependant le maillon faible. Mais bien entendu, il y a des possibilités d’amélioration et j’abonde dans ce sens.

Toutefois, l’intéressé était titulaire d’une habilitation de sécurité de niveau TRES SECRET. Il n’y avait dès lors, pour le SGRS, a priori pas de raison de le soupçonner quant à l’utilisation des moyens mis à sa disposition pour l’exécution de ses missions, tels que carte d’accès électronique, accès au réseau “secure” du SGRS, photocopieuses ou ordinateur.

En raison du dispositif de cartes d’accès électronique, il n’est pas anormal que le personnel de garde ne contrôle pas systématiquement les personnes disposant d’une telle carte.

De plus, le personnel de garde n’est pas habilité à procéder à des fouilles de personnes entrant et sortant du bloc sans accord de leur part. Recourir à la Police militaire ne serait d’aucune utilité dans la mesure où les compétences de celle-ci se limitent à certaines infractions de roulage. Les policiers militaires ne sont pas habilités, au contraire des agents de la police fédérale ou locale, à effectuer des fouilles. De surcroît, en dehors des heures normales de travail, elle ne dispose que d’une permanence minime dans le quartier militaire réservé au SGRS.

L’augmentation du contrôle systématique d’accès sur les réseaux informatiques en dehors des heures normales de service, l’installation d’un point central pour copier et imprimer, la fermeture de toute possibilité de copier sur les ordinateurs des utilisateurs même et finalement un contrôle journalier du listing des présences exceptionnelles en dehors des heures normales de service par l’officier de sécurité seront envisagés.

D’autre part, s’il y a lieu de déposer une plainte auprès des autorités judiciaires, celle-ci ne peut être effectuée qu’après que l’intéressé ait été entendu et que les copies et CD’s aient été soigneusement examinés. Ce qui explique quelque peu le délai écoulé entre la prise de connaissance de l’incident et le dépôt de la plainte.

A l’avenir, il sera évidemment fait en sorte que ce genre d’incident ne se reproduise plus.”

CHAPITRE 2 : ENQUETE COMMUNE DES COMITES P ET R RELATIVE A LA COORDINATION ENTRE LES DIFFERENTS SERVICES DE RENSEIGNEMENT ET DE POLICE DANS LA LUTTE CONTRE LE TERRORISME

Lors de la réunion conjointe des Comités permanents P et R du 11 décembre 2003, il fut décidé d'ouvrir une enquête de contrôle commune sur le thème de la coordination entre les services de police et de renseignements dans la lutte contre le terrorisme.

Le 17 décembre 2003, cette enquête fut portée à la connaissance des présidents de la Chambre et du Sénat.

Les ministres de la Justice et de la Défense en furent également informés par une lettre datant du 23 décembre 2003.

Il fut convenu que les Comités enverraient un questionnaire commun aux différents services sous leur responsabilité.

Le 12 janvier 2004, la Sûreté de l'État et le Service général du renseignement et de la sécurité furent dès lors interrogés par le Comité permanent de contrôle des services de renseignements.

Les 2 et 3 février 2004, ces services répondirent à l'enquête.

Cette enquête donna une image des services concernés par cette problématique et de la méthode de travail utilisée.

Les informations récoltées (et par ailleurs confidentielles) ne constituaient pas la partie la plus importante de l'enquête. Il s'agissait surtout de connaître les réponses relatives au thème principal : la coordination entre les services de renseignements et les services de police dans la lutte contre le terrorisme.

Les réponses fournies révélèrent que tant la collaboration entre les services de renseignements eux-mêmes qu'entre les services de renseignements et les services de police pouvait être améliorée.

En matière de coordination aussi, cette enquête confirma le besoin régulièrement constaté par le Comité permanent R de clarifier la manière dont les différents services peuvent collaborer. La problématique soulevée par cette enquête confirma ainsi celle signalée par le Comité permanent R concernant la collaboration et la coordination.

Dans l'intervalle, les avis du Comité permanent R furent repris par le gouvernement et les travaux relatifs à la création d'un nouvel organe de coordination (OCAM) sont en cours.

L'objectif de cette enquête (améliorer la coordination en matière de terrorisme) a dès lors perdu son intérêt, de telle sorte que l'attention pourra se porter sur la manière dont les services respecteront cette nouvelle législation.

TITRE 2

LES ENQUETES DE CONTROLE

C. PLAINTES DE PARTICULIERS ET DENONCIATIONS

CHAPITRE 1 : PLAINTE D'UN PARTICULIER À L'ENCONTRE DE L'ADMINISTRATEUR GÉNÉRAL DE LA SÛRETÉ DE L'ÉTAT

En juin 2004, le Comité permanent R a reçu la plainte d'un particulier qui imputait à M. DASSEN, administrateur général de la Sûreté de l'État, la rupture de certaines promesses et de certains contrats de consultance passés avec certaines administrations publiques. Le plaignant imputait ces ruptures à une animosité personnelle que lui aurait vouée M. DASSEN.

Le Comité permanent R n'a pas trouvé la moindre trace d'animosité personnelle de M. DASSEN à l'égard du plaignant. Tout semble indiquer que les relations entre ces deux personnes ont commencé sous un jour neutre sinon favorable. Ensuite, M. DASSEN s'est quelque peu distancié du plaignant avant de couper les ponts avec lui suite à certaines de ses déclarations dans la presse. Cette rupture n'est cependant pas apparue comme étant ferme et définitive.

Le Comité permanent R n'a pas la compétence d'examiner les décisions prises par certains ministres de rompre certains contrats ou engagements pris avec le plaignant.

Il est apparu que ces décisions ont été prises par les ministres compétents après avoir reçu un avis de la Sûreté de l'État, par les soins de M. DASSEN. Cet avis ne visait pas à la rupture des relations contractuelles entamées avec le plaignant mais à établir une clause de confidentialité dans ces relations. Le Comité permanent R estime que cet avertissement de la Sûreté de l'État aux autorités n'était ni disproportionné, ni dénué de fondement.

Le SGRS a également recommandé une certaine prudence dans les contacts que le SPF Défense nationale pourrait nouer avec le plaignant mais il n'a nullement cherché à en dissuader son ministre.

Ayant informé les autorités de la sorte, la Sûreté de l'État et le SGRS ont agi en conformité avec leurs missions légales. Ces services ne peuvent subir le reproche d'avoir atteint aux droits du plaignant.

Ce dernier ayant par ailleurs fait savoir qu'il retirait sa plainte, le Comité permanent R a décidé de la clôturer en l'état.

Avis de la Vice-première ministre et ministre de la Justice ONKELINX

Le 1^{er} juin 2006, la Vice-première ministre et ministre de la Justice a adressé un courrier au Comité dans lequel elle n'émet aucune remarque quant à la publication du présent rapport.

CHAPITRE 2 ENQUÊTE SUR LES INFORMATIONS RECUEILLIES, TRAITÉES ET COMMUNIQUÉES PAR LA SÛRETÉ DE L'ÉTAT À PROPOS DE LA DEMANDE DE RÉGULARISATION DE SÉJOUR D'UN PLAIGNANT

Au mois de novembre 2005, le Comité permanent R a ouvert une enquête de contrôle sur la plainte d'un particulier à l'égard de la Sûreté de l'État. Le plaignant estimait que les informations communiquées à l'Office des Étrangers par la Sûreté de l'État à propos de sa demande de régularisation de séjour étaient erronées et qu'elles devaient être modifiées.

Après avoir consulté les données recueillies par la Sûreté de l'État, le Comité permanent R a estimé que les informations communiquées par ce service n'étaient pas erronées et que les droits du plaignant n'avaient pas été transgressés. Sa plainte n'était pas fondée.

Avis de la Vice-première ministre et ministre de la Justice ONKELINX

Par courrier du 31 mai 2006, Madame la ministre de la Justice nous a fait part de ses remarques :

« Je prends bonne note du fait que le Comité R estime que les informations qui ont été communiquées par la Sûreté de l'Etat à l'Office des étrangers n'étaient pas erronées, et que les droits du plaignant en l'espèce n'ont pas été transgressés. »

Je n'ai pas d'objection à ce que cette conclusion soit bien entendu publiée dans votre rapport général d'activité pour l'année 2005. »

CHAPITRE 3

ENQUÊTE DE CONTRÔLE SUITE À UNE PLAINTE D'UN PARTICULIER CONCERNANT LA TRANSMISSION D'INFORMATIONS PAR LA SÛRETÉ DE L'ÉTAT À L'OFFICE DE LA NAISSANCE ET DE L'ENFANCE

1. INTRODUCTION

Au cours du mois d'avril 2005, le Comité permanent R a pris connaissance, via plusieurs articles de presse, d'une polémique entre l'Union professionnelle des accoucheuses belges et l'Office de la Naissance et de l'Enfance (ONE).

En cause, une circulaire largement diffusée par l'ONE auprès du monde médical mettant en garde les acteurs de la santé contre l'infiltration du secteur de la petite enfance par une secte appelée « Cercle des Amis de Bruno Gröning ». L'origine de cette information serait une lettre adressée à l'ONE par la Sûreté de l'État.

Plusieurs journalistes se sont interrogés sur le rôle que la Sûreté de l'État a joué dans cette affaire tournant à polémique.

Ces informations ont attiré l'attention de certains membres du Parlement de la Communauté française qui ont questionné la ministre de la Santé et de l'Aide à la Jeunesse. L'infiltration possible du secteur de la petite enfance par une secte a fait l'objet d'un débat en commission le 12 avril 2005¹⁶.

2. PROCÉDURE

Le 20 mai 2005, le Service d'enquêtes R a reçu une plainte émanant de madame X, sage-femme de profession, dirigée contre la Sûreté de l'État. Le Comité permanent R a approuvé le présent rapport non classifié le 4 novembre 2005. Il a été adressé à la ministre de la Justice le 7 novembre 2005. Celle-ci en a accusé réception et a communiqué ses premières remarques au Comité permanent R le 21 novembre 2005.

3. L'OBJET DE LA PLAINTE

Madame X, sage-femme de profession, reproche à la Sûreté de l'État le contenu d'un courrier adressé à l'Office de la Naissance et de l'Enfance le 7 février 2005. Aux termes de ce courrier ce service dénonçait l'infiltration par la secte « les amis de Bruno Gröning » dans certains secteurs liés à l'enfance.

Madame X ne conteste nullement avoir fait partie du groupe de prière des « amis de Bruno Gröning » à une époque où elle connaissait des problèmes dans sa vie privée.

¹⁶ Commission de la Santé, des Matières de l'Aide à la Jeunesse du Parlement de la Communauté française, session 2004-2005 – CRlc N° 43-Santé 11 – compte rendu intégral 12 avril 2005

Selon madame X, la Sûreté de l'État fut au courant de son adhésion à ce groupe par le simple fait qu'une conférence fut organisée à Bruxelles et que son nom figurait sur la liste des participants. Elle déclare qu'elle ne fait plus partie de cette organisation depuis 2001 et déplore que la Sûreté de l'État n'ait pas effectué d'enquête pour déterminer si elle constituait un risque pour les organisations dans lesquelles elle travaille, notamment au travers d'activités de propagande

Madame X explique que cette information diffusée par la Sûreté de l'État, et répercutée dans le monde médical, nuit gravement, non seulement à sa propre réputation, mais également à celle du secteur professionnel auquel elle appartient.

Madame X demande au Comité permanent R :

- de vérifier ce qui a poussé la Sûreté de l'État à lancer pareilles informations à son sujet ;
- de vérifier la pertinence de ces informations en rapport avec sa vie actuelle puisqu'elle affirme avoir mis fin à sa participation aux activités de ce groupe de prière au début de l'année 2001 ;
- de vérifier si la Sûreté de l'État a pris soin de vérifier si son activité professionnelle a été influencée de manière négative par ces activités qui relèvent de sa vie privée ;
- de vérifier si la Sûreté de l'État a pris soin de vérifier dans son milieu professionnel si elle adoptait une attitude de prophylaxie lors de ses activités professionnelles ;
- de rectifier les données à son sujet qui reposent dans les dossiers de la Sûreté de l'État ;
- enfin, de redresser l'image de marque de la profession en donnant des informations sur les maisons de naissance et la profession de sage-femme. »

4. LES VÉRIFICATIONS EFFECTUÉES PAR LE COMITÉ PERMANENT R

Le Comité permanent R a donné instruction à son service d'enquêtes :

- de se faire remettre copie de toutes les informations, notes et rapports dont la Sûreté de l'État dispose à propos de madame X;
- d'examiner quand et comment ces informations ont été obtenues, recoupées, actualisées et analysées ;
- de vérifier de quelle manière la Sûreté de l'État fut informée de la participation de madame X à une réunion publique du « *Cercle des amis de Bruno Gröning* » en septembre 2000 ;
- d'examiner dans quel but ces informations ont été transmises aux autorités ;
- d'en apprécier tant la véracité que la pertinence par rapport aux missions légales de la Sûreté de l'État.

5. CONSTATATIONS

Le 7 février 2005, la Sûreté de l'État a adressé le courrier suivant, non classifié, à l'administratrice générale de l'Office National de l'Enfance et de la Naissance.

Extraits :

« Objet : le Cercle des Amis de Bruno Gröning – infiltration du secteur de la petite enfance (maisons de la naissance et autres activités pour enfants)

« Le Cercle des Amis de Bruno Gröning présente un certain nombre de caractéristiques propres à lui faire rencontrer la définition de l'organisation sectaire nuisible posée par les articles 7 et 8 de la loi du 11.12.1998 (lire : loi du 30.11.1998) organique des services de renseignement et de sécurité. Au nombre de ces caractéristiques, il convient de mentionner le danger potentiel que les préceptes doctrinaux de ce mouvement sont susceptibles de faire courir aux adeptes, principalement en mettant en péril leur intégrité physique.

Il est établi que ce mouvement s'intéresse au corps médical et para-médical et que, par ce biais, il tente également d'infiltrer le milieu de la petite enfance. Une des membres du Cercle active dans cette stratégie est madame X, accoucheuse, ayant lancé une maison de la naissance, à Liège, (la Maisonnée), faisant partie du réseau Alter-natives. Les deux ASBL ont été reconnues par l'ONE. Outre Liège, le concept des maisons de la naissance s'est étendu à Namur et, semble-t-il, à La Louvière ainsi qu'en Flandre (sans autre précision possible à cette date).

Le concept des maisons de la naissance rencontre sur certains points les thèses de ce groupement qui s'inspire de l'enseignement du gourou allemand, Bruno Gröning. Les adeptes croient en la prééminence d'une intervention divine, grâce à l'intercession de Bruno Gröning, dans la prévention, le traitement et la guérison des maladies. Dans cette logique, la place de la médecine traditionnelle est essentiellement supplétive.

Dans les faits, ceci représente un danger potentiel pour les malades qui tombent entre leurs mains. Le Cercle n'hésite d'ailleurs pas à porter cette contestation sur la place publique en organisant des conférences et des séminaires de sensibilisation à destination du corps médical. C'est au cours d'une réunion organisée par ce mouvement, à Bruxelles (...), que madame X est intervenue en septembre 2000.

Qu'en est-il aujourd'hui ? L'intérêt du Cercle des Amis de Bruno Gröning pour le secteur de la petite enfance se précise et s'articule autour de deux cibles.

En premier lieu, il reste le réseau des maisons de la naissance. On peut signaler l'ouverture de l'ASBL la Maison de la naissance à Bruxelles (rue du Vieux Moulin, 67 à 1160 Bruxelles) dont il ressort qu'elle s'inspire des idées de Bruno Gröning. Comme la Maisonnée à Liège, elle offre un accompagnement aux futurs parents au cours de tout le processus allant de la grossesse à la naissance, en ce compris une aide particulière en cas de décès. Les promoteurs de la maison de Bruxelles insistent sur le choix qui est offert aux parents d'accoucher en dehors du cadre établi qu'est le milieu hospitalier.

Ce dernier élément suscite des interrogations en cas de grossesse ou de naissance difficile, compte-tenu des opinions affichées par le Cercle des Amis de Bruno Gröning et, ce malgré les assurances données par madame X dans des interventions récentes dans la presse. (...)

La seconde forme d'infiltration du secteur de la petite enfance que le Cercle des Amis de Bruno Gröning a l'intention de privilégier est l'organisation d'activités ludiques à destination des enfants.

Au regard de ce qui précède et compte tenu de la nocivité du Cercle des Amis de Bruno Gröning, il nous paraît utile d'attirer l'attention des autorités concernées sur le risque encouru par le secteur de la petite enfance, à cause des desseins précis que nourrit ce mouvement à l'endroit des enfants et de leurs parents. »

La lettre est signée par l'administrateur général adjoint de la Sûreté de l'État. Un courrier semblable est également adressé à Madame la ministre de la Justice ainsi qu'au Procureur fédéral.

Le 16 mars 2005, la Sûreté de l'État donne son accord pour que l'ONE fasse état des informations fournies dans le cadre d'une circulaire. Il est cependant demandé de porter attention à la problématique générale plutôt qu'à des aspects particuliers.

Dans une circulaire du mois de mars 2005, forte de l'autorisation obtenue, l'ONE répercute quasi littéralement le point de vue de la Sûreté de l'État, sans référence toutefois au patronyme de madame X.

Le 12 avril 2005, la ministre de l'enfance, de l'aide à la jeunesse et de la santé est interpellée au Parlement de la Communauté française sur la circulaire de l'ONE. Elle justifie de la manière suivante la mise en garde que cet organisme a adressée aux professionnels de la naissance et de la petite enfance : (extraits) « *Il m'apparaît que l'ONE ainsi que son administration générale ont agi dans le sens et dans le cadre des responsabilités de l'Office vis-à-vis des enfants et des familles en transmettant les informations reçues d'une source aussi crédible que la Sûreté de l'État à ces professionnels, et ce sans en modifier la teneur. (...) Nous constatons par ailleurs que le courrier de la Sûreté de l'État – institution spécialisée dans le renseignement s'il en est – était rédigé d'une manière affirmative, laissant peu de place au doute et aux nuances* »¹⁷.

Madame X s'adresse à la Sûreté de l'État le 14 avril 2005 : « *au vu des erreurs et mensonges figurant dans la lettre de l'ONE, je souhaiterais que me soit adressée une copie de ce qui figure dans mon dossier à la Sûreté de l'État afin que j'en vérifie le contenu* ».

Le 13 mai 2005, l'Administrateur général de la Sûreté de l'État adresse une réponse à la plaignante. Après avoir précisé que la Sûreté de l'État ne détient pas de dossiers au sujet de personnes mais assure le suivi de phénomènes conformément à la loi du 30 novembre 1998, il conseille à madame X de s'adresser à la *Commission de la Protection de la Vie Privée*, compétente en vertu de l'article 13 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Compte tenu de la polémique déclenchée par ces courriers, la Sûreté de l'État explicite sa position à l'intention de l'ONE.

Nous reproduisons littéralement les passages essentiels d'un document daté du 14 avril 2005.

¹⁷ Commission de la Santé, des Matières de l'Aide à la Jeunesse du Parlement de la Communauté française, session 2004-2005 – CRIC N° 43-Santé 11 – compte rendu intégral 12 avril 2005.

« Dans sa stratégie, cette organisation¹⁸ a ciblé des associations de femmes accoucheuses dont celles regroupées parmi les maisons de (la) naissance. Ces ASBL ne sont pas elles-mêmes sectaires mais certaines d'entre elles font déjà l'objet d'une ingérence de la part du "Cercle des Amis de Bruno Gröning". Cette infiltration est insidieuse dans la mesure où l'une de leur tactique est que les membres ne fassent pas état de leur appartenance à la secte. Si nos soupçons concernant l'infiltration de certaines maisons de naissance sont nettement fondées (« La Maisonnée », notamment), la mention de l'ASBL la Maison de la naissance de Bruxelles dans la note de la Sûreté de l'État s'appuie sur de nombreux signes (cf. ci-dessous) pour le moins interpellants indiquant une très grande proximité entre celle-ci et les Maisons de naissance. Les accointances fortes, relevées dans nos recherches, entre ces diverses entités ont conduit à émettre la thèse selon laquelle La Maison de la naissance de Bruxelles était, à son tour, l'objet d'une infiltration de la part du "Cercle des Amis de Bruno Gröning".

Et la Sûreté de l'État d'énumérer une série de signes qui, selon son analyse, incitent à la confusion.

6. LA POSITION DE LA SÛRETÉ DE L'ÉTAT

Dans un courrier adressé au Comité permanent R le 21 avril 2005, l'Administrateur général de la Sûreté de l'État justifie son intervention auprès de l'ONE de la manière suivante :

« Conformément à l'article 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, la Sûreté de l'État a informé l'ONE qu'une organisation sectaire nuisible, en l'occurrence le Cercle des Amis de Bruno Gröning, tentait d'infiltrer le milieu de la petite enfance (domaine de compétence de l'ONE) et plus spécifiquement les ASBL qui sont citées dans la note du 7 février 2005.

L'objectif de la Sûreté de l'État était donc d'attirer l'attention de l'autorité compétente – l'ONE – du danger que représente pour les enfants et leurs parents l'infiltration d'une organisation sectaire nuisible au sein d'institutions proposant leur accompagnement au cours de la période qui précède et qui suit la naissance d'un enfant.

La démarche de la Sûreté de l'État s'inscrit donc dans le processus d'information d'une autorité administrative en vue de lui permettre de mener, en connaissance de cause, la gestion de ses affaires et de prendre les mesures qu'elle estime nécessaires et/ou utiles.

Dans ce contexte, la transmission par la Sûreté de l'État des informations qu'elle possède ne doit pas s'apprécier au regard de l'attitude que les destinataires des informations pourraient éventuellement adopter – attitude par rapport à laquelle la Sûreté de l'État doit par ailleurs rester neutre, compte tenu qu'il ne lui appartient pas de s'immiscer dans la gestion des affaires d'une autre autorité administrative. La crainte d'une attitude inadéquate ne peut pas être un critère de non-communication de ses informations aux autorités compétentes, notamment lorsqu'il s'agit d'une menace à l'égard de la sûreté intérieure de l'État, en l'occurrence la sécurité et la sauvegarde physique et morale des personnes.

Suivi de cette affaire : Il convient d'observer que les enquêtes concernant l'infiltration du milieu de la petite enfance, notamment par l'organisation sectaire nuisible concernée, se poursuivent compte tenu de l'évolution de ce phénomène ».

¹⁸ Le Cercle des Amis de Bruno Gröning

7. CONCLUSIONS

L'intérêt que la Sûreté de l'État porte au Cercle des Amis de Bruno Gröning se justifie par l'une de ses missions légales qui est d'enquêter sur les menaces potentielles émanant des organisations sectaires nuisibles.

Plusieurs associations privées et organismes officiels attirent l'attention du public sur certaines caractéristiques pouvant conférer au Cercle des Amis de Bruno Gröning la qualification d'organisme sectaire nuisible.

Ce mouvement est notamment mentionné dans le rapport publié en 1998 par la commission d'enquête du parlement allemand « *on So-called Sects and Psychogroups* » (p. 258). Ce rapport est intitulé : « *New Religious and Ideological Communities and Psychogroups in the Federal Republic of Germany* »¹⁹. Le rapport bisannuel 2003/2004 du Centre d'Information et d'Avis sur les Organisations Sectaires Nuisibles (CIAOSN) consacre lui aussi une note d'information sur le Cercle des Amis de Bruno Gröning²⁰. Ce mouvement est en outre cité sur les sites de quelques associations « *anti sectes* »²¹.

Le souci de la Sûreté de l'État d'avertir les autorités civiles, politiques et judiciaires des tentatives d'infiltrations des milieux sectaires et des menaces insidieuses qu'elles représentent pour la société civile est justifié.

Ce souci légitime a pourtant amené la Sûreté de l'État à mettre en cause l'activité professionnelle de madame X auprès d'une autorité administrative. Affirmant un rôle actif de sa part dans cette stratégie d'infiltration, la Sûreté de l'État a nommément cité la plaignante dans un courrier adressé à l'Office National de l'Enfance et de la Naissance.

Portées à la connaissance des médias, les allégations de ce service ont provoqué une polémique et des réactions d'indignation de la part tant de la plaignante que de l'association professionnelle dont elle est membre. C'est l'ensemble d'une catégorie professionnelle qui s'est estimé injustement attaqué.

La seule information avérée dont disposait alors la Sûreté de l'État quant à l'appartenance supposée de madame X au Cercle des Amis de Bruno Gröning était sa participation, comme oratrice, à une conférence organisée par cette association à Bruxelles le 17 septembre 2000. Ce seul fait patent et reconnu par la plaignante ne peut cependant être considéré comme suffisant pour attribuer un rôle clé à madame X dans une stratégie d'infiltration sectaire dans les milieux de la petite enfance et de la naissance.

L'affirmation selon laquelle les ASBL créées ou soutenues par madame X peuvent servir de lieu de recrutement au cercle des Amis de Bruno Gröning n'était donc qu'une simple hypothèse formulée par la Sûreté de l'État.

La Sûreté de l'État n'a pas pris la peine de faire vérifier, analyser et confirmer cette hypothèse avant de la communiquer, sans nuance et comme fait avéré, à l'ONE, au parquet fédéral et à la ministre de la Justice.

¹⁹ Disponible sur www.csi.org/infoserv_articles/german_enquete_commission_report.htm

²⁰ document 7, (pages 37 et 38) disponible sur www.ciaosn.be/rapport_bisannuel/2003-2004.pdf

²¹ notamment www.unafdi.org - www.prevensectes.com - www.voltairenet.org/article372.html

Le Comité permanent R estime qu'en agissant de la sorte, la Sûreté de l'État a agi avec légèreté : non seulement elle a attenté à la vie privée de la plaignante, mais elle a aussi mis en péril sa réputation et son intégrité. Interpellée par l'ONE et par la polémique provoquée par sa note, la Sûreté de l'État a par la suite tenté de justifier sa position, tout en admettant alors qu'il ne s'agissait que d'une hypothèse et de soupçons. L'enquête menée par la Sûreté de l'État pour mettre à jour ses données après le déclenchement de la polémique ne confirme pas l'activisme de madame X au sein du Cercle des Amis de Bruno Gröning. Cette enquête attire par contre l'attention sur l'influence que tentent encore de prendre d'autres groupes réputés sectaires sur le milieu de la naissance et de la petite enfance. Il s'agit d'associations signalées comme étant liées à des sectes par plusieurs organismes officiels (MIVILUDES en France, CIAOSN en Belgique, ...) et associations anti-sectes ²².

8. RECOMMANDATIONS

Le Comité permanent R invite la Sûreté de l'État à plus de prudence et à un meilleur travail d'analyse et d'actualisation lorsqu'elle met une personne en cause auprès d'une autorité administrative, politique ou judiciaire.

Le Comité rappelle la recommandation qu'il avait émise dans ses rapports d'activités des années 1996 et 1997 :

« Le Comité estime qu'une personne qui fait état d'un préjudice matériel ou moral vraisemblable en rapport avec des informations contenues sur elle dans un dossier des services de renseignements devrait pouvoir obtenir, sous certaines conditions mais de manière plus large qu'aujourd'hui, un droit de consulter ces documents. L'opportunité de permettre ou de refuser cet accès ne doit pas être laissée à la seule appréciation des services de renseignements »²³.

Le Comité estime que la présente enquête illustre de manière évidente la pertinence de cette recommandation.

9. ECHANGE DE VUES ENTRE LA MINISTRE DE LA JUSTICE, LE COMITÉ PERMANENT R ET LA SÛRETÉ DE L'ÉTAT.

Par courrier du 21 novembre 2005, la Ministre de la Justice ONKELINX a communiqué la réaction suivante au Comité :

« C'est avec beaucoup d'attention que j'ai lu vos conclusions et estime effectivement que la Sûreté de l'État doit faire preuve d'énormément de prudence lorsqu'elle émet des considérations à propos d'une personne physique.

En l'espèce, je relève également que la Sûreté de l'État s'est directement adressée à une autorité administrative relevant de la compétence de la Communauté française.

²² Voir notamment BEL, B., « Infiltration de mouvements religieux dans le milieu naissance – périnatalité » <http://pro.wanadoo.fr/tansen/bioethics/society/religion/omaep/infiltration.htm>

²³ Comité permanent R, « Les droits d'accès du particulier à son dossier individuel auprès d'un service de renseignement », Rapport d'activités 1997, Bruxelles, 1998 (pp. 54 à 78) www.comiteri.be

Or, à plusieurs reprises, j'ai signalé à l'Administrateur de la Sûreté de l'État qu'en tant que Ministre de tutelle de la Sûreté de l'État, il m'appartenait d'apprécier dans quelle mesure les informations qu'elle communiquait à propos de matières relevant de la compétence des entités fédérées, pouvaient être communiquées à celles-ci. Je constate que cette consigne n'a pas été respectée en l'espèce. Je ne peux que le déplorer.

Je transmets le rapport précité à l'Administrateur général afin qu'il puisse me communiquer ses commentaires. Je ne manquerai pas de vous informer des suites réservées à ma requête. »

Le présent rapport et ses conclusions ont ensuite donné lieu à un échange de courriers classifiés entre la ministre de la Justice, la Sûreté de l'État et le Comité permanent R.

De manière générale, l'administrateur général de la Sûreté de l'État justifie sa position et maintient l'analyse faite par son service dans cette affaire. Un membre de la Sûreté de l'État a laissé entendre que son service disposait d'autres éléments confortant cette analyse.

Le Comité permanent R a donc chargé son Service d'enquêtes de procéder à des devoirs d'enquêtes complémentaires auxquels l'administrateur général de la Sûreté de l'État s'est d'abord opposé en invoquant les articles 48 §2, alinéa 3 et 51 de la loi organique du contrôle des services de police et de renseignements.

Après intervention de Madame la ministre de la Justice, le Comité permanent R a reçu de nouveaux éléments d'information. Après les avoir examinés, le Comité en a conclu que ceux-ci ne permettraient toujours pas de confirmer l'activisme de madame X au sein du CABG après sa participation à la conférence de l'année 2000.

Le Comité permanent R a donc maintenu ses conclusions. La Sûreté de l'État maintient les siennes.

L'administrateur général a également manifesté son désaccord sur les recommandations du Comité tendant à ne pas laisser à la seule appréciation des services de renseignements l'opportunité de permettre ou de refuser l'accès à un dossier à une personne qui s'estime lésée par son contenu :

« Il convient de souligner, à ce propos, que les services de renseignement sont tenus à une obligation légale de protection de leurs sources humaines et des informations qu'elles communiquent. Or, les services de renseignement ne sont en mesure de respecter cette obligation que s'ils sont maîtres de l'accès à ces informations. Si une autorité distincte peut décider d'accorder l'accès aux informations des services de renseignement, ces derniers ne pourront plus garantir la sécurité des données protégées par l'article 18 de la loi organique des services de renseignement et de sécurité. D'autre part, il ne faut pas négliger l'existence d'une procédure donnant un accès indirect aux particuliers à l'égard des données qui les concernent. » (extrait d'une lettre du 7 décembre 2005)

CHAPITRE 4 PLAINTÉ D'UN SOUS-OFFICIER À L'ENCONTRE DU SGRS

En juin 2005, un sous-officier a déposé plainte contre le Service général du Renseignement et de la Sécurité lui imputant la responsabilité d'une mutation qu'il estimait arbitraire.

L'enquête menée par le Service d'enquêtes a fait apparaître qu'un différend a opposé le plaignant à son chef hiérarchique, attaché militaire belge à l'étranger, et à l'aide de camp de ce dernier. Des questions de service sont à l'origine de ce différend. A cette occasion, le plaignant a formulé des griefs à l'encontre de l'attaché militaire et de son aide de camp, leur imputant des faits constitutifs d'une infraction pénale.

Une mission d'enquête interne fut mise sur pied au sein du SGRS afin d'examiner les faits sus-dits. L'inspection générale et le service de médiation du SPF Défense nationale ainsi que l'auditorat militaire général furent aussi saisis de ces faits.

Ni l'auditorat militaire général, ni la mission d'enquête du SGRS n'ont pu réunir le moindre indice étayant les allégations du plaignant à charge de l'attaché militaire et de son aide de camp. L'inspection générale et de médiation du ministère de la défense nationale a confirmé le classement sans suite du dossier.

Le Service d'enquêtes R a examiné la manière dont le SGRS avait traité les accusations formulées par le plaignant. Il en ressort que l'enquête du SGRS a été menée avec diligence et impartialité.

Le rappel de l'intéressé de son poste à l'étranger vers Bruxelles fut une mesure d'ordre prise à la suite des accusations qu'il a portées à l'égard de ses supérieurs. Cette mesure ressortait de la compétence du SGRS, elle ne fut ni arbitraire ni injustifiée.

En conséquence de quoi, le Comité permanent R a décidé de ne pas donner d'autre suite à la plainte.

TITRE 2

LES ENQUETES DE CONTROLE

D. LES ENQUETES EN COURS

Quelques enquêtes de contrôle ont été ouvertes ou se sont poursuivies au cours de l'année 2005 sans être encore clôturées. Le Comité permanent R fait le point sur ces enquêtes toujours en cours.

CHAPITRE 1 LE RÔLE DES SERVICES DE RENSEIGNEMENT EN MATIÈRE DE LUTTE CONTRE LA PROLIFÉRATION

Le 17 mars 2004, Madame la députée fédérale MURIEL GERKENS a demandé au Comité permanent R de vérifier la manière dont nos services de renseignement s'occupaient du problème de la prolifération nucléaire.

Le 24 juin 2004, le Comité permanent R a décidé de reprendre une enquête démarrée en 2001 mais dont l'exécution avait dû être postposée compte tenu d'autres enquêtes urgentes en cours.

Étant donné que la loi organique des services de renseignement inclut le trafic « *de systèmes d'armements non conventionnels ou très avancés* » dans les missions de la Sûreté de l'État d'une part, que cette mission vise notamment « *le développement de programmes d'armement nucléaire, chimique et biologique, les systèmes de transmission qui s'y rapportent, ainsi que les personnes, structures ou pays qui y sont impliqués* » d'autre part, le Comité permanent R a décidé d'élargir cette enquête sur le rôle des services de renseignement en matière « *de moyens biologiques et chimiques dans les actions terroristes* » et de la rebaptiser « *enquête de contrôle sur le rôle des services de renseignement en matière de lutte contre la prolifération d'armements non conventionnels ou très avancés* ».

Vu ses compétences légales, le Comité permanent R ne peut examiner la problématique de la prolifération elle-même. Ses enquêtes portent donc sur la contribution qu'apportent ou que peuvent apporter les services de renseignement belges à cette matière. Le Comité permanent R espérait pouvoir déposer son rapport général dans le courant de l'année 2005. Toutefois, au cours de cette même année, le Comité a dû ouvrir deux enquêtes ponctuelles en rapport avec le sujet d'ordre général de la présente enquête. Il s'agit :

- de l'enquête spécifique sur la manière dont la firme EPSI avait éventuellement été suivie par les services de renseignement dans le cadre de la lutte contre la prolifération (3 mai 2005).
- de l'enquête sur la manière dont une SNC-Lavalin a éventuellement été suivie par la Sûreté de l'État dans le cadre de la lutte contre la prolifération.

Cette enquête est toujours en cours. Les éléments recueillis lors de ces deux enquêtes seront comparés et alimenteront ainsi les conclusions plus générales qui restent à tirer sur rôle des services de renseignement en matière de lutte contre la prolifération d'armements non conventionnels ou très avancés. Néanmoins, les constatations effectuées lors de l'enquête sur l'affaire EPSI ont déjà permis au Comité permanent R de formuler les recommandations exposées dans le titre 2 les enquêtes de contrôle, chapitre 1 l'enquête de contrôle sur la manière dont la firme Epsi a éventuellement été suivie par les services de renseignement dans le cadre de la lutte contre la prolifération.

CHAPITRE 2**DÉPLACEMENTS DE PERSONNES VERS DES ZONES SENSIBLES**

Faisant suite au courrier reçu de la Présidente du Sénat le 11 août 2005, le Comité permanent R a ouvert le 31 août 2005 une enquête de contrôle sur les suivis accordés par les services de renseignement aux déplacements de personnes passant par la Belgique et/ou quittant le pays pour se rendre dans certaines zones sensibles (Irak, Iran, Pakistan, Afghanistan, etc.).

CHAPITRE 3**LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE : ENQUÊTE SUR LE SUIVI ÉVENTUEL D'UNE FIRME BELGE**

Il s'agit d'une enquête sur le suivi éventuel d'une firme belge de haute technologie par les services de renseignement.

Au cours du deuxième semestre de l'année 2005, la presse a indiqué qu'une firme belge de haute technologie avait vendu sa filiale à un groupe de Défense britannique lui-même contrôlé par un puissant groupe américain.

Cette firme étant titulaire d'une habilitation de sécurité industrielle auprès du ministère de la Défense nationale, il a semblé intéressant d'examiner si celle-ci avait déjà attiré l'attention de nos services de renseignement, soit la Sûreté de l'État dans le cadre de la protection du potentiel scientifique et économique, soit le SGRS dans le cadre de la sécurité militaire.

CHAPITRE 4 :**SUIVI DE L'ENQUÊTE SUR L'ISLAMISME RADICAL**

Dans son rapport d'activités de l'année 2001, le Comité permanent R a fait rapport sur la manière dont les services de renseignement s'intéressaient aux activités islamistes extrémistes et terroristes. Ce rapport était essentiellement consacré au suivi de ce sujet par la Sûreté de l'État. Il y était toutefois annoncé qu'une seconde enquête s'intéresserait aussi à l'action du SGRS en cette matière.

Compte tenu d'enquêtes ponctuelles menées en 2002, 2003 et 2004 sur le suivi d'activités islamistes par les services de renseignement, le Comité n'a pas encore été en mesure de poursuivre son enquête générale auprès du SGRS.

Le Comité permanent R a néanmoins décidé le 4 novembre 2005 de reprendre cette enquête générale sur le suivi de l'islamisme radical tant à la Sûreté de l'État qu'au SGRS.

CHAPITRE 5**LA MANIÈRE DONT LE SGRS ORGANISE LA CONSERVATION, LA GESTION ET L'EXPLOITATION (INFORMATIQUE) DES DONNÉES À CARACTÈRE PERSONNEL QU'IL RECUEILLE**

Faisant suite à l'incident de sécurité précité, le Comité permanent R a aussi ouvert le 4 novembre 2005 une enquête de contrôle sur la manière dont le SGRS organisait la conservation, la gestion et l'exploitation (informatique) des données à caractère personnel qu'il recueille.

TITRE 3

LE CONTRÔLE DES INTERCEPTIONS DE SECURITE

Une forme particulière d'enquête de contrôle est celle qui porte sur les interceptions de sécurité. En 2005, le Comité Permanent R a organisé des réunions de travail avec le Service Général du Renseignement et de la Sécurité ayant pour but de vérifier quelles mesures concrètes avaient été adoptées par ce service aux fins de réaliser les interceptions de sécurité légalement permises. (cf. art. 44 et suivants de la loi organique des services de renseignement et de sécurité). Des contrôles ont également été effectués sur place.

En raison de la sensibilité de cette matière, le Comité Permanent R ne peut entrer dans les détails. Néanmoins, le Comité Permanent suit avec une attention particulière le respect des prescrits légaux en la matière et formulera ultérieurement des recommandations.

TITRE 4
LES ENQUETES JUDICIAIRES

L'article 40, alinéa 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement prévoit que d'initiative ou sur réquisition du Procureur du Roi ou du Juge d'instruction compétent, le Service d'enquêtes du Comité permanent R effectue, en concurrence avec les autres officiers et agents de police judiciaire et même avec un droit de prévention sur ceux-ci, les enquêtes sur les crimes et délits à charge des membres des services de renseignements.

Au cours de l'année 2005, le Service d'enquêtes du Comité permanent R a mené deux enquêtes judiciaires, la première sur l'initiative du Parquet de Bruxelles, la seconde sur l'initiative du Parquet fédéral :

- une enquête a été menée sur un incident de tir survenu en novembre 2004 dans les locaux de la Sûreté de l'État. Au cours de cette enquête, un membre de ce service a été privé de sa liberté et mis à la disposition de la Justice.
- une enquête entamée en septembre 2004 a également été poursuivie sur un incident de sécurité survenu au SGRS. Comme le Comité permanent menait également une enquête de contrôle sur les mêmes faits, celui-ci a fait application de l'article 69 §§ 1 à 5 (section 2) de son règlement d'ordre intérieur. Cet article dispose ce qui suit :

« Lorsqu'à l'occasion d'une enquête de contrôle, un membre du Service d'enquêtes constate un crime ou un délit commis par un membre des services de renseignements, l'instruction judiciaire relative à ces faits prend la priorité sur l'enquête de contrôle.

L'enquête de contrôle se poursuit le cas échéant, en se limitant aux éléments qui sont nécessaires à l'accomplissement des missions du Comité R. Le chef du Service d'enquêtes en avise alors le magistrat responsable de l'enquête judiciaire. »

Par ailleurs, le Parquet fédéral a saisi le Service d'enquêtes du Comité permanent R de deux infractions de roulage commises par des membres des services de renseignement alors qu'ils étaient en mission au volant de véhicules de service.

Au total, le Service d'enquêtes a rédigé 25 procès-verbaux au cours de l'année 2005.

TITRE 5

LES QUESTIONS POSÉES AUX SERVICES DE RENSEIGNEMENT

Outre les enquêtes qu'il mène à la demande du Parlement, des ministres compétents ou de sa propre initiative, le Comité permanent R a estimé que ses compétences légales l'autorisaient à questionner régulièrement les responsables des services de renseignement sur certains sujets traités 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. Cette méthode permet au Comité permanent R de se tenir sommairement informé sur les priorités du moment, sur la manière dont les services de renseignement traitent une matière déterminée ou donnent suite aux conclusions et recommandations formulées dans de précédents rapports.

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, attestations et avis de sécurité a été attribué à certaines réponses données au Comité permanent R, ce qui ne lui permet donc pas d'en donner connaissance intégrale dans un rapport d'activités destiné à être publié.

Le Comité permanent 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 des années 2003, 2004 et 2005.

CHAPITRE 1	L'APPLICATION DES STATUTS SYNDICAUX DES MEMBRES DU PERSONNEL DU SGRS
-------------------	---

Dans son rapport d'activités de l'année 1997¹, le Comité permanent R avait examiné les statuts syndicaux applicables aux différentes catégories de personnel (militaires, civils, gendarmes) actives dans ce service. Le Comité avait souligné l'absence de statut syndical pour les agents des services extérieurs de la Sûreté de l'État. Le Comité avait recommandé d'envisager la création d'un tel statut pour ces agents.

Lors des discussions menées au Parlement fédéral sur la création d'un statut syndical propre aux agents des services extérieurs de la Sûreté de l'État, le Comité permanent R a ouvert une enquête de contrôle sur l'application des statuts syndicaux au sein du SGRS. Le Comité permanent R estimait utile de procéder de la sorte en vue de formuler des recommandations éventuelles pour le futur statut syndical des membres de la Sûreté de l'État.

Le Parlement ayant entre-temps adopté la loi du 17 mars 2004 organisant les relations entre les autorités publiques et les organisations syndicales du personnel des services extérieurs de la Sûreté de l'État, le Comité permanent R n'a pas poursuivi plus avant son enquête. Il n'a formulé aucune recommandation en la matière.

Les premières constatations effectuées donnent les indications suivantes :

Selon le statut auquel il appartient, le membre d'un service de renseignement est soumis, soit au statut syndical général de la fonction publique (agents administratifs et agents civils du Service de sécurité militaire), soit au statut syndical spécifique des militaires.

Les relations entre les autorités publiques et les syndicats du personnel militaire ont gagné en importance au sein d'une armée professionnelle. En vertu de ce statut, les militaires sont libres de s'affilier, soit à une organisation syndicale professionnelle de militaires, soit à une organisation syndicale affiliée à une organisation syndicale représentée au Conseil national du travail.

Les procédures de négociation et de concertation, les mesures de contrôle de la représentativité, l'agrément et les prérogatives des organisations syndicales de militaires sont comparables à celles prévues par la loi du 19 décembre 1974.

Six associations et ASBL sont actuellement agréées en tant qu'organisations syndicales du personnel militaire. La représentativité a été accordée aux trois syndicats qui sont représentés au Conseil national du travail ainsi qu'au plus grand syndicat professionnel de l'armée².

Aucun recensement des affiliés aux syndicats n'est tenu par le SGRS. La hiérarchie de ce service soutient que le nombre d'agents syndiqués parmi le personnel civil est assez élevé, surtout au sein du Service de sécurité militaire où le taux d'affiliation à un syndicat serait supérieur à 80 %.

¹ Comité permanent R, *Rapport d'activités 1997*, Bruxelles, 1998 (www.comiteri.be).

² Voir Chambre des Représentants: questions parlementaires n° 136 de M. Lahaye (1^{er} juillet 1996) et n°167 de Mme Van den Poel - Welkenhuysen (20 septembre 1996).

Par contre, le nombre d'affiliés parmi les agents contractuels serait nettement moins élevé. Ces agents sont en général plus jeunes que les agents nommés et ils se sentent sans doute moins liés au Service Public traditionnel dont les syndicats sont une composante historique. De manière générale, on retient que les « anciens » sont davantage syndiqués que les jeunes.

Les organisations syndicales agréées ont le droit d'exercer leurs prérogatives dans les locaux du SGRS, notamment d'y tenir des réunions, même pendant les heures de service. Elles ont le droit d'y percevoir les cotisations des membres, d'y afficher des avis moyennant visa donné par la hiérarchie. Le visa ne peut être refusé que si l'avis porte atteinte à la dignité des personnes, des institutions ou des autres organisations syndicales, ou s'il contient des faits auxquels l'autorité a préalablement attribué un caractère secret.

Le Comité de négociation compétent pour le personnel civil du SGRS est le Comité du secteur XIV, compétent pour tout le personnel de la Défense nationale. Sauf dans quelques cas d'urgence, ce Comité a été consulté pour chaque Arrêté royal et pour chaque arrêté ministériel touchant au statut des agents du Service de sécurité militaire.

Les syndicats du personnel civil de la Défense nationale réclament l'application de la révision générale des barèmes décidée au début de l'année 1994.

L'Arrêté royal du 28 septembre 1984 précise cependant que les procédures de négociation et de concertation ne sont pas requises lorsque la mesure à prendre concerne l'organisation de la sécurité ou de la défense nationale. Dans ce cas, l'autorité est néanmoins tenue de motiver sa décision de ne pas procéder à la négociation ou à la concertation (article 5).

Il existe une liste de délégués syndicaux pour tout le département. Les délégués syndicaux jouissent de congés syndicaux, accordés sur base d'une convocation datée et signée par l'organisation syndicale à laquelle ils appartiennent.

Les délégués syndicaux sont tenus à la discrétion quant aux faits et documents à caractère confidentiel. Ils ne peuvent pas divulguer des faits ou des documents auxquels l'autorité a préalablement attribué un caractère secret (article 85 de l'A.R. du 28 septembre 1984). La violation de cette règle par un délégué syndical peut entraîner le retrait de son agrément en tant que tel et l'interdiction pour lui d'en encore exercer ses prérogatives.

De l'avis général, les délégués syndicaux n'éprouvent aucune difficulté particulière à exercer leurs fonctions au SGRS. Selon la hiérarchie du service, les délégués syndicaux adoptent un comportement particulièrement raisonnable dans leur fonction. Un climat de confiance existe entre le commandement du service et le personnel, ce qui permet un dialogue permanent et institutionnalisé.

L'action des syndicats du personnel civil du SGRS concerne le statut et les revendications générales des agents des Services Publics. Les syndicats restent attentifs au bien-être de leurs affiliés et au respect de leurs droits. Dans ces conditions, les syndicats n'interviennent généralement pas dans les questions spécifiques au SGRS, sauf en ce qui concerne les actions globales destinées à offrir un soutien dans les efforts fournis en vue d'obtenir un nouveau statut.

Ainsi, une action syndicale commune aux trois organisations agréées a eu lieu au cours de l'année 2002 en vue d'accélérer l'évolution du dossier relatif au changement du statut du personnel statutaire civil du Service de sécurité militaire toujours régi par l'arrêté royal du 20 août 1969. Les affiliés restent particulièrement sensibles à cette évolution.

Toute forme de grève est interdite aux militaires; elle ne l'est pas en principe aux agents civils. Selon la hiérarchie du SGRS, aucun moyen de pression n'a été utilisé jusqu'à présent. Pas plus que pour le personnel militaire, il n'y a jamais eu la moindre grève au SGRS. Ce fait est la conséquence du dialogue et du climat de confiance existant entre la hiérarchie et les délégués syndicaux.

En conclusions, de l'avis général, les relations entre les syndicats et la hiérarchie du SGRS paraissent bonnes tant en ce qui concerne le personnel civil que le personnel militaire. Aucun délégué n'est empêché d'agir, pas plus qu'il n'est empêché de recruter d'autres membres du personnel. Les délégués n'ont jamais nui à la bonne marche du service.

CHAPITRE 2	L'APPLICATION DE L'ARTICLE 14 DE LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ - ACCORDS ÉVENTUELLEMENT PASSÉS ENTRE LA SÛRETÉ DE L'ÉTAT ET DES SERVICES PUBLICS
-------------------	---

L'article 14 de la loi organique des services de renseignement et de sécurité prévoit que :
« dans le respect de la loi et sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent communiquer d'initiative au Service de Renseignement et de Sécurité concerné les informations utiles à l'exécution de ses missions.

De même, à la requête d'un Service de Renseignement et de Sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent, dans le respect de la loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, communiquer au Service de Renseignement et de Sécurité concerné les informations utiles à l'exécution de ses missions. »

Le 22 juin 2004, le Comité permanent R a demandé aux services de renseignement si - faisant application des dispositions précitées - ceux-ci avaient conclu des accords avec des administrations publiques fédérales, régionales, communautaires ou autres. Dans l'affirmative, le Comité permanent R a demandé de pouvoir obtenir une copie de ces accords. Dans la négative, le Comité permanent R voulait en connaître les raisons. La Sûreté de l'État et le SGRS ont-ils déjà tenté de conclure de tels accords avec un service public ? Avec qui et sur quels sujets ? Pour quelles raisons de tels accords n'ont-ils jamais été conclu ?

Le 6 juillet 2004 le Comité permanent R a reçu la réponse de la Sûreté de l'Etat. Il ressort de la réponse donnée par l'administrateur-général DASSEN qu'un certain nombre de textes étaient déjà d'application pendant que des négociations étaient en cours concernant d'autres protocoles. On a estimé utile de conclure des accords complémentaires étant donné que de tels accords de coopération présentaient divers avantages pour toutes les parties concernées. Ainsi des négociations ont e.a. été entamées avec la police fédérale, le commissariat général aux réfugiés et apatrides, l'Office des étrangers, le SPF Affaires économiques et les établissements pénitentiaires.

En raison de l'importance que le Comité permanent R accorde aux accords de coopération, il s'est intéressé à l'état d'avancement des travaux.

Le 18 avril 2006 la Sûreté de l'Etat a fait savoir que les protocoles d'accord dont question ci-dessus étaient toujours en phase de négociation pour différentes raisons qui lui sont étrangères.

CHAPITRE 3	LA CONTRIBUTION APPORTÉE PAR LES SERVICES DE RENSEIGNEMENT À LA CONFECTION DES LISTES TERRORISMES
-------------------	--

En vue de préparer la journée d'étude du Sénat relative à l'établissement de listes de personnes et d'organisations terroristes à l'encontre desquelles des mesures de gel de leurs avoirs financiers dans le cadre du droit international doivent être prises, les soi-disant 'listes terroristes'³, le Comité permanent R a adressé les questions suivantes aux services de renseignement le 16 février 2005 :

- a) Votre service participe-t-il de manière directe ou indirecte à l'élaboration de ces listes de personnes et d'organisations terroristes ?
- b) Si oui, selon quelle(s) procédure(s) ? Quels autres services, autorités et instances participent à cette élaboration ?
- c) Votre service utilise-t-il ces listes dans l'exercice de ses missions ?
- d) Si oui, de quelle manière ?
- e) Votre service se réfère-t-il notamment à ces listes pour déterminer les sujets qu'il suit ?
- f) Votre service a-t-il déjà été consulté par une autorité belge ou étrangère afin de communiquer des informations utiles à la confection de l'une des ces listes.

Le SGRS a transmis ses réponses le 8 avril 2005, la Sûreté de l'État a répondu à son tour le 11 octobre 2005. Cette dernière a invoqué une charge de travail importante pour justifier le long délai qu'elle a mis à répondre. Ci-après se trouve un résumé succinct de la correspondance tant du SGRS que de la Sûreté de l'État

La réponse du SGRS

- a) Aucune division du SGRS n'a jamais participé de quelque manière que ce soit à l'élaboration ou au contrôle de ces listes de personnes et d'organisations terroristes.
- b) Question sans objet vu la réponse négative à la question précédente.
- c) Le SGRS n'utilise pas les listes terroristes dans l'exercice de ses missions.
- d) Certaines divisions du SGRS se tiennent au courant des listes élaborées par les Nations Unies, l'Union européenne et les États-Unis d'Amérique, les analysent et les comparent l'une à l'autre.
- e) Le SGRS effectue ses propres analyses. Ce service s'intéresse principalement au terrorisme islamiste international. Les sujets qu'il suit correspondent de fait à certaines entités qui figurent sur ces listes. Le SGRS s'y réfère, si nécessaire, pour ajuster le niveau de priorité de recherche à accorder à certaines organisations, niveau qui figure dans le Plan Directeur du Renseignement de Sécurité (PDRS).

³ Voir Titre 6 Etudes et activités, chapitre 3 Listes terroristes.

- f) Le SGRS n'a jamais été consulté par une autorité belge ou étrangère afin de communiquer des informations utiles à la confection de l'une des ces listes.

Le SGRS commente ses réponses de la manière suivante : « *La difficulté majeure (...) est de prouver que les organisations pressenties sont bien des organisations terroristes, de par leurs actes, de par des jugements qui ont entériné cette qualification. Les services de renseignement (...) ne peuvent généralement y apporter que des 'suspensions' ou des 'intimes convictions' ayant trait à des actes ou des comportements desdites organisations ou des gens qui les composent, commis sur le territoire national. Les actes de propagande, de collectes de fonds, par exemple, sur le territoire belge, sont-ils à considérer comme des actes terroristes ?* »

La réponse de la Sûreté de l'État

- a) Tous les services concernés, y compris la Sûreté de l'État, la CTIF et le Trésor, peuvent apporter leur contribution à la liste belge et même prendre l'initiative de proposer des adaptations.
Tous les services concernés, (Sûreté de l'État, GIA, SGRS, Police fédérale), peuvent être consultés sur la mise à jour de la liste européenne.

- b) La liste belge est élaborée et régulièrement mise à jour suivant les adaptations apportées à la liste des Nations Unies.

La position belge quant à la liste européenne est établie par le Comité des représentants permanents (CoRePer) auprès de l'Union européenne. Ce Comité organise les réunions de coordination des services concernés au niveau belge et fait rapport aux instances européennes.

- c) La Sûreté de l'État n'utilise pas systématiquement les listes terroristes de l'Union européenne ou des États-Unis.
- d) Ces listes peuvent néanmoins servir à étoffer des notes adressées aux autorités.
- e) Les listes reflètent souvent le travail de recherche des services de renseignement et en sont donc le résultat. Elles peuvent avoir une répercussion a posteriori sur les activités de la Sûreté de l'État.

La Sûreté de l'État indique aussi que « *faire figurer une personne ou une entité sur une telle liste, particulièrement pour ce qui concerne le volet belge, est toujours la suite de soupçons d'une implication possible dans des activités terroristes (...)* qui peuvent être apportés par la Sûreté de l'État elle-même.

Le Comité permanent R reviendra sur la problématique juridique de l'établissement de ces 'listes terroristes'.

CHAPITRE 4	LA	DIFFUSION	D'IMAGES	SATELLITAIRES	SUR
		L'INTERNET			

Le Comité permanent R s'est toujours intéressé à la problématique de l'exploitation des sources ouvertes (OSINT) dans le monde du renseignement. D'ailleurs une énorme quantité d'informations devient chaque jour de plus en plus accessible au public via l'Internet.

Ainsi par exemple, le programme *Google Earth* permet de télécharger de façon gratuite des images satellitaires de grande précision et de contempler les détails urbanistiques de certaines villes notamment américaines et européennes. Plusieurs installations – dont certaines se révèlent critiques – (établissements militaires, centrales nucléaires, barrages hydrauliques) – seraient trop facilement visualisables et, par conséquent, gravement exposées à des risques de sécurité.

Ainsi, *Google Earth* offrirait pour chaque point du globe observé une série de coordonnées de géoréférencement GPS. Selon certains observateurs de telles données pourraient être utilisées à mauvais escient, notamment à des fins de frappes ou d'attaques terroristes. Il semblerait que certaines autorités seraient déjà intervenues auprès des dirigeants de la firme *Google* pour leur demander de dégrader ou de retirer les images de certaines installations sensibles.

Le 8 septembre 2005, le Comité permanent R a questionné les responsables de la Sûreté de l'État et du SGRS sur ce sujet.

« Certains articles parus récemment dans la presse indiquent que le nouveau service en ligne proposé par la firme Google, à savoir le logiciel Google Earth, aurait éveillé les craintes de certains services de renseignement. Le Comité permanent R voudrait savoir si votre service se préoccupe des images diffusées par Google Earth et s'il a déjà alerté les autorités belges à propos de risques éventuels pour notre pays ».

La réponse de la Sûreté de l'État

La réponse de la Sûreté de l'État est parvenue au Comité permanent R le 26 septembre 2005.

« Description »

Google Inc. a été fondée en 1998 par Larry Page et Sergey Brin. L'entreprise a développé le moteur de recherche sur Internet Google. Google est désormais devenu le moteur de recherche sur Internet le plus populaire, mais aussi le plus important avec un accès à 3 milliards de pages Web. Le nom « Google » a été dérivé du terme « googol » qui correspond au nombre 10^{100} .

Ce terme reflète l'objectif de Google, à savoir organiser et rendre accessible une quantité extrêmement importante d'informations sur Internet. Les revenus proviennent essentiellement des possibilités de publicité ciblée offertes aux clients.

A l'origine, le moteur de recherche sur Internet était le seul service de Google Inc. Par la suite, d'autres services s'y sont ajoutés, tels que la messagerie instantanée (SMS), le chat (bavardage), Gmail (service de messagerie électronique), etc. Google Maps et Google Earth constituent les derniers services ajoutés.

Google Maps offre une technologie de cartographie via Internet comparable aux planificateurs d'itinéraires connus. Google Maps peut calculer des itinéraires et indiquer des informations commerciales (par exemple : les hôtels à proximité d'un endroit déterminé). En outre, il peut également reproduire des images satellitaires en superposant éventuellement des données de cartes ordinaires. La résolution des images satellites est très grande pour certaines zones : il est même possible de voir les véhicules sur la route.

Google Earth est un programme indépendant qui offre plus de fonctionnalités que Google Maps. Google Earth combine des images satellitaires, la cartographie et le moteur de recherche Google dans un environnement graphique. Ainsi, il est par exemple possible d'effectuer un voyage visuel depuis l'espace vers un endroit de votre choix sur la terre. Pour un certain nombre de villes, il est également possible de visualiser une représentation en 3D des bâtiments et de naviguer dans les rues.

Trois versions de Google Earth sont disponibles. La première version est gratuite et offre les fonctionnalités de base de Google Earth. Google Earth Plus (prix : 20 \$) permet en outre la prise en charge d'un GPS, l'importation de tableurs et une résolution d'impression plus importante.

Pour les utilisateurs professionnels, Google propose également Google Earth Pro au prix de 400 \$. Cette version peut être intégrée à d'autres logiciels (par exemple : un logiciel de présentation de banques de données immobilières). Cette version est par exemple destinée aux agences immobilières, aux bureaux d'architectes, aux pouvoirs publics...

Évaluation

La technologie à la base de Google Maps et de Google Earth n'est pas nouvelle et n'est pas non plus unique (p.ex. Keyhole). Ce type de service était déjà proposé par d'autres auparavant (de façon publique sur Internet et de façon privée). Via le planificateur d'itinéraires en ligne Mappy (www.mappy.be), il était déjà possible de demander par exemple une photo aérienne ou satellitaire détaillée de l'Avenue du Roi Albert II avec une superposition de données de carte. Par contre, ce qui est nouveau, c'est la notoriété de l'offrant, l'offre étendue de documents et le niveau de détail de certaines photos. L'incorporation de la fonctionnalité GPS est également une nouveauté à cette échelle.

L'offre de photos satellites couvre pratiquement toute la surface de la Terre. Cependant, l'offre d'images de (très) haute résolution est encore relativement limitée. Pratiquement toute l'Amérique du Nord est disponible en haute résolution. Certaines villes américaines peuvent même être visualisées sous forme de présentation graphique 3D ! Pour le moment, il y a beaucoup moins d'images haute résolution disponibles pour les autres continents. Google affirme néanmoins ajouter continuellement des images haute résolution à sa base de données. Un certain nombre de grandes villes d'Europe occidentale (Londres par exemple) est cependant déjà disponible en haute résolution. Par contre, il y a peu d'images détaillées d'Afrique, d'Asie et d'Amérique du Sud.

Il n'y a également que peu d'images détaillées de la Belgique pour le moment.

Google propose des images haute résolution pour quatre régions seulement. Ces régions ne comprennent aucun grand centre urbain. Les installations nucléaires de Doel et l'aéroport de Zaventem n'y figurent pas non plus. L'aéroport de Charleroi et l'aéroport militaire de Kleine Brogel ou Bierset sont par contre visibles de façon détaillée.

Le danger de la disponibilité de telles images détaillées d'installations sensibles réside dans le fait que ces images peuvent éventuellement être utilisées pour la préparation d'attaques terroristes. La combinaison avec la fonctionnalité GPS peut également être utile pour des terroristes (pour le guidage d'un avion ou d'un missile par exemple).

Il est également possible que la sécurité des installations militaires soit de ce fait compromise. La question est cependant de savoir quand la base de données Google comprendra plus d'images haute résolution de la Belgique. En outre, il ne faut pas oublier que ces informations peuvent vraisemblablement être aussi obtenues par d'autres canaux.

Google Inc. se rend également compte que cette technologie peut être utile pour le secteur de la sécurité, comme en témoigne la mention de « Homeland Security » et de « Defence/Intelligence community » en tant que clients potentiels pour la version professionnelle de Google Earth. Le site Web de Google ne permet cependant pas d'établir si les autorités américaines utilisent aussi réellement ce logiciel.

Conclusion

(...)

L'évolution du secteur informatique est extrêmement rapide. En outre, de plus en plus d'informations du secteur privé se retrouveront vraisemblablement sur Internet (ou sur d'autres nouveaux médias) à l'avenir. Il se peut que cela concerne également des informations sensibles pour la sécurité.

Cette diffusion rapide et anonyme sur Internet d'une quantité d'informations extrêmement importante rend particulièrement difficile tout suivi approfondi permanent.

Quoi qu'il en soit, la Sûreté de l'État est intéressée par ces évolutions et les suit dès lors dans la mesure du possible. En ce sens, nous pouvons par exemple faire référence à notre note concernant les entreprises SEVESO.

Le ministère de l'Intérieur a publié, sur son site Web, un relevé par entreprise SEVESO des substances chimiques dangereuses qui y sont présentes. La Sûreté de l'État a attiré l'attention de l'autorité en question sur le risque que représente un tel inventaire pour la sécurité, à la suite de quoi le site Web a été adapté et les informations sensibles, supprimées.

En outre, dans le cadre de sa politique du personnel, la Sûreté de l'État souhaite, à l'avenir, se consacrer attentivement à l'approche opérationnelle du 'phénomène Internet'. Pour cela, il convient toutefois de mettre en œuvre la réorientation prévue de la section informatique actuelle, qui exerce plutôt une fonction de support logistique pour le moment.

La Sûreté de l'État constate qu'Internet met une quantité énorme d'informations à la disposition d'un public immense. Il y a donc toujours un risque que certaines personnes ou organisations puissent abuser de ces moyens et informations mis à disposition. Une analyse générale des risques du phénomène requiert énormément de temps et de moyens.

La Sûreté de l'État se concentre plutôt sur ces personnes et organisations qui pourraient éventuellement abuser du système et examine le système en se demandant dans quelle mesure il est ou peut être utilisé comme modus operandi par ces personnes.

Pour le moment, il n'y a aucune indication ou même aucun début d'indication que le système mis à disposition par Google Earth constitue un modus operandi potentiel pour des terroristes ou des groupements radicaux. Il importe à cet égard de souligner la disponibilité générale de telles cartes et la résolution peu élevée de ces cartes proposées par Google Earth. »

La réponse du SGRS

La réponse du SGRS est parvenue au Comité permanent R le 17 novembre 2005. Ci-après quelques passages importants :

« Dans votre lettre du 8 septembre, vous faisiez part de vos inquiétudes quant aux possibilités offertes par le logiciel Google Earth en matière d'imagerie satellitaire. Le Centre belge d'interprétation d'images satellites (...) s'est penché sur ce sujet dès qu'il en a eu connaissance. Les conclusions sont les suivantes :

Toute personne qui souhaite acquérir une image satellite de n'importe quel point du globe peut s'adresser auprès de nombreux fournisseurs d'images satellites commerciales. Ces fournisseurs sont principalement américains, européens ou asiatiques. Cette possibilité existe depuis de nombreuses années, sans restriction et permet d'obtenir des images relativement récentes, de bonne qualité, moyennant le paiement d'un prix d'achat conséquent. Google Earth ne propose en fait qu'un recensement de quelques photos d'archives, fournies par un fournisseur américain important (Digital Globe).

Les produits proposés par Google Earth ne sont que des photos digitales, sans grande précision géographique, qui ne possèdent pas la richesse d'informations que l'on trouve dans les images satellites achetées directement chez les fournisseurs.

Disposer d'une image satellite est une chose, pouvoir l'analyser et en extraire un renseignement est un métier qui requiert une longue formation, beaucoup d'expertise et surtout des renseignements collatéraux obtenus par différents organes de collecte.

En résumé, nous pensons que la publication sur Google Earth de photos satellites digitales est une formidable opération commerciale, qui va susciter chez certains l'envie d'acheter des images chez le fournisseur (Digital Globe), faciliter l'accès à un type d'information qui existait déjà depuis de nombreuses années et « vulgariser » l'application possible de l'imagerie satellitaire. Mais, il n'y a là rien de neuf pour quiconque cherchait auparavant à obtenir ce type d'information. Le renseignement est autre chose qu'une belle photo digitale.

Ceci n'empêche pas le service de s'inquiéter que de telles images circulent librement sur l'Internet, surtout dans la version payante de GOOGLE EARTH (environ 400 EUR par an) qui fournit des images « récentes » (de quelques heures). »

CHAPITRE 5	LE FONCTIONNEMENT DE LA SECTION « LÉGISLATION EN MATIÈRE D'ARMES » DE LA SÛRETÉ DE L'ÉTAT
-------------------	--

Dans son rapport d'activités de l'année 2000⁴, le Comité permanent R a relevé que la section d'étude « législation armes » de la Sûreté de l'État exerçait deux types de compétences en matière d'exécution de la législation sur les armes à feu : une compétence décisionnelle et une compétence d'avis.

Ainsi, la Sûreté de l'État délivrait des autorisations de détention d'une arme à feu de défense et des permis de port d'arme de défense :

- aux étrangers qui n'ont pas de domicile en Belgique;
- aux belges qui sont domiciliés à l'étranger.

Les catégories d'étrangers n'ayant pas de domicile en Belgique pour lesquelles la Sûreté de l'État était compétente étaient :

- les personnes à statut diplomatique visés par l'article 1^{er} de l'arrêté royal du 30 octobre 1991 lesquels ne font pas l'objet d'une mention dans les registres communaux (pour des motifs de défense personnelle avec autorisations de détention et permis de port d'arme);
- les militaires étrangers en poste au SHAPE pour la pratique du tir sportif avec autorisation de détention ;
- les agents d'entreprises de gardiennage étrangères reconnues en Belgique et qui y exercent certaines activités professionnelles;
- les étrangers qui désirent acquérir en Belgique une arme soumise à autorisation soit en vue de son exportation, soit pour la laisser dans un club de tir sportif en vue de la pratique de cette activité avec autorisation de détention ;
- les étrangers non membres de l'Union Européenne qui désirent pratiquer le tir sportif et la chasse avec des armes soumises à autorisation en Belgique (autorisation de détention);
- les membres des services de protection étrangers officiels pour la protection de leurs personnalités nationales en visite en Belgique ;
- les tireurs sportifs étrangers (non membres d'un club de tir) et chasseurs étrangers qui participent exceptionnellement à une compétition de tir ou à une chasse ou qui transitent par la Belgique avec des armes qui nécessitent une autorisation (autorisation de détention temporaire d'une arme à feu de défense ou de guerre).

Le Comité permanent R s'est demandé si cette énumération de compétences en matière d'armes était toujours d'actualité.

Une question parlementaire posée au Sénat par monsieur NOREILDE a attiré l'attention du Comité permanent R. Cette question portait notamment sur l'usage et le port d'armes par

⁴ Comité permanent R, *Rapport d'activités 2000*, Bruxelles, 2001 (www.comiteri.be).

des agents de sécurité étrangers dans les bâtiments de l'aéroport et/ou sur le tarmac de Zaventem⁵.

Le Comité permanent R a donc interrogé la Sûreté de l'État à ce sujet. Il lui a demandé ce qu'il en était :

- des agents qui ont pour mission d'assurer la sécurité des vols de compagnies aériennes étrangères au départ ou à destination de la Belgique ;
- des douaniers américains présents sur le territoire national en application de l'accord « *Container Security Initiative* ».

La première réponse de la Sûreté de l'Etat

«L'énumération des compétences de la Sûreté de l'État, telles que contenues dans votre lettre citée en référence est toujours d'actualité et concerne les étrangers qui n'ont pas de domicile en Belgique et les Belges qui sont domiciliés (plutôt que résident) à l'étranger.

Veuillez trouver ci-après un aperçu des différentes catégories concernées, ainsi que le nombre d'autorisations délivrées en 2005.

DEMANDES AUX NOMS DE(S)	AUTORISATION	N°
<i>Personnes à statut diplomatique, lesquelles ne font pas l'objet d'une mention dans les registres communaux (pour des motifs de défense personnelle ou tir sportif)</i>	<i>Autorisation de détention (Modèle 4)</i>	23
	<i>Permis de port (Modèle 5)</i>	13
Ambassades, Représentations...	<i>Autorisation de détention (Modèle 4)</i>	6
Agents d'entreprises de gardiennage étrangères reconnues en Belgique et qui y exercent certaines activités professionnelles	<i>Depuis 2002 aucune demande n'a été reçue</i>	0
Chauffeurs du Gouvernement Luxembourgeois dans le cadre de leurs activités pour ce Gouvernement	<i>Depuis 2002 aucune demande n'a été reçue</i>	0
Militaires étrangers en poste au SHAPE pour la pratique du tir sportif	<i>Autorisations de détention (modèle 4)</i>	67

⁵ Questions & Réponses Sénat – 5 juillet 2005 (n° 3-44) et 30 août 2005 (n° 3-48) Questions n° 3-2736 et 3-2737 de monsieur Noreilde du 24 mai 2005.

DEMANDES AUX NOMS DE(S)	AUTORISATION	N°
Personnes domiciliées à l'étranger qui désirent acquérir en Belgique une arme soumise à autorisation soit en vue de son exportation, soit pour la laisser dans un club de tir ou leur résidence en Belgique, en vue de pratique de cette activité :	Autorisations de détention (modèle 4)	7
Personnes domiciliées à l'étranger dans le but de pouvoir participer au tir parcours (sur base de leur Carte européenne ou Modèle 4)	Permis de port (modèle 5)	4
Étrangers non membres de l'UE qui désirent pratiquer le tir sportif, tir de parcours ou la chasse avec des armes soumises à autorisation	Autorisations temporaires de détention et de port	9
Membre des services de protection étrangers officiels pour la protection de leurs V.I.P. nationales en visite en Belgique	Autorisations temporaires détention et de port	2400
Tireurs sportifs , membres de l'U.E. (en possession d'une Carte européenne d'armes à feu), qui participent occasionnellement à une compétition de tir de parcours	Autorisations temporaires de port	52
Tireurs sportifs ou chasseurs étrangers membres de l'UE et (en général) membre d'un club de tir en Belgique	Validations pour la Belgique des «Cartes européennes d'arme à feu »	298
Patrouilles mixtes transfrontalières	Autorisations temporaires de détention et de port	3
Policiers, gendarmes et troupes armées qui sont présents sur le territoire belge (entre autres transit, transport nucléaire, tour cyclistes ou exercices, p.e. formation à Marche en Famenne		24

En ce qui concerne les agents d'entreprises de gardiennage étrangères reconnues en Belgique et qui y exercent certaines activités professionnelles, aucune demande n'a été introduite depuis 2002.

Pour ce qui a trait aux « étrangers qui désirent acquérir en Belgique une arme soumise à autorisation soit en vue de son exportation, soit pour la laisser dans un club de tir sportif en vue de la pratique de cette activité avec autorisation de détention », il peut être ajouté après « club de tir sportif » : « ou dans une résidence en Belgique ».

En ce qui concerne les tireurs sportifs étrangers ressortissants d'un État de l'Union Européenne, la Sûreté de l'État valide pour le territoire belge les cartes européennes d'arme à feu des personnes qui sont membres d'un club de tir en Belgique.

La Sûreté de l'État n'a jamais reçu de demandes d'agents qui ont pour mission d'assurer la sécurité des vols des compagnies aériennes étrangères au départ ou à destination de la Belgique (mais c'est la loi étrangère qui s'applique dans les avions de sociétés étrangères). De même, aucune demande n'est arrivée concernant les douaniers américains présents sur le territoire national (en fait à Anvers et à Zeebrugge) en application de l'accord « Container Security Initiative » (la douane belge assure le contrôle sur place)».

Cette réponse semble conforter la constatation faite par le Comité permanent R en 2000 selon laquelle, dans la pratique, la Sûreté de l'État n'avait pas une vue globale sur les autorisations de détention et port d'armes délivrés en Belgique. Le Comité permanent R avait donc recommandé de porter remède à cette lacune, notamment en permettant l'accès de la Sûreté de l'État au registre central des armes. Le Comité avait aussi recommandé d'accorder une compétence générale et préalable d'avis en la matière, quelle que soit le domicile du demandeur, en Belgique ou à l'étranger.

Le Comité permanent R a donc demandé à la Sûreté de l'État si ce service :

- disposait à présent d'un accès au registre central des armes ?
- connaissait le nombre total d'autorisations de détention et ports d'armes délivrés en Belgique au cours des années précédentes ?
- était consulté préalablement 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 quelle que soit la résidence du demandeur, en Belgique ou à l'étranger ?
- quelles raisons ou circonstances pouvaient empêcher la concrétisation de telles recommandations ?

La deuxième réponse de la Sûreté de l'Etat

Par courrier du 8 février 2006, l'administrateur général de la Sûreté de l'État a fait parvenir la réponse suivante au Comité permanent R.

« Notre service dispose d'un accès direct au Registre Central des Armes. Rappelons que selon le point 2, 4 de la circulaire coordonnée 3630/1/8 du 30 octobre 1995 relative à l'application des dispositions légales et réglementaires relatives aux armes le Registre Central des Armes est « une banque de données où sont enregistrées les informations sur la détention d'armes à feu dans notre pays. Il est géré par un service de la direction générale de l'appui opérationnel de la Police fédérale portant le même nom. Il est au service des services de police et il n'est pas accessible au public ».

Une des recommandations prônées par le Comité R a donc été rencontrée.

Même si la Sûreté de l'État a un accès direct au Registre central des Armes, notre service ne connaît pas pour autant le nombre total des autorisations de détention et de port d'armes délivrées en Belgique au cours des années précédentes. En effet, notre accès au Registre Central des Armes ne permet aucunement d'avoir une vue générale du nombre de détention ou de port d'armes délivré en Belgique.

La Sûreté de l'État n'est pas consultée préalablement à la délivrance ou au retrait de toute autorisation de détention d'une arme à feu de défense et de guerre ainsi que de tout permis de port d'armes de défense quelle que soit la résidence du demandeur, en Belgique ou à l'étranger. Comme déjà exposé dans ma lettre du 19 décembre 2005, la Sûreté de l'État est seulement compétente pour la délivrance des autorisations de détention et de permis de port d'armes à feu aux personnes, belges et étrangères, qui ne sont pas domiciliées en Belgique.

Ce nonobstant, la Sûreté de l'État garde une compétence d'avis vis-à-vis d'autres instances belges. En matière d'agrément des armuriers, fabricants, courtiers et collectionneurs, le Gouverneur de province peut solliciter l'avis de la Sûreté de l'État en application du point 4.4.4. de la circulaire coordonnée du 30 octobre 1995 relative à l'application des dispositions légales et réglementaires relatives aux armes.

Concernant la délivrance de permis de port d'arme aux membres des missions diplomatiques étrangères en Belgique, non exempts d'inscription aux registres communaux, le point 6.4.4.c de la même circulaire précise que les Gouverneurs de province sont priés de prendre l'avis de la Sûreté de l'État avant de statuer.

La Sûreté peut également être consultée par les Gouverneurs de province avant la délivrance de permis de port d'arme aux membres, domiciliés en Belgique, de services de gardiennage d'organisations internationales et d'ambassades étrangères en Belgique.

L'office des étrangers nous consulte à propos de demandes d'achat ou de détention d'armes à feu introduites par des étrangers, ceci sur base du point 5.6.4. de la circulaire précitée du 30.10.1995. Ce point traite de la personnalité du demandeur et notamment du fait que l'enquête locale de la police tient compte d'une éventuelle activité politique violente.

Enfin, sur base du même point de cette circulaire la police locale nous consulte parfois avant de délivrer une autorisation de détention d'une arme à feu.

La section législation en matière d'armes, qui a longtemps fait partie du service d'études s'occupant du PES⁶ et de la Prolifération, a été intégrée début 2004 dans le service Enquêtes de sécurité, dont il est une sous-section, composée de deux fonctionnaires.

Le plan de personnel prévoit le recrutement de fonctionnaires pour le service D.3. Ce plan est en exécution au niveau de l'Administration centrale.

En ce qui concerne le transfert éventuel des compétences de la Sûreté de l'État en matière de délivrance d'autorisations de détention et de permis d'armes à feu à une autre administration, la Ministre de la Justice n'a pas encore arrêté sa position de façon définitive.

Comme vous le savez, en vertu de l'article 1er, 7° de l'arrêté royal du 26 juin 2002 relatif à la détention et au port d'armes par les services de l'autorité ou de la force publique, les agents faisant partie des services extérieurs de la Sûreté de l'État sont autorisés à détenir et porter une arme, ceci bien entendu dans le cadre du service et sous l'autorité de la hiérarchie. En dehors de ce cadre, ces agents sont soumis à la réglementation applicable à chaque citoyen.

⁶ Potentiel économique et scientifique

Pour le reste, la Sûreté de l'État n'exerce pas de contrôle sur les autorisations de détention et les permis de port d'armes à feu accordés aux membres de son personnel ».

Conclusions

Le Comité permanent R constate et se réjouit que l'une de ses recommandations formulées dans son rapport d'activités de l'année 2000 ait été rencontrée, même s'il apparaît à première vue qu'il n'y a pas de base légale pour accès direct.

Le Comité permanent R regrette cependant que - bien qu'ayant un accès au Registre Central des Armes - la Sûreté de l'État n'a toujours pas une vue globale sur le nombre d'autorisations de détention et port d'armes délivrés en Belgique.

Le Comité permanent R recommande à nouveau qu'il soit porté remède à cette lacune.

Le Comité reste persuadé que les compétences décisionnelles de la Sûreté de l'État n'ont aucun lien avec les activités normales d'un service de renseignement. La mission essentielle de ce service consiste avant tout à informer les autorités des menaces tant internes qu'externes pouvant peser sur la Belgique. La compétence d'avis de ce service est donc celle qui entre le mieux dans le cadre de la mission d'information précitée.

Le Comité permanent R s'étonne que dans son dernier écrit (cf. 8 février 2006) la Sûreté de l'État ne mentionne pas la loi du 3 mai 2005 qui modifie la loi du 11 décembre 1998. Le Comité permanent R poursuivra l'examen de cette matière, plus précisément dans le cadre des enquêtes de contrôle en matière d'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, comme modifié par la loi du 3 mai 2005 et de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes.

TITRE 6
ETUDES ET ACTIVITES

CHAPITRE 1	L'ETUDE SUR LE POTENTIEL SCIENTIFIQUE ET ECONOMIQUE
-------------------	--

La mission légale du Comité permanent R est de veiller à la protection des droits que la Constitution et la loi confèrent aux personnes, mais aussi à la coordination et à l'efficacité des services de renseignements belges.

C'est ainsi que le Comité permanent R s'est régulièrement intéressé à la manière dont la Sûreté de l'État avait pris en charge sa mission de protection du « *potentiel scientifique ou économique* » du pays. Cette mission est prévue par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Un chapitre du rapport d'activités 2003¹ du Comité permanent R est consacré au rôle que peuvent jouer les services de renseignement privés et publics dans la protection de ce potentiel scientifique ou économique. Le Comité y a constaté la difficulté de cerner cette notion de potentiel scientifique ou économique. Au sens des articles 7, 1° et 8, 4° de la loi du 30 novembre 1998 précitée, on entend par "*potentiel scientifique ou économique*", "*la sauvegarde des éléments essentiels du potentiel scientifique ou économique*". Il appartient au Comité ministériel du Renseignement et de la Sécurité de définir plus avant cette notion.

Le Comité permanent R a attiré l'attention sur la difficulté de protéger les secrets scientifiques et économiques dans le contexte actuel de la société de l'information. Dominée par les progrès technologiques, celle-ci est caractérisée autant par son internationalisme que par son ouverture d'esprit scientifique. Le Comité permanent R a également montré combien il était difficile de définir le rôle que la Sûreté de l'État devait jouer dans la protection du potentiel scientifique et économique du pays dans le cadre d'une société fondée sur l'accès ouvert à tous les marchés, la libre entreprise, la mondialisation et la déréglementation.

Lors d'un colloque organisé au Sénat le 3 décembre 2004, Vice- Première ministre et ministre de la Justice ONKELINX s'est déclarée sensible au rapport du Comité permanent R et à ses recommandations. Elle a donc chargé le Comité permanent R de lui soumettre une proposition de définition des éléments essentiels de notre potentiel scientifique et économique à sauvegarder.

Le Comité permanent R a estimé qu'il ne pouvait se hasarder dans l'élaboration d'une telle définition sans avoir préalablement consulté un panel d'acteurs des milieux impliqués. La formulation d'une telle définition devait, selon le Comité, résulter d'une approche multidisciplinaire abordant les aspects scientifiques, technologiques et économiques du problème mais aussi politiques, juridiques et criminels.

C'est la raison pour laquelle le Comité permanent R s'est adressé à un ensemble de personnes et d'instances représentatives des milieux scientifiques, académiques et économiques spécialisés. Le Comité a également estimé nécessaire de recourir à l'expertise d'un spécialiste de la sécurité dans le monde des entreprises. Force est de constater que les éléments de réponse obtenus furent peu nombreux et que ceux-ci sont loin d'épuiser la réflexion sur le sujet. Ceci démontre à nouveau la difficulté de cerner cette notion de potentiel scientifique ou économique et de définir le rôle que la Sûreté de l'État doit jouer dans sa protection.

¹ Comité permanent R, *Rapport général d'activités 2003*, Bruxelles, 2004 (www.comiteri.be).

Le présent chapitre rend compte des résultats de cette consultation ainsi que du rapport d'expertise.

1. LA DIFFICULTÉ DE DÉFINIR LE POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE D'UN PAYS

En ces temps de mondialisation croissante, est-il encore de mise de parler de protection du patrimoine scientifique et économique d'un pays ? Cette conception ne s'oppose-t-elle pas à l'universalité et à la modernité de la mondialisation. Celle-ci touche de nombreux domaines parmi lesquels le commerce, les finances, l'industrie, les techniques, l'agriculture et même la culture et les habitudes alimentaires. Il existe même un domaine où la mondialisation est ancienne, c'est celui des sciences pures. C'était déjà la mondialisation de la connaissance scientifique. Par contre, les applications de ces connaissances, c'est-à-dire les techniques, furent toujours protégées par ceux qui les maîtrisaient.

On ne se protège pas dans l'absolu, mais contre des menaces précises ! Pour mettre en oeuvre une défense du patrimoine, il faut d'abord définir avec précision ce qui le menace. Quand la menace est identifiée, toute protection – même celle du patrimoine – doit résulter d'une réflexion globale.

2. NOTIONS CONNEXES : LES MATIÈRES D'INTÉRÊT ÉCONOMIQUE STRATÉGIQUE, LES BESOINS ET LES INTÉRÊTS VITAUX DE LA NATION, LE POTENTIEL SOCIO-ÉCONOMIQUE DU PAYS

Il est peut-être utile de comparer la notion de « *potentiel économique* » contenue dans la loi organique des services de renseignement à celles de « *matières d'intérêt économique stratégique* », de « *besoins de la Nation* », « *d'intérêts vitaux de la Nation* » et de « *potentiel socio-économique* » contenues dans d'autres réglementations.

2.1. La loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques

Cette loi organise les conditions de l'autonomie de gestion dont jouissent à présent des organismes d'intérêt public tels que Belgacom, la Société Nationale des Chemins de Fer belges (SNCF) ou La Poste dans certains secteurs industriels ou commerciaux donnés.

Les règles et conditions spéciales selon lesquelles ces entreprises exercent leurs missions légales de service public, sont arrêtées dans un contrat de gestion conclu entre l'État et l'entreprise concernée. Ce contrat de gestion définit notamment les « tâches de service public » qui doivent être assumées, les règles de tarification de ces services, les règles de conduite vis-à-vis des usagers... et, « *le cas échéant, les matières d'intérêt économique stratégique pour lesquelles la passation des marchés est soumise à l'approbation, selon le montant, du Ministre dont relève l'entreprise publique* » concernée². Le contrat de gestion peut désigner ce que sont ces matières d'intérêt économique stratégique.³

² Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, article 3, §2, 6°.

³ *Idem*, article 11, §2, alinéa 2.

L'article 156 de la loi de 1991 définit les missions de service public de la SNCB en particulier. Outre le transport intérieur de voyageurs et la gestion de l'infrastructure ferroviaire, cette disposition mentionne les prestations que la SNCB « *est tenue de fournir pour les besoins de la Nation* ». Cette notion est précisée dans l'article 32 du titre V du contrat de gestion de la SNCB

« A la requête des institutions dûment mandatées, le SPF Intérieur, à l'intermédiaire de la Direction générale du Centre de Crise (DGCC), et le Ministère de la Défense, à l'intermédiaire de l'État-major de l'Armée, la SNCB participe selon ses compétences à la préservation des intérêts vitaux de la Nation et à la satisfaction des besoins essentiels de la population :

- 1) *l'ordre public, c'est-à-dire la tranquillité, la salubrité et la sécurité publique ;*
- 2) *le potentiel socio-économique du pays ;*
- 3) *la souveraineté nationale et les institutions publiques établies par la Constitution et les lois ;*
- 4) *l'intégrité du territoire national. »*

La SNCB doit exercer cette mission en temps de paix comme de guerre. A cet effet, elle doit notamment se conformer aux « avis contraignants » du Comité ministériel du Renseignement et de la Sécurité. Elle doit aussi agir en concertation avec le « Bureau de défense en charge des relations et des études liées aux besoins de la Nation » et avec l'OTAN. Ces mêmes dispositions sont reprises dans l'arrêté royal du 5 juillet 2005 portant approbation du contrat de gestion conclu entre l'État et Infrabel. Infrabel est cette nouvelle société anonyme de droit public, chargée de gérer l'infrastructure ferroviaire belge.

2.2. L'arrêté royal du 18 avril 1988 portant création du Centre Gouvernemental de Coordination et de Crise⁴

La notion de « *potentiel socio-économique du pays* » se retrouve aussi dans l'article 2 de cet arrêté royal qui mentionne le « *potentiel socio-économique du pays* » parmi les « *intérêts vitaux de la Nation ou les besoins essentiels de la population* » dont le Centre est chargé de gérer les crises. Cette disposition ne comporte pas de définition plus avancée du potentiel socio-économique.

2.3. L'arrêté royal du 31 janvier 2003 portant fixation du plan d'urgence pour les événements et situations de crise nécessitant une coordination ou une gestion à l'échelon national⁵

Le préambule de cet arrêté royal établit un constat et précise les domaines de vulnérabilité de l'économie belge.

« Pour rappel, le territoire de la Belgique est soumis à un certain nombre de risques traditionnellement répertoriés comme suit :

- *les risques naturels d'inondations et de tempêtes ;*

⁴ M.b., 4 mai 1988, modifié par l'A.R. du 11 mai 1990 (M.b. du 1er juin 1990).

⁵ M.b., 21 février 2003.

- les risques technologiques résultant notamment d'une forte concentration d'activités industrielles et d'un réseau de transports et de communications extrêmement développé.

Il existe d'autant plus de risques d'aboutir à des situations d'urgence que la Belgique présente des caractéristiques telles que :

- une haute densité de population, principalement au nord et au centre du territoire national (Bruxelles, Anvers, Gand, Liège et Charleroi) ;
- une présence de points sensibles ou stratégiques de première importance (OTAN, SHAPE, Conseil européen et Commission européenne) ;
- une concentration de points vitaux dans les domaines :
 - de la production et de la distribution d'énergie ;
 - de la fourniture d'eau potable ;
 - des transports et des communications ;
 - de la chaîne alimentaire, etc. ;
- l'existence de 5 sites nucléaires et de 240 industries de type Seveso.

2.4. L'arrêté royal du 17 octobre 2003 portant fixation du plan d'urgence nucléaire et radiologique pour le territoire belge⁶

Cet arrêté royal prévoit la création d'une cellule socio-économique, qui doit analyser sous un angle économique et social les conséquences des mesures prises à la suite d'un incident nucléaire, et ce, tant a priori qu'a posteriori de la décision. Cet arrêté royal stipule également :

« 2.1.8 Affaires économiques et Énergie

Le ministre des Affaires économiques et de l'Énergie prend toutes les mesures nécessaires pour que, dans une situation d'urgence radiologique, l'approvisionnement en énergie soit assuré. Il veille à ce que les activités économiques vitales de la Nation soient maintenues dans la mesure du possible (AR du 27 juillet 1950 déterminant les besoins vitaux à satisfaire pour l'exécution de la loi du 19 août 1948)».

2.5. La Banque de données CRIVISEN (points CRitiques, VItaux et SENSibles)

Historiquement, les concepts de points « vitaux » et « sensibles » furent définis par l'OTAN dans le cadre de la menace d'un conflit entre l'Est et l'Ouest. Dans ce contexte, un accord de protocole fut conclu en 1997 entre les ministres de l'Intérieur et de la Défense nationale concernant :

- l'établissement d'une liste des points vitaux et sensibles ;
- la détermination de mesures de protection ;
- le partage de responsabilités entre la gendarmerie et l'armée.

La dernière modification de la liste des points vitaux et sensibles datait de 1991 à l'occasion de la première guerre du Golfe.

⁶ M.b., 20 novembre 2003.

Les attaques du 11 septembre 2001 confirmèrent que la menace actuelle était « asymétrique » et se présentait sous la forme d'un risque indéterminé, davantage lié au terrorisme qu'à des opérations militaires telles que celles prévues pendant la guerre froide. L'ancienne Commission pour les Problèmes Nationaux de Défense (CPND/CNVV)⁷, avait reçu pour mission de revoir l'inventaire de ces points et de développer la banque de données CRIVISEN (points CRItiques, VItaux et SENSibles). Cette mission devait se réaliser en collaboration avec (et au profit de) tous les départements et niveaux de responsabilités concernés. La banque de données CRIVISEN s'intéresse donc à trois catégories de points :

Les 'points vitaux' dans le domaine socio-économique

Il s'agit des installations, constructions ou ouvrages d'art dont l'existence, les produits ou services :

- sont vitaux pour la population ou pour le maintien ou le rétablissement de l'ordre public ;
- ou dont la destruction ou la mise hors service aurait des conséquences graves à catastrophiques en raison de l'absence éventuelle de solutions de remplacement (Ex. les centrales nucléaires, les installations portuaires, certains ponts...).

Les 'points sensibles' dans le domaine militaire

Il s'agit des installations, constructions ou ouvrages d'art dont l'existence, les produits ou services :

- sont de la plus haute importance ou indispensables pour le potentiel de défense national ou allié ;
- ou dont la perte aurait des conséquences catastrophiques en raison de l'absence de solutions de remplacement ou dont le remplacement ne serait possible qu'au prix d'un préjudice grave aux efforts de défense vitaux (Ex. les casernes, les centres de transmission de l'armée...).

Une catégorie ajoutée après le 11 septembre 2001 : les 'points critiques'

Il s'agit des personnes (autorités politiques ou morales, belges ou non), communautés, institutions, bâtiments, installations, lieux et marchandises qui peuvent faire l'objet d'une menace réelle ou potentielle. Celle-ci peut être de nature politique ou purement criminelle.

Les grands domaines retenus dans la banque de données CRIVISEN sont donc militaire et assimilé, institutions belges, institutions non belges, institutions internationales, lieux liés à des cultes reconnus, transports, industries/laboratoires dangereux ou indispensables, bâtiments scolaires, espaces commerciaux et de loisirs – événements de masse, protection de la population, réseaux d'information, de télécommunication et de distribution, alimentation et eau, finances et secteur bancaire, emblèmes et bâtiments nationaux.

3. LA CONSULTATION : QUESTIONS ET REPONSES

Le 7 mars 2005, un courrier a été adressé à 33 personnes et instances représentatives des milieux scientifiques, académiques et économiques.

⁷ Transférée depuis lors des Services du Premier ministre à ceux du ministre de l'Intérieur (Centre de crise).

Madame LIZIN, Présidente du Sénat et Madame ONKELINX, Vice-Première Ministre et Ministre de la Justice en ont été avisées le même jour. Le 3 mai 2005, un membre du Comité permanent R a présenté la démarche du Comité aux membres du Conseil Central de l'Économie (CCE).

A la date du 1^{er} février 2006, le Comité permanent R n'a reçu que les réponses de huit personnes et instances. M. VAN CAMP, recteur de la Vrije Universiteit Brussel a proposé que cette matière très complexe soit soumise à plusieurs experts afin d'avoir un aperçu complet de la problématique. Il a suggéré que cette question fasse l'objet d'une recherche approfondie. D'autres autorités académiques et institutions ont annoncé leur intention de répondre à la demande d'avis du Comité permanent R mais elles ont fait savoir qu'elles souhaitaient une concertation préalable entre recteurs et doyens avant de se prononcer.

Le réseau LIEU (Liaison Entreprises - Universités) fut chargé d'examiner la question. Ce réseau regroupe les interfaces et cellules de valorisation des universités de la communauté Wallonie - Bruxelles.

Le 13 septembre 2005, un membre du Comité permanent R a présenté la démarche du Comité aux membres du Réseau LIEU. Le produit de cette concertation n'a pas encore été adressé au Comité.

Le 3 octobre 2005, le Comité permanent R a confié une mission d'expertise à Monsieur DE MESMAEKER, conseiller en sécurité d'entreprises. La mission était de formuler un avis sur les éléments essentiels de la définition du potentiel scientifique et économique que les services de renseignement belges ont mission de protéger. Monsieur DE MESMAEKER a remis son rapport au Comité le 28 décembre 2005.

Deux représentants du Comité permanent R ont assisté au colloque « *Rencontres Innovation, Compétitivité et Connaissances* » organisées à Paris par l'association SCIP France et Veille Magazine.⁸

Différents textes et rapports officiels ont été consultés compte tenu de leur intérêt pour la matière ici examinée.

3.1. Les questions posées

Les questions posées aux experts ont été les suivantes :

- Comment définir les éléments essentiels du potentiel scientifique ou économique d'un pays comme la Belgique ?
- Qui sont les moteurs de ce potentiel scientifique et économique ?
- A quelles menaces est exposé ce potentiel scientifique et économique ?
- A quelles difficultés se heurte la protection du potentiel économique et scientifique de notre pays ?
- Comment attribuer un caractère national au potentiel économique et scientifique présent dans notre pays ?
- Comment définir le secret en matière économique, scientifique et technologique et situer sa place dans une économie caractérisée par les mutations technologiques, la circulation de l'information et son ouverture internationale ?
- Comment la Sûreté de l'État doit-elle prendre sa mission en charge dans cette matière ?

⁸ Voir Titre 8 La composition et le fonctionnement du Comité permanent R, chapitre 5.

3.2. Les réponses obtenues

3.2.1. La réponse de M. POULLET - doyen de la faculté de Droit des Facultés universitaires Notre Dame de la Paix à Namur (lettre du 14 mars 2005)

« Votre lettre en date du 7 mars a retenu ma meilleure attention. Votre souci de réunir les avis des experts sur un sujet aussi délicat vous honore. Hormis ce que nous avons déjà écrit Jean-Marc Dinant et moi-même, dans le rapport « Echelon », établi à votre demande, je vois mal ce que je pourrais ajouter. Il est clair en effet que les risques liés à la digitalisation de l'information et à sa circulation sur des infrastructures de communication constituent une préoccupation importante vu les possibilités pour des puissances étrangères de capter de tels messages. A cet égard, nous plaidons, comme déjà recommandé dans le rapport et dans les rapports européens en suite à l'affaire Echelon, pour une politique indépendante européenne de cryptologie (cf. le projet Galileo)».

3.2.2. La réponse de M. DE MARET, recteur de l'Université Libre de Bruxelles (lettre du 17 mars 2005)

Monsieur DE MARET a souhaité que les questions posées par le Comité permanent R soient examinées au cours d'une discussion collégiale de l'ensemble des Recteurs des Universités francophones. Il a cependant d'emblée fait part de ses inquiétudes sur la protection des données industrielles : *« Le 'hacking' et le vol en vue d'obtenir des informations confidentielles sur des collaborations industrielles doit être évalué. »*

3.2.3. La réponse de M. DE BUYSER - Directeur général de la Société anonyme de droit public ASTRID (lettre du 21 mars 2005)

« La mission confiée par le législateur à la S.A. A.S.T.R.I.D. figure dans la loi du 8 juin 1998 relative aux radiocommunications des services de secours et de sécurité.

L'article 3, § 1 définit cette mission comme « la constitution, l'exploitation, l'entretien et les adaptations et élargissements évolutifs d'un réseau de radiocommunications pour la transmission de voix et de données au profit des services de secours et de sécurité, de la Sûreté de l'État et d'institutions, sociétés ou associations, de droit public ou privé, qui fournissent des services dans le domaine des secours et de la sécurité ».

Pour réaliser cet objectif, A.S.T.R.I.D. a développé trois systèmes intégrés : un réseau de radiocommunications pour la transmission de voix et de données, des centres de dispatching provinciaux et un réseau de paging. Chaque système a été mis sur pied ces dernières années. À présent, la S.A. a essentiellement pour mission d'exploiter et d'entretenir ces systèmes. En plus de la transmission de voix normale, le réseau de radiocommunications permet également la transmission de données. À l'heure actuelle, seuls les services de police utilisent les possibilités de transmission de données d'A.S.T.R.I.D., essentiellement via les banques de données de la police connectées aux centrales de dispatching.

La S.A. et ses collaborateurs mettent les différents systèmes à la disposition des services de secours et de sécurité uniquement en tant que support pour l'envoi et la réception de ces données. Les collaborateurs de la S.A. n'interviennent à aucun moment dans l'utilisation opérationnelle de ces données et n'ont pas non plus accès au contenu des banques de données.

La S.A. ne sait pas ce qui est considéré comme « potentiel scientifique et économique du pays » dans ces banques de données et il nous semble que cette question intéresse davantage les services de secours et de sécurité. Nous suggérons dès lors d'adresser votre requête à des services de sécurité, tels que la Police fédérale et le Centre gouvernemental de crise.

Vu l'importance des différents systèmes ASTRID pour la communication nécessaire des services de secours et de sécurité dans ce pays, nous estimons que l'ensemble de l'infrastructure et les connaissances techniques de la S.A. doivent bénéficier d'une protection particulière. Des mesures ont déjà été convenues à cet égard avec différents services de secours et de sécurité (tels que la police locale et fédérale et le centre gouvernemental de crise). Il est difficile de répondre à la question de savoir si l'infrastructure et le savoir-faire de cette société doivent relever de la définition du « potentiel scientifique et économique du pays », étant donné l'absence d'une définition claire. Nous pouvons toutefois souligner son intérêt dans le cadre de la sécurité nationale ».

3.2.4. La réponse de M. QUADEN, - gouverneur de la Banque nationale de Belgique (lettre du 4 avril 2005)

«Je vous remercie de m'avoir associé à votre réflexion sur la définition des éléments essentiels à sauvegarder du potentiel scientifique et économique du pays.

Après la lecture fort instructive du Rapport d'activités établi par votre instance pour l'année 2003, je me permets d'attirer votre attention sur trois aspects qui ne me semblent pas pouvoir être négligés dans la définition du potentiel économique et qui risqueraient de ne pas être couverts si l'on se base sur la liste des domaines d'activité jugés prioritaires par la Sûreté de l'État dans sa note du 31 mai 2001 au Comité ministériel du renseignement et de la sécurité.

Le bon fonctionnement du système financier et des grandes infrastructures financières belges est indispensable à l'activité économique du pays et même au-delà de nos frontières, compte tenu de l'imbrication du système belge dans des réseaux internationaux, liée notamment à la localisation sur notre territoire de plusieurs infrastructures transfrontalières. Selon les éléments repris dans votre rapport, ces infrastructures ne sont pas reprises dans les domaines prioritaires cités par la Sûreté de l'État, alors que leur protection ainsi que celle de la continuité du service qu'elles rendent devraient assurément être rangées au rang de priorité pour la préservation du potentiel économique du pays.

Il s'agit des systèmes opérés par la Banque même, ELLIPS, CEC et NBB Clearing, ainsi que de systèmes importants à l'échelle nationale, tels Banksys, ou européenne et mondiale, tels Euroclear (y compris le CIK), SWIFT et Mastercard Europe. Il pourrait être utile d'examiner si cette liste ne devrait pas être étendue aux grandes banques belges, ou à des systèmes gérés par celles-ci, tels ISABEL.

La Banque est elle-même fortement impliquée dans la surveillance de ce domaine d'activité. Une de ses missions légales est en effet de contribuer à la stabilité financière et, à ce titre, elle est plus spécifiquement chargée de l'oversight des systèmes de paiements et de règlement titres. (...).

Votre rapport évoque par ailleurs la difficulté de savoir si la protection des éléments essentiels du potentiel économique et scientifique du pays doit se limiter aux entreprises nationales ou s'étendre aussi aux entreprises sous contrôle étranger localisées sur notre territoire.

L'économie belge est caractérisée par un degré d'ouverture considérable et sa capacité à attirer ou retenir des investissements étrangers est déterminante pour l'évolution de sa prospérité, et notamment de l'emploi dans notre pays. De ce point de vue, la capacité des autorités à assurer un bon niveau de sécurité économique peut jouer un rôle dans la décision de localiser une activité en Belgique plutôt qu'ailleurs. Je peux donc me rallier au point de vue exprimé par la Fédération des entreprises de Belgique et repris dans votre Rapport selon lequel doit être considérée comme belge toute entreprise implantée sur le territoire national et qui y crée de la valeur ajoutée, quelle que soit la nationalité de ses actionnaires ou de ses dirigeants.

Une autre dimension à laquelle il faut être attentif lorsqu'est évoquée la protection des infrastructures publiques est que compte tenu de la tendance récente des autorités à privatiser certaines entreprises publiques ou à contracter des partenariats avec le secteur privé pour le financement et/ou la gestion de certains équipements, l'on ne néglige pas certaines infrastructures privées essentielles, je pense en particulier à l'aéroport de Bruxelles-national sous le contrôle de BIAC ».

3.2.5. La réponse de M. VAN CAMP - recteur de la Vrije Universiteit Brussel (lettre du 15 avril 2005)

« En réponse à votre lettre du 7 mars dernier, je souhaiterais, par la présente, vous expliquer comment la VUB (Vrije Universiteit Brussel) conçoit la protection des recherches dotées d'un « potentiel scientifique ou économique ».

La VUB, qui est financée par la Communauté flamande, est soumise à la législation flamande pour toutes les questions relatives à la recherche et la valorisation.

Attendu que la majeure partie de la recherche universitaire est financée par les deniers publics, l'université doit remplir sa mission au nom de cette communauté, tout en favorisant une exploitation optimale des connaissances universitaires au bénéfice de la société. La valorisation stimule l'enseignement et la recherche en mettant des moyens financiers à disposition et en exhortant les nouvelles recherches et le savoir-faire novateur.

Les décrets (décrets universitaires, décrets relatifs aux services scientifiques et sociaux) s'appliquent à la VUB.

Eu égard aux services scientifiques ou sociaux, l'université veille rigoureusement à contrôler et approuver tous les contrats de recherche conclus avec des tiers, et ce, avant qu'ils puissent être mis en œuvre. Non seulement, cette mesure revêt une importance pour les aspects juridiques, mais elle garantit en outre que les recherches sont effectuées dans le respect des dispositions du décret en vigueur, et plus particulièrement, qu'elles ont lieu sur la base d'une couverture des coûts et que l'université reçoit une indemnisation équitable en cas de valorisation éventuelle.

Quant aux droits de propriété des recherches dotées d'un potentiel scientifique et/ou économique, la réglementation flamande s'énonce comme suit : les recherches, y compris les droits patrimoniaux y afférents, sont la propriété de l'Université, sauf dispositions contraires dans les réglementations et/ou accords approuvés par l'Université, et ce, dans la mesure où ces recherches et les découvertes qui en découlent sont effectuées par des chercheurs dans le cadre d'activités confiées par l'Université. L'on entend par « chercheur » toute personne physique qui, seule ou en groupe, effectue des recherches dans l'Université, dans le cadre d'un contrat de travail, d'un statut de fonctionnaire ou d'une bourse octroyée par l'Université ou par un tiers, ou dans toute autre relation avec l'Université.

Sur cette base, la Vrije Universiteit Brussel (et peut-être aussi toutes les autres universités flamandes) a élaboré un règlement de valorisation interne qui régit les droits et devoirs de l'université et des inventeurs en cas de valorisation de ces recherches.

Étant donné que le principe de liberté universitaire est une donnée importante dans le milieu universitaire, la VUB a repris les éléments suivants dans son règlement de valorisation : les recherches valorisables doivent être signifiées à l'Université, mais les chercheurs ont le droit de les rendre publiques. En outre, l'Université ne peut s'opposer à cette publication que si la protection intellectuelle préalable de ces recherches le requiert ou pour ne pas mettre en péril leurs chances de valorisation. Cette décision de report de publication doit toujours être motivée.

Concrètement, cela signifie que la VUB peut gérer ses recherches dotées d'un potentiel scientifique et/ou économique d'une manière relativement close, et qu'elle veille à ce qu'elles soient dûment protégées dans l'intérêt de la nation.

J'aimerais, par ailleurs, souligner que les décrets tels qu'ils sont d'application en Flandre n'existent pas de la même manière en Wallonie. Les universités wallonnes doivent dès lors prendre d'autres mesures si elles souhaitent protéger les droits de propriété des recherches menées dans leur institution.

Du reste, de nombreux problèmes se posent lorsque des recherches menées avec des moyens publics flamands sont valorisées dans d'autres Régions. Il est alors question de conflit de compétences entre régions, ce qui en soi ne porte pas préjudice à la protection dans l'intérêt du pays.

Dans le cadre de collaborations purement scientifiques, qui sont bien sûr généralement internationales, il ne peut, à mon avis, être exclu que certains résultats soient échangés sans s'être pleinement assuré d'un potentiel scientifique et économique éventuel (souvent dans un avenir lointain). Je pense toutefois que nos chercheurs peuvent se voir confier la responsabilité de veiller, dans ces échanges scientifiques, à ce que l'entrée (input) et la sortie (output) soient de valeurs comparables.

J'aimerais également préciser que M. XX (Note : un membre de la Sûreté de l'État) est venu par deux fois discuter avec le responsable Valorisation de la VUB, M. De Greef. Ils se sont entretenus de la protection de la propriété intellectuelle, des procédures d'octroi de la VUB et de l'accès au campus par les externes, matière pour laquelle il fut renvoyé au « facility manager » de la VUB, M. Steen.

Comme, dans la présente réponse, je m'en tiens aux questions qui concernent la Vrije Universiteit Brussel dans le cadre de ses services scientifiques et sociaux et de ses activités de valorisation, je propose que cette matière très complexe soit également soumise à plusieurs experts, afin d'avoir un aperçu complet de la problématique. Cette question peut peut-être faire l'objet d'une recherche approfondie. »

3.2.6. Réponse de M. VANDENBORRE - directeur général de l'administration des douanes et accises (lettre du 10 mai 2005)

« À mon avis, les éléments essentiels du potentiel économique comprennent la capacité à produire des biens et des services ainsi que celle des opérateurs à participer au commerce international. On pourrait définir le potentiel scientifique comme la capacité des scientifiques à développer de nouvelles techniques et nouveaux produits dans les deux processus précités afin d'agir de façon plus effective et/ou plus efficace.

Les moteurs peuvent notamment être les suivants : un climat économique mondial favorable, des centres de recherche bien équipés, une tendance à l'innovation au sein de la population, la stimulation du climat des entreprises, de bonnes infrastructures et la création d'un environnement où les dernières techniques informatiques peuvent être exploitées et appliquées.

Pour le moment, les plus grosses menaces se situent au niveau du terrorisme et de la sécurité mondiale. Toutefois, les menaces ne se limitent pas aux aspects purement terroristes mais comprennent également les aspects économiques, sociaux et environnementaux. Outre ces menaces générales, chaque participant à la vie économique peut également être confronté à des menaces liées à sa situation spécifique en raison, par exemple, d'une concurrence déloyale à la suite d'un abus de son savoir-faire, de secrets commerciaux, de relations commerciales, etc. L'obtention d'informations sur un procédé commercial spécifique par des concurrents peut avoir un impact négatif sur la position d'une entreprise sur le marché, entraînant une faillite dans le pire des cas, et peut donc nuire au potentiel économique d'un pays.

En ce qui concerne les problèmes de protection du potentiel scientifique et économique, l'on peut dire ce qui suit du point de vue des Douanes :

- En raison du flux croissant de marchandises, il est devenu difficile de réaliser des contrôles efficaces sans perturber les flux commerciaux légitimes.*
- Des mesures peuvent être facilement appliquées aux flux de marchandises en vue de protéger le potentiel scientifique et économique mais si ces menaces découlent d'une opération non liée à des marchandises, telle que la diffusion et le transfert de connaissances, l'impact est beaucoup plus faible.*

En tant que Douanes, nous avons un faible impact à cet égard vu nos capacités limitées de contrôle. Lorsqu'il s'agit d'affaires matérielles, il est possible de prévoir un contrôle des marchandises, intégral ou non, éventuellement complété par un régime de licences. Lors de la diffusion ou du transfert de connaissances, davantage de problèmes peuvent se poser. Les livres et autres imprimés pourraient encore être détectés et contrôlés au moyen d'un contrôle ciblé des marchandises. C'est toutefois moins évident pour les disquettes, les CD-ROM et les memory sticks. Par ailleurs, les connaissances d'une personne ne peuvent nullement être contrôlées.

En tant que Douanes, nous opérons dans un environnement communautaire et, pour nous, le caractère national d'un bien est subordonné au caractère communautaire. À titre d'exemple de définition du caractère national, nous mentionnons ci-dessous la définition générale des « produits originaires » telle qu'utilisée par les Douanes :

Sont considérés comme « produits originaires » :

- a) les biens extraits, récoltés, cultivés ou attrapés sur le territoire ou dans le pays en question ainsi que les produits de la pêche pêchés en mer au moyen de bateaux battant pavillon de ce pays ;*
- b) produits tels que visés au point a) ;*
- c) les biens qui ont été fabriqués dans le pays ou sur le territoire en question et dans lesquels sont intégrés des biens d'origine étrangère, à condition que ces biens aient subi, sur le territoire en question, un traitement tel que l'on peut accorder aux biens ainsi obtenus le caractère de biens originaires de ce pays ou territoire ;*
- d) les biens qui, à l'origine, ont été importés en tant que « produits originaires » de la CE et qui sont de nouveau exportés vers la CE.*

En ce qui concerne la définition de secret, il convient, selon moi, d'établir une distinction selon le point de vue que l'on adopte. Du point de vue des entreprises, cette définition sera davantage axée sur le commercial (savoir-faire, techniques de production, relation commerciale...). Par contre, du point de vue des autorités, elle sera davantage liée au respect des lois (informations confidentielles à fournir notamment aux parquets, aux greffes des cours, des tribunaux et de toutes les juridictions ; institutions ou établissements publics...). L'Administration des douanes et accises est confrontée aux deux aspects car les informations concernant l'importation, l'exportation et le transit de marchandises peuvent comprendre des données entrant en ligne de compte pour l'un des aspects ou pour les deux.

Dans le cadre de notre collaboration avec le Customs and Border Protection des États-Unis, nous avons veillé, en tant que douanes, à ce que toutes les informations concernant les flux de marchandises à contrôler soient fournies à nos services, tant dans le cadre de la CSI (Container Security Initiative), que dans le cadre de l'initiative « Megaports » (Second Line of Defense). C'est seulement à un stade plus avancé de l'enquête que sont partagées les informations concernant l'envoi en question.

Dans le cadre de la protection de la chaîne logistique, il est prévu que les 25 États membres de l'UE travaillent « sans papier » afin de faciliter l'échange de données. Le fait que 25 administrations des douanes vont être reliées par un réseau met au premier plan le problème de la protection des données. En outre, les Douanes adopteront davantage un rôle de « meneur de jeu » aux frontières extérieures pour les autres services de prévention et de répression. Il convient d'éviter, grâce à une transmission de données sécurisée, que des informations se retrouvent entre les mains de destinataires non autorisés.

La protection de la chaîne logistique et le contrôle en temps réel impliquent que les Douanes disposent d'informations sur les flux de marchandises, les flux de données liés aux flux de marchandises et les transactions financières, et ce, depuis le départ de l'envoi chez le fabricant jusqu'à l'arrivée chez le destinataire. Nous bénéficierons dès lors d'informations mondiales. Il s'agit d'une énorme mine d'informations commerciales. Cela pose un gros problème en matière de protection des fichiers dans lesquels ces données sont stockées. Il y a non seulement lieu d'éviter le vol de ces informations, mais également les manipulations au sein du système. »

3.2.7. Réponse de M. COOLS - professeur à la faculté de Droit de l'Université de Gand et le Vrije Universiteit Brussel (lettre du 13 mai 2005)

Le professeur COOLS a fait parvenir au Comité un texte intitulé « *les services de renseignement et le potentiel scientifique* »⁹ destiné à être publié dans un livre consacré à la Sûreté de l'État. Monsieur COOLS y affirme que la tâche de la Sûreté de l'Etat en cette matière est de sensibiliser, de conseiller et d'informer, le cas échéant via la *Plate-forme permanente de concertation pour la protection des entreprises* (PCPE) mise en place par la Fédération des Entreprises de Belgique (FEB).

L'auteur préconise que la Sûreté de l'Etat joue un rôle moteur dans l'élaboration d'une plate-forme de concertation analogue avec les services publics concernés par la recherche scientifique, les universités, les écoles supérieures, les entreprises privées innovantes à haute valeur ajoutée et les laboratoires de recherche. Et Monsieur COOLS de se référer au rapport Carayon en France ainsi qu'aux missions de la DST :

⁹ Cet article a été publié dans COOLS, M., 'Inlichtingendiensten en het wetenschappelijk potentieel', dans COOLS, M., DASSEN, K., LIBERT, R. et PONSAERS, P., (eds.), *La Sûreté. Essais sur les 175 ans de la Sûreté de l'Etat*, Bruxelles, Politeia, 2005, pp. 313-320.

« Dans l'article 7 de la Loi organique des services de Renseignement et de Sécurité, le législateur a donné à la Sûreté de l'État la mission de rechercher, d'analyser et de traiter le renseignement qui menace ou pourrait menacer le potentiel scientifique ou économique défini par le Comité ministériel.

Selon nous, le législateur a ainsi placé la Sûreté de l'État (SE) devant sa mission la plus difficile. La science est en effet une connaissance libératoire pour l'homme (l'humanité) et doit dès lors être disponible universellement dans un environnement ouvert et transparent. Compte tenu de ce raisonnement, protéger ces connaissances libératoires, veiller sur elles en les enfermant pourrait être contraire à l'intérêt de tous les individus. La SE servirait ainsi un intérêt non légitime pour l'individu.

Néanmoins, la science est irrévocablement liée à l'exercice du pouvoir politique et économique et elle est pratiquée par des individus et/ou des collectivités. Ceci peut nuancer le raisonnement précédent et légitimer l'intérêt de la SE dans cette matière. Mais cet intérêt légitime ne peut être justifié sans attribuer des droits de propriété à la science.

Lorsque la science est financée par les pouvoirs publics, elle relève, par définition, de la propriété de ces pouvoirs publics, ce qui génère alors l'intérêt légitime de la SE dans sa mission. Bien entendu, il en va différemment lorsque la science est financée par des acteurs privés en général et par l'industrie en particulier. Dans cette matière qui relève du droit de la propriété, les pouvoirs publics, et avec eux la SE, doivent s'abstenir de toute intervention, à moins que celle-ci ne soit explicitement sollicitée par les propriétaires. La mission la plus difficile pour la SE peut également devenir sa plus belle mission. Dans sa mission de sensibilisation, de conseil et d'information, elle peut contribuer à libération de l'individu. »

3.2.8. La Fédération des Entreprises de Belgique (FEB)

Bien que le Comité permanent R n'a pas reçu de réponse de la Fédération Belge des entreprises (FEB), on ne peut pas ne pas tenir compte du point de vue de cette fédération patronale. C'est la raison pour laquelle le Comité permanent R renvoie vers la contribution que Madame VEN, directrice du département économique de la FEB, a publiée précédemment¹⁰. Il y est expliqué la perception qu'à la FEB du potentiel économique et scientifique de notre pays ainsi que le rôle que peut jouer les services de renseignements belges d'après la FEB.

Les thèmes abordés par la consultation du Comité permanent R sont discutés au sein d'un groupe de travail de la «*Plate-forme de concertation permanente pour la protection des entreprises*» (PCPE) mise en place en 1995. Un protocole d'accord a été signé en décembre 2001 afin d'établir les bases de la collaboration entre le gouvernement fédéral et la FEB au sein de cette plate-forme de concertation.

¹⁰ VEN, C., 'Het belang van de inlichtingendiensten voor de bescherming van het wetenschappelijk en economisch potentieel van onze bedrijven', dans PETERMANN, S. et CLAES, W., *Les services de renseignements en Belgique et les nouvelles menaces*, Bruxelles, Politeia, 2005, p. 145 et dans le même sens STEENLANT, J. et VEN, C., 'Het belang van de inlichtingendiensten voor de bescherming van het economisch potentieel voor onze bedrijven', dans COOLS, M., DASSEN, K., LIBERT, R., et PONSAERS, P., o.c., p. 321 e.s.

L'économie belge est particulièrement dépendante des développements qui se produisent dans le reste de l'Union européenne. La Belgique a des relations économiques très étroites avec ses voisins directs mais aussi avec le reste du monde. Ces relations ne se limitent pas à des liens commerciaux, l'actionnariat de beaucoup d'entreprises y est en tout ou en partie détenu par des groupes étrangers. Le réseau Internet renforce cette tendance à la globalisation puisqu'il permet de trouver très facilement des partenariats étrangers.

« L'intérêt de la Recherche et du Développement ne peut manquer de figurer dans la description du potentiel scientifique et économique d'un pays. L'excellence dans la recherche et le développement constitue en effet une réponse à la concurrence des pays à faibles salaires ; elle nous permet de placer la productivité et le potentiel de développement à son plus haut niveau. (...)

D'autres ingrédients traditionnels comptent aussi à côté de la Recherche et du Développement, à savoir l'infrastructure du pays. Il s'agit bien sûr de ses transports et, plus généralement, de ses capacités logistiques telles que le réseau routier, les chemins de fer et, très important en Belgique, de ses installations portuaires.

Des réseaux industriels d'électricité et de télécommunication bien développés sont d'un intérêt capital pour le potentiel économique d'un pays. On peut encore compléter les ingrédients précités du potentiel scientifique et économique par une politique générale d'encadrement juridique et économique.

Pour que les entreprises puissent se développer et traduire leurs idées innovantes en croissance économique, profit et emploi, une politique économique de soutien doit être menée. L'esprit d'entreprise doit être stimulé, les charges sur les entreprises doivent être limitées au maximum et la sécurité juridique doit être assurée».

Selon Madame VEN, les services de renseignement peuvent jouer un rôle crucial dans la protection du potentiel scientifique et économique :

«La difficulté de définir leur rôle dans une libre économie de marché, caractérisée de surcroît par une globalisation croissante, ne doit pas certainement constituer un obstacle. Il faut bien sûr être attentif à ce que leur intervention soit conciliable avec les principes de base de la libre entreprise.

De même, la difficulté de collaborer avec des services étrangers, dont les intérêts nationaux ne sont pas nécessairement les mêmes que les nôtres, ne doit pas entraver leur action. Les principes de base du libre marché et de la dérégulation n'empêche aucunement que les services de renseignement jouent un rôle de soutien à la politique générale en avertissant des dangers potentiels.

Par leur analyse des tendances et des menaces actuelles, aussi bien nationales qu'internationales, ils contribuent grandement à la détermination des actions à entreprendre dans le cadre de la politique générale. »

Et Madame VEN de citer la mise en place en 2004 d'une procédure d'alerte rapide dans le cadre de la plate-forme permanente de concertation sur la sécurité des entreprises. Ce système permet de signaler des agissements suspects au sein d'entreprises dans le cadre de menaces terroristes. Ceci doit se passer d'une manière très confidentielle, selon que la menace concerne un secteur, une activité ou une entreprise spécifique. En cette matière, la confidentialité est une condition nécessaire de la bonne collaboration entre l'autorité et le secteur privé.

Madame VEN estime aussi que les services de renseignement pourraient créer une très grande valeur ajoutée en s'engageant dans des actions de sensibilisation du monde économique. Une information sur les menaces pouvant viser les entreprises ainsi que sur les moyens pour s'en protéger permet à celles-ci de mieux prendre leurs responsabilités concernant la sécurité de leurs intérêts économiques et scientifiques.

Il va de soi, selon Madame VEN, qu'une action efficace exige une meilleure collaboration entre services de renseignement nationaux. Un premier pas en ce sens pourrait être réalisé dans le cadre d'une future politique européenne de sécurité. La nature changeante des menaces et la montée du terrorisme offre déjà un terrain suffisant de collaboration. La représentante de la FEB plaide aussi pour une meilleure collaboration des services de renseignement avec les autorités judiciaires. Elle insiste également pour que la Sûreté de l'État dispose enfin de moyens suffisants pour exécuter sa mission. Enfin, un dialogue permanent doit s'instaurer entre la Sûreté de l'État et le secteur privé à propos de la manière dont ce service doit s'acquitter de sa mission de protection du potentiel scientifique et économique. Cette concertation est nécessaire pour connaître les besoins des entreprises et établir une analyse correcte des risques.

Et plus loin, Madame VEN d'insister sur l'importance de la sécurisation des réseaux de télécommunication, surtout pour les PME innovantes qui investissent énormément dans la R & D. Celles-ci sont vulnérables et peuvent être victimes des nouvelles menaces liées à l'informatique : virus, spam, vols de données, perte de confidentialité, sabotage du système informatique.... « *La sécurité informatique est un 'must' et les entreprises doivent en être rendues conscientes* ».

4. LE RAPPORT D'EXPERTISE

Le Comité permanent R a décidé (*supra*) de confier une mission d'expertise à Monsieur DE MESMAEKER. Monsieur DE MESMAEKER a remis son rapport au Comité le 28 décembre 2005. Le Comité permanent R reproduit ici quelques extraits parmi les plus significatifs de ce rapport.

«Cela fait déjà plusieurs années que le contenu exact de la définition par le Comité Ministériel du Renseignement et de la Sécurité fait l'objet de discussions. Il serait dès lors présomptueux d'affirmer qu'une brève étude pourrait rapidement apporter la solution. Aussi avons-nous choisi d'examiner de manière pragmatique en quoi ce PSE pourrait consister et, surtout, comment la Sûreté de l'État pourrait contribuer, éventuellement avec d'autres acteurs pertinents, à la protection du PSE. L'on constate d'emblée que de très nombreux points de vue et opinions existent en la matière. Bien que toutes ces sources aient abondamment contribué aux réflexions concernant le PSE, il convient de préciser que ce rapport ne reflète pas nécessairement la vision d'un ou de tous les acteurs consultés.

L'on peut entendre par « Potentiel Scientifique et Économique » (PSE) :

- *Potentiel scientifique : le savoir et le savoir-faire que l'on a pour faire « quelque chose »*
- *Potentiel économique : les structures et les moyens matériels dont on dispose pour réaliser « quelque chose »*

Un potentiel n'a cependant de sens que si on l'utilise réellement pour faire « quelque chose ». En d'autres termes, la finalité de l'utilisation du potentiel est importante.

Le site Web du SPF Justice (www.just.fgov.be) indique que la sauvegarde du PSE est l'une des tâches principales de la Sûreté de l'État, notamment la protection des valeurs fondamentales et des intérêts de l'État. Du point de vue des valeurs fondamentales et, surtout, des intérêts de l'État, nous pourrions affirmer, de manière pragmatique, que le PSE contribue à ces intérêts s'il est utilisé pour créer de la richesse matérielle, dans notre cas bien sûr en Belgique.

Nous pourrions définir cette richesse matérielle par le maintien, à long terme, et/ou la création d'une Valeur ajoutée et/ou d'Emplois en Belgique. En partie grâce aux mécanismes de redistribution, cette prospérité économique engendrera alors une hausse générale du bien-être social collectif. Cette conception élude dès lors la question, complexe et difficile, de savoir ce qu'est exactement une entreprise ou organisation « belge » (localisation du centre de décision ?, nationalité de la direction ?, nationalité des membres du conseil d'administration ?, origine du capital ?...), en affirmant que ce sont les bénéficiaires (à long terme) des activités économiques qui déterminent si une entité contribue de manière significative aux intérêts de l'État.

Nous pourrions dès lors définir le PSE belge de la manière suivante :

L'ensemble des connaissances, du savoir-faire, des structures et des moyens matériels qui permettent de générer une prospérité économique en maintenant de façon dynamique et à long terme une valeur ajoutée et des emplois.

Le terme « dynamique » signifie ici que l'on ne doit pas se concentrer sur une valeur ajoutée ou sur de l'Emploi individuel(le), mais qu'il convient de s'attacher à tout processus dynamique et naturel de perte et de création dont le résultat répond aux besoins.

Notons que, dans la description ci-dessus, la richesse matérielle doit profiter à la Belgique. Ce qui signifie également que les activités menées à l'étranger mais qui créent une valeur ajoutée en Belgique font partie du PSE belge.

En outre, il convient d'interpréter « l'intérêt belge » dans le sens large du terme et cela aussi bien géographique que temporel. Certains développements ne peuvent en effet avoir une influence positive ou négative qu'à long terme. Ceci ne signifie bien sûr pas que cela ne vaille pas la peine que la Sûreté de l'État s'y intéresse dès le départ. D'un point de vue géographique, les analyses économiques ne peuvent plus s'arrêter aux frontières de la Belgique, mais doivent évaluer la situation dans un contexte européen, voire mondial.

Les projets d'étude menés avec des partenaires étrangers peuvent dès lors donner lieu à un flux de connaissances utiles vers l'étranger. Tant que l'on obtient un équilibre général entre les flux entrant et sortant, ce mécanisme fait bien entendu partie des modalités d'une coopération. Il convient toutefois d'éviter qu'un trop grand déséquilibre (déficitaire) ne se forme et de veiller à ce que « la partie belge » soit au moins consciente de l'éventuel flux négatif.

Notons en marge que, dans un contexte belge, où les intérêts économiques sont de plus en plus régionalisés, l'on peut se demander si le PSE doit être examiné sous l'angle régional ou national.

La description susmentionnée peut certainement être affinée, adaptée et complétée, mais elle présente l'avantage d'être simple et de correspondre à la perception intuitive du concept.

La création à plus long terme d'une Valeur ajoutée et d'Emplois requiert tout d'abord plusieurs facteurs constitutifs et environnants que nous pourrions qualifier « d'infrastructure de base » :

- A. un environnement social structuré, ce qui signifie que l'État (ordre juridique, ordre public & sûreté, principales institutions...) doit fonctionner correctement ;*
- B. des équipements de base qui répondent aux besoins primaires (aliments et boissons, soins médicaux et assistance...);*
- C. des services disponibles, en termes d'équipements d'intérêt général (énergie, télécommunications, poste, transport, infrastructure financière...).*

Les entités économiques (ou d'autres entités économiques) qui génèrent des produits ou services spécifiques peuvent se développer sur cette infrastructure de base.

Le développement de ces entités économiques, évalué en termes de Valeur ajoutée et/ou d'Emploi, dépend ensuite fortement du savoir et du savoir-faire disponibles.

Remarquez qu'eu égard au point A, la protection des valeurs fondamentales et des intérêts de l'État, ainsi que le maintien de l'ordre démocratique et constitutionnel font déjà partie des tâches confiées à la Sûreté de l'État. Les points B et C relèvent, quant à eux, de ce que nous pouvons qualifier « d'Infrastructure Vitale ».

Pour Monsieur DE MESMAEKER, la protection du PSE par la Sûreté de l'État implique donc :

- la protection de l'infrastructure vitale du pays,
- la protection du Savoir et du Savoir-faire.

La manière dont la législation belge entend protéger l'Infrastructure Vitale du pays a déjà été examinée.

La protection du Savoir et du Savoir-faire

«Le Savoir et le Savoir-faire doivent également être protégés contre leur perte injuste ou résultant de la naïveté/négligence au profit d'une entité qui les utiliserait d'une manière qui générerait une richesse nulle ou moindre en Belgique.

Lorsque ce savoir et ce savoir-faire ont été accumulés grâce aux deniers publics, le gouvernement pourrait même imposer des mesures contraignantes en la matière. S'ils ont été acquis sans l'aide de l'État, toute mesure coercitive est bien sûr inadmissible et serait même contre-productive à l'égard des efforts que les organisations sont disposées à consentir en Belgique pour acquérir un savoir et un savoir-faire. Concernant ce dernier point, seul un incitant positif s'avérerait constructif ».

Et Monsieur DE MESMAEKER de préciser comme suit les notions de « savoir » et de « savoir-faire ».

« Le savoir et le savoir-faire sont à la base de la création des facteurs de prospérité économique « Valeur ajoutée » et « Emploi ». Ce savoir et ce savoir-faire peuvent prendre diverses formes :

- *résultats exploitables de recherches scientifiques ;*
- *maîtrise d'un processus de production ;*

- expérience dans l'optimisation de lignes d'assemblage ;
- connaissance des fournisseurs d'ingrédients fondamentaux de qualité supérieure ;
- connaissance de la problématique des clients ;
- connaissance du marché et de la concurrence ;
- connaissance des marchés de niche et identification des clients potentiels ;
- ...

Le savoir et le savoir-faire englobent donc les domaines scientifiques, techniques, technologiques et commerciaux. Ils n'ont toutefois de valeur que s'ils génèrent une richesse économique en créant, éventuellement à plus long terme, une Valeur ajoutée et/ou des Emplois.

Pour les entreprises, la somme de leur Valeur ajoutée et leur Emploi est déjà une indication de leur contribution à la prospérité économique. Cette approche doit toutefois être affinée. Ainsi, d'importants investissements en R & D (et ce, tant concernant l'infrastructure de recherche que les salaires des chercheurs) accroîtront la probabilité que la Valeur ajoutée et/ou l'Emploi se maintiennent ou augmentent dans le futur.

Ceci est d'autant plus vrai pour les universités, les centres de recherche, etc. dont le produit est principalement constitué de connaissances qui seront utilisées par d'autres organisations pour la production de Valeurs ajoutées et/ou d'Emplois.

Outre la « quantité » de Valeurs ajoutées et/ou d'Emplois fournis, il convient également de tenir compte de la « qualité » de ces facteurs. Plus l'on crée de valeur ajoutée avec les facteurs de production Travail et Capital, plus la productivité sera élevée et plus la spécialisation de l'Emploi sera de qualité

Un précédent rapport du Comité R mentionnait qu'au Canada, l'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.

En termes de choix techniquement ingénieux et de stratégie novatrice, cette productivité est donc également vitale pour la préservation, à plus long terme, des facteurs de prospérité économique que sont la Valeur ajoutée et l'Emploi. »

Monsieur DE MESMAEKER propose alors une méthode afin d'identifier les organisations importantes pour le PSE.

« Afin d'identifier les organisations qui contribuent ou contribueront de façon significative à la richesse économique, il s'avérerait utile de voir s'il est possible de tirer des conclusions pertinentes et surtout exploitables en se fondant sur un nombre restreint de paramètres, tels que :

- valeur ajoutée ;
- emploi ;
- productivité du Travail et du Capital ;
- spécialisation de l'emploi ;
- investissements en R & D ;

- appartenance ou non à l'Infrastructure Vitale (étant donné que la disparition de celle-ci peut avoir un impact direct sur de nombreuses autres organisations qui créent une richesse économique) ;
- ...

À cet égard, il est bien sûr important d'identifier les « grands acteurs » (en valeur absolue). D'autre part, l'on devrait également définir un prorata selon, par exemple, le Travail et/ou le Capital, afin de pouvoir identifier les organisations performantes de plus petite taille.

Cette méthode quantitative ne permet sans doute pas d'identifier des entités très petites qui disposent d'un Savoir ou d'un Savoir-faire prometteurs. Pour cela, une approche ad hoc serait peut-être mieux indiquée. Le Centre de Crise a déjà dressé une carte de l'Infrastructure Vitale dans sa base de données CRIVISEN. Une synergie est probablement envisageable. Le secteur privé est également prêt à collaborer à cet inventaire, dans le cadre du groupe de travail PSE de la Plate-forme de concertation permanente sur la protection des entreprises, où sont d'ailleurs déjà représentées la Sûreté de l'État et la Direction générale du Centre de crise.

En ce qui concerne l'identification des autres organisations qui contribuent considérablement au PSE, la méthode décrite ci-dessus peut sans doute être utilisée pour les acteurs de taille moyenne et grande. Pour les très petites entités, et nous pensons ici aux chercheurs entrepreneurs et aux spin offs à haute intensité de connaissances qui ne comptent qu'un nombre limité de collaborateurs, il peut être indiqué de sensibiliser sur une base plus large et adaptée et de laisser ces entités se révéler spontanément.

Nous pensons ici à des présentations faites par la Sûreté de l'État en collaboration, par exemple, avec les facultés de sciences ou de sciences appliquées des universités et hautes écoles, avec des associations d'ingénieurs (telles que la K.VIV ou la FABI, etc.). Grâce à des présentations de qualité et adaptées aux besoins de ces petites entités, elles répondront logiquement à l'invitation de se faire connaître et il sera alors possible d'avancer avec le groupe ainsi identifié ».

(...)

Le rôle de la Sûreté de l'État

« Le rôle premier de la Sûreté de l'État devrait dès lors consister à identifier les organisations pertinentes pour le PSE (parce qu'elles font partie de l'infrastructure vitale et/ou qu'elles disposent d'un savoir et d'un savoir-faire précieux), à les sensibiliser aux menaces potentielles et à les informer sur les mesures de précaution éventuelles.

En outre, il s'avérerait que la Sûreté de l'État entreprenne également des analyses de tendances afin d'informer le gouvernement et, avec l'accord de ce dernier, de sensibiliser les acteurs économiques pertinents. En matière d'analyses de tendances, la Sûreté de l'État peut collaborer avec des institutions spécialisées dans l'analyse économique et qui disposent de collaborateurs hautement spécialisés dans ce domaine. Nous pensons ici plus particulièrement à la Banque Nationale et au Bureau du Plan. L'apport de la Sûreté de l'État peut dès lors consister à (faire) examiner les tendances observées avec toute l'attention requise pour le PSE et avec une saine méfiance à l'égard des intentions dissimulées ou malveillantes.

Pour ce qui est des contacts avec les entreprises et organisations, la Sûreté de l'État travaille déjà en trois phases :

- sensibilisation par le biais de conseils et de contacts informels ;*
- contrôle dans le cadre de l'octroi d'habilitations de sécurité ;*
- réactivité en cas d'incidents.*

Cette approche pourrait être développée :

- 1. en identifiant les organisations pertinentes pour le PSE, comme indiqué ci-dessus. Notons qu'il s'agit d'un processus continu au cours duquel il faut sans cesse identifier de nouvelles entités. D'éventuelles priorités peuvent être définies en fonction des analyses de tendances susmentionnées et des phénomènes observés par le service.*

La Sûreté de l'État pourrait également mener une campagne d'information et de sensibilisation auprès des services de police locaux. La Police locale est en effet un témoin de premier ordre lors d'effractions, de vols et d'autres incidents qui peuvent dépasser le vol banal de biens matériels et viser l'obtention d'informations (c.-à-d. l'espionnage).

- 2. en demandant la désignation d'une personne de contact qui serait l'interlocuteur privilégié de la Sûreté de l'État dans chacune des organisations identifiées au point précédent (pour l'Infrastructure vitale, ces personnes de contact existent peut-être déjà et pour les organisations qui disposent d'habilitations de sécurité, il pourrait s'agir de l'Officier de sécurité).*
- 3. La Sûreté de l'État pourrait également désigner une personne de contact fixe et un auxiliaire fixe, de manière à donner un visage à la Sûreté de l'État auprès de ces organisations. Ces personnes devraient être joignables 24h/24 et devraient pouvoir nouer un contact personnel et une relation de confiance avec les organisations concernées. Sans cela, les organisations sont confrontées à un service impersonnel et la relation a peu de chance (voire aucune) de devenir productive.*
- 4. Une fois les personnes de contact connues de part et d'autre, une interaction peut s'enclencher où :*
 - la Sûreté de l'État informe régulièrement cette communauté sur les tendances, les modus operandi observés et donne des conseils appropriés ;*
 - les personnes de contact dans les organisations pertinentes pour le PSE peuvent établir une relation de confiance avec leur personne de contact au sein de la Sûreté de l'État et peuvent également leur signaler les incidents, les actes suspects... et demander conseil. »*

5. LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE À L'ÉTRANGER

5.1. En France

L'approche française se caractérise par la volonté de promouvoir le « *patriotisme économique* ». D'aucun critiquent cette nouvelle forme de « protectionnisme ».

L'article 410-1 du code pénal français inaugure le titre premier du livre IV « *des crimes et délits contre la nation, l'État et la paix publiques* ». Selon cette disposition, les intérêts fondamentaux de la nation se caractérisent par : son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine de ses institutions, les moyens de sa défense, sa diplomatie, la sauvegarde de sa population, l'équilibre de son milieu naturel et de son environnement, les éléments essentiels de son potentiel scientifique et économique et son patrimoine culturel.

Cet article ne donne pas de définition de la notion d'intérêts fondamentaux de la nation, se bornant à énumérer ses éléments constitutifs. L'article ne précise pas davantage ce que sont les éléments essentiels du potentiel scientifique et économique. L'ajout du patrimoine culturel permettrait d'étendre la protection du code pénal non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent la force ou la compétitivité du pays¹¹.

Les articles 411-5 à 411-8 définissent une série d'infractions relatives aux « *intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents* » et à la livraison d'informations à celles-ci.

Une circulaire du ministre de l'économie, des finances et de l'industrie datée du 14 février 2002 a pour objet de présenter les différents aspects de la défense économique et de décrire son organisation aux niveaux national, zonal, régional et départemental avec les responsabilités afférentes. Au même titre que la défense nationale et la défense civile, la défense économique constitue l'une des trois composantes de la défense de la Nation¹².

En décembre 2003, Monsieur ALAIN JUILLET, ex-numéro deux de la Direction générale de la sécurité extérieure (DGSE), a été nommé « *M. Intelligence économique* » auprès du premier ministre.¹³ Son rôle consiste à transformer l'État en « État stratégie ». Son premier objectif est d'insuffler un esprit d'intelligence économique à toutes les administrations. Son second objectif à plus court terme est d'établir une liste des secteurs économiques sensibles – essentiellement les industries et les services qui mettent en cause la souveraineté de l'État.

¹¹ VITU, A. dans « *Jurisclasseur pénal* » cité par le 13^{ème} rapport d'activité 2004 de la Commission nationale de contrôle des interceptions de sécurité (Observations sur le motif d'interception « protection économique » p. 65 e.s.).

¹² *Journal Officiel*, 23 mars 2002, n° 70, p. 5164.

¹³ Voir Titre 8 La composition et le fonctionnement du Comité permanent R, chapitre 5, point 5.

Les services de renseignement français

Les services de renseignement français ont une mission de service public qui est d'informer les autorités de l'État, non les intérêts privés. Les services de l'État n'ont pas à se substituer aux entreprises défaillantes qui négligent de mettre en place une cellule d'intelligence économique en leur sein.

L'Intelligence Économique est un concept qu'il appartient aux entreprises de mettre en œuvre, pas aux services de renseignement. Ceci n'empêche pas les uns et les autres de se rencontrer malgré les nombreuses barrières qui rendent ces rencontres difficiles : différence de cultures et de mentalité, sens du secret pour les uns, nécessité de communiquer pour les autres.

En France, c'est essentiellement la Direction de la Surveillance du Territoire (DST) qui a pour mission d'entretenir des contacts avec les entreprises. Depuis 1981, ce service accorde une assistance aux entreprises, aux labos et aux collectivités territoriales confrontées au phénomène de l'espionnage économique. Les missions de la DST dans cette matière sont le contre-espionnage, le contre-terrorisme, la protection du patrimoine et la lutte contre la prolifération.

Les contacts avec les entreprises et les chercheurs sont quotidiens. Ils consistent essentiellement en séances d'information et briefing de sensibilisation sur les dangers et vulnérabilités des labos et des entreprises (sécurité physique, fiabilité des personnes, sécurité des systèmes d'information...).

Cela représente quelque 600 conférences touchant +/- 35.000 personnes par an. Un véritable partenariat s'est établi avec les entreprises, les établissements d'enseignement supérieur et les labos. Les informations que la DST en retire (ponctuelles ou générales) remontent vers les ministères concernés.

Pour établir ses contacts avec les entreprises, la DST n'a pas défini de secteurs prioritaires. « Notre démarche est empirique » précise un commissaire de la DST. « *On approche les secteurs qui nous paraissent les plus ciblés par les SR étrangers. A partir de ces contacts, on essaye de conceptualiser les tendances. Dans l'avenir, nous devons peut-être donner la priorité aux secteurs sensibles défini par le gouvernement mais ces secteurs correspondent assez bien à ceux que nous couvrons jusqu'à présent* »¹⁴.

Sur le terrain, il y a collaboration avec les Renseignements Généraux et la Gendarmerie. La DST collabore aussi avec la Direction Générale de la Sécurité Extérieure. Ces services sont tous représentés au sein de la délégation générale à l'Intelligence Économique.

Les Renseignements Généraux informent l'État de toute menace ou de toute vulnérabilité via les préfets et le ministère de l'Intérieur. Les informations intéressant le monde des entreprises sont orientées vers la Délégation générale à l'Intelligence Économique. Les préfets sont chargés de la mise en œuvre des politiques régionales d'Intelligence Économique.

¹⁴ Intervention de M. PETRONILLE, commissaire de la DST aux rencontres "Innovation, Compétitivité et Connaissances" organisées à Paris les 28, 29 et 30 septembre 2005 par l'association SCIP France et Veille Magazine.

Le général GUYAUX, ancien directeur et conseiller scientifique de la DST explique comment la perception de la protection du patrimoine scientifique est passée au cours des années quatre-vingt-dix d'une vision « traditionnelle » de surveillance des individus à une conception plus globale de « sécurité des systèmes d'information ». ¹⁵

5.2. Aux Pays Bas

À la demande du gouvernement néerlandais, l'institut TNO¹⁶ a publié, en 2003, un rapport sur les infrastructures critiques aux Pays-Bas. Dans ce cadre, TNO identifie onze secteurs vitaux, représentant ensemble 31 produits ou services vitaux. Ces onze secteurs vitaux concernent essentiellement l'infrastructure de base du pays, c'est-à-dire les équipements de base répondant aux besoins primaires (aliments et boissons, soins médicaux et assistance...) ainsi que les services et équipements d'intérêt général (énergie, télécommunications, poste, transport, infrastructure financière...).

Le ministre de l'Intérieur a ainsi établi une liste confidentielle d'entreprises présentant un intérêt vital pour les Pays-Bas et dont l'« *Algemene Inlichtingen- en Veiligheidsdienst (AIVD)* » doit assurer la protection.

L'une des missions légales de l'AIVD est de favoriser des mesures de protection des données dont la confidentialité s'impose dans l'intérêt de l'État, des secteurs des pouvoirs publics et du monde économique et qui sont de l'avis des ministres compétents, d'un intérêt vital pour le maintien de la vie en société. Cette définition large des missions inclut la protection de l'économie nationale.

Dans ce cadre, l'AIVD enquête sur les activités des services de renseignement étrangers dirigées contre les intérêts économiques des Pays-bas. Dès sa création le AIVD 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 réalisation d'enquêtes de sécurité fait partie du processus de préservation de la sécurité. Les postes de confiance sont le dernier maillon de la chaîne des mesures de sécurité. Pour évaluer s'il est nécessaire de désigner une fonction de confiance, l'AIVD examine minutieusement l'ensemble de la sécurité d'une organisation.

Eu égard à la préservation de la sécurité, l'AIVD distingue quatre piliers :

- fourniture de renseignements particuliers ;
- secteurs vitaux ;
- intégrité de l'administration publique ;
- personnes et objets (internationaux) .

Pour pouvoir mettre en œuvre la préservation de la sécurité, l'AIVD dispose d'un certain nombre d'instruments :

- les avis de sécurité ;
- l'analyse des menaces ;
- l'encadrement lors des analyses de risques ;

¹⁵ GUYAUX, J., 'Sécurité informatique', 2003, avril, n° 44, disponible sur <http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num44.pdf>

¹⁶ Le *Nederlandse Organisatie voor Toegepast natuurwetenschappelijk Onderzoek (TNO)* est un institut de recherche néerlandais dont la vocation est de promouvoir l'exploitation pratique des connaissances scientifiques par les entreprises

- le “security scan”;
- le “security survey”;
- les enquêtes de sécurité.

Les produits finaux, obtenus à l'aide d'instruments tels que les avis de sécurité et les analyses de menaces, trouvent divers « destinataires ». Outre les acteurs gouvernementaux (gouvernement national, organisations internationales, police, OTAN...), l'AIVD compte également l'industrie parmi ses « clients ». La loi hollandaise sur les services de renseignement autorise aussi le AIVD 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 AIVD relative au domaine économique a été complétée comme suit :

- le contrôle sur le recueil par des services de renseignement étrangers de données économiques essentielles concernant des firmes néerlandaises;
- la détection des lancements de campagnes de presse calomnieuses dans le but de discréditer des entreprises néerlandaises.

Les Pays-Bas semblent donc avoir adopté une politique purement défensive mais qui associe de manière active le monde économique et le monde politique.

Comme la DST, l'AIVD situe essentiellement sa mission en matière de protection du potentiel scientifique et économique sur le plan préventif. Ce service associe aussi cette mission à la lutte contre la prolifération d'armes de destruction massive. Il tente donc de s'opposer à l'acquisition par des services de renseignement étrangers ou par des groupes terroristes, via le territoire néerlandais, de connaissances ou de matériels susceptibles de favoriser le développement de telles armes.

L'AIVD informe donc les secteurs économiques et scientifiques concernés sur la manière d'éviter de contribuer à la prolifération d'armes de destruction massive. Ainsi un rapport publié en décembre 2003¹⁷ met en garde les sociétés commerciales et industrielles ainsi que les institutions scientifiques néerlandaises. Ce document leur rappelle la responsabilité et les risques qu'elles courent si elles sont impliquées dans le détournement de technologies ou de connaissances utiles à la prolifération : sanctions pénales et risques d'atteinte à leur image et à leur réputation, pertes financières, etc. Viennent ensuite quelques indications utiles aux entreprises et aux institutions pour détecter les tentatives de détournement ou d'espionnage et d'identifier les situations à risque.

5.3. En Allemagne

Dans un entretien accordé au mensuel français “*Le Monde du Renseignement*”¹⁸, Monsieur FRISCH, le chef du “*Bundesamt für Verfassungsschutz*” (l'office de protection de la Constitution ou BfV) déclare que la notion de “*patrimoine économique stratégique*” a conduit son service à développer des collaborations avec certaines entreprises. 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.

¹⁷ « *Proliferation of weapons of Mass destruction, Risks for companies and scientific institutions* », disponible sur <http://www.fas.org/irp/world/netherlands/wmdrisks.pdf> Voir aussi: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Spionage, en veiligheidsrisico's; actueel, onzichtbaar en divers*, La Haye, 2005, 18 p. (www.aivd.nl).

¹⁸ *Le Monde du Renseignement*, n° 375, 3 février 2000.

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 für Verfassungsschutz*", c'est-à-dire les services de renseignement des länders.

Le BfV entretient des contacts avec des firmes et des institutions de recherche afin de les informer sur les programmes d'armement poursuivis par certaines puissances étrangères. Ce service indique quelles sont les technologies et les savoir-faire recherchés par les services de renseignement étrangers et sensibilise ses interlocuteurs sur les risques encourus lorsqu'ils sont en relation avec certaines firmes ou centres de recherche étrangers. Ainsi le département du contre-espionnage du BND ferait circuler une liste d'une quarantaine d'entreprises et d'organismes étrangers suspectés de participer à des dispositifs de renseignement technologique en Allemagne.¹⁹

5.4. En Grande Bretagne

La législation britannique 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)*"²⁰. 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 Committee*" du gouvernement, par la section économique du "*Joint Intelligence Committee*" et même par le Trésor et la Banque d'Angleterre. Les ministres concernés doivent désigner les entreprises clés pour l'économie britannique.

Ils donnent des directives par le canal du "*Joint Intelligence Committee*" (JIC). Ils demandent, par exemple, aux services de renseignement de s'informer sur la manière dont le prix du pétrole va varier de manière à permettre au ministre d'adapter sa politique financière.

Les services de renseignement travaillent donc pour l'État à qui ils diffusent les informations et non pour les entreprises directement. 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.

¹⁹ *Intelligence On Line* 2005, novembre, n° 511.

²⁰ "*Etude de la législation du Royaume-Uni relative aux services de renseignement et de sécurité*", dans Comité permanent R, *Rapport général d'activités 1998*, Bruxelles, 1999 (www.comiteri.be).

6. LE CONTRÔLE DES INVESTISSEMENTS ÉTRANGERS

6.1. En Europe

En Europe, hormis les Pays-Bas, la Belgique et l'Autriche, les États membres de l'Union européenne ont mis en place des dispositifs de contrôle des investissements étrangers en vue de garantir l'ordre public et la défense nationale. Divers événements survenus dans l'économie belge ont récemment fait ressurgir la question du contrôle des investissements étrangers dans notre pays.

Ainsi l'offre publique d'achat (OPA) du groupe français SUEZ sur Electrabel. Le contrôle d'une telle société stratégique par un groupe étranger ne met-il pas en péril l'indépendance énergétique du pays ? Qu'en est-il de l'indépendance de décision du gouvernement belge en cette matière, du contrôle des conditions de production et d'utilisation ?

On peut aussi évoquer la prise de contrôle par des fonds d'investissement étrangers de plusieurs PME belges qui ont développé des technologies de pointe notamment dans le secteur spatial. Selon Monsieur DE MESMAEKER : « *Alors que les menaces telles que le terrorisme et le sabotage sont clairement visibles et malveillantes, la reprise du contrôle d'une infrastructure vitale par un acteur étranger peut, par exemple, constituer une menace potentielle, surtout lorsque cette infrastructure vitale occupe une position dominante sur le marché. Un acteur étranger pourrait en effet torpiller une infrastructure vitale au détriment des intérêts nationaux, que ce soit par opportunité économique ou par une stratégie consciente* ».

Monsieur DE MESMAEKER estime qu'un petit pays à l'économie ouverte comme la Belgique doit se garder de tout comportement protectionniste contre-productif. Ce qui n'empêche pas, ajoute-t-il qu'une institution telle que la Sûreté de l'État devrait s'intéresser à de tels scénarios et signaler aux acteurs (gouvernementaux) concernés ces possibilités et, *a fortiori*, ces indices.

Si d'aucuns s'interrogent donc sur la mainmise de groupes étrangers sur un tel secteur stratégique ou sur une industrie de pointe du pays, d'autres considèrent au contraire que c'est tout à fait positif. Le « *patriotisme économique* » ne serait qu'une forme déguisée de protectionnisme et conduirait à une « *sanctuarisation* » de l'activité économique nationale.²¹ Reste qu'une réflexion semble indispensable sur les matières qui sont d'intérêt économique stratégique ou sur les sociétés qui représentent un atout inestimable pour la collectivité.

6.2. En France

L'exemple de la France semble intéressant à examiner. Depuis 1999, certaines prises de contrôle de fonds d'investissement américains (QinetiQ, Bofors Weapons, Gemplus, Danone....) dans certains secteurs de l'industrie européenne, notamment liés à la défense ont mené un certain nombre d'observateurs à se poser des questions.

²¹ DE SALLE, C. "Patriotisme économique : l'irrépressible pulsion protectionniste des États nations" , *La libre entreprise*, 24 septembre 2005.

En mars 2005, deux députés français, M. DEFLESSELLES (UMP, Bouches-du-Rhône) et M. MICHEL (PS, Puy-de-Dôme), ont rédigé un rapport sur « *La participation de capitaux étrangers aux industries européennes d'armement* ». ²² Ce document pointe notamment du doigt le parcours de certains cadres issus des services de renseignement américains. Un constat qui *"laisse à penser que ces derniers entretiennent des liens étroits avec la communauté du renseignement et l'administration américaine"*, notaient les députés.

Le ministère français de la défense a commandé une étude à sa Délégation aux Affaires Stratégiques (DAS) sur *"La stratégie des fonds d'investissement américains en Europe"*. Cette enquête, remise début juin 2005, a passé en revue un certain nombre d'opérations, et cherché à déterminer les critères de décision de ces fonds d'investissement. La question était de savoir si, oui ou non, ceux-ci sont *"les instruments de la politique géostratégique des États-Unis"*. ²³

L'étude indique qu'elle ne peut exclure a priori cette hypothèse, mais elle souligne que, faute de preuves avérées, elle est de l'ordre de la conjecture et qu'une logique strictement économique de maximisation du profit peut suffire à justifier ces mouvements -des fonds- vers des activités de défense. Selon Monsieur PAILLARD, chef du bureau prospective technologique et industrielle au sein de la DAS, l'étude *"n'a pu conclure sur l'existence d'une menace vis-à-vis de nos intérêts de défense"*.

Quoi qu'il en soit, l'attrait des américains pour les firmes européennes travaillant pour la défense est, *"indiscutablement stratégique pour l'Europe, qui y perd les moyens militaires de sa souveraineté et les capacités connexes de recherche et développement"*, prévient l'étude.

L'étude a identifié cinq critères qui semblent guider les décisions des fonds américains. Deux de ces critères sont assez classiques, concernant des investisseurs. Les fonds jouent ainsi le rôle de société de capital à risque vis-à-vis de "jeunes pousses" à fort potentiel dans des secteurs de pointe (nanotubes de carbone, gels de décontamination radioactive, acier à faible émission de CO2...). Ils convoitent aussi des entreprises mal gérées ou sous-valorisées dans le but de dégager une plus-value après restructuration.

Plus stratégique apparaît le critère d'*"anticipation de la demande américaine"*. *"Le partenariat public-privé est au cœur du dispositif d'intelligence économique des États-Unis"*, rappelle Monsieur PAILLARD.

Par leurs liens avec les élites politiques, administratives et financières américaines - voire, parfois, avec les services de renseignement -, les fonds d'investissement peuvent avoir une vision à long terme des besoins en équipement du *Department of Defense*, le ministère de la défense. *« Lorsque, sur un secteur donné du marché américain, ils estiment que la hausse de la demande va surpasser les capacités de l'offre, ils se repositionnent en conséquence. On peut donc logiquement déduire qu'il est possible d'anticiper les prochaines cibles des fonds d'investissement américains en Europe par un travail de veille quant aux évolutions majeures du marché américain. (...) Le marché de la sécurité intérieure connaissant une très forte dynamique de hausse aux États-Unis, (...) on peut s'attendre à des prises de contrôle sur ce secteur en Europe*", prédit aujourd'hui l'auteur de l'étude.

La constitution de véritables pôles sectoriels à partir d'une *"entreprise plate-forme"* et l'acquisition de *"banques de données et de vecteurs de communication"* sont les deux derniers critères d'investissement identifiés par l'étude.

²² DEFLESSELLES, . et MICHEL, J., *"La participation de capitaux étrangers aux industries européennes d'armement"*, Assemblée nationale, 2005, n. 2202.

²³ MANOU, Y., 'Les fonds américains irriguent l'industrie de défense européenne', *Le Monde*, 15 juillet 2005.

Pour conclure, le rapport de la DAS souligne que les fonds d'investissement américains contribuent largement, par leurs capitaux et leur action, à la modernisation de l'industrie de défense en Europe. *"L'Union européenne n'a pas le capital pour financer le développement de l'industrie civile et militaire ; il y a pénurie de capitaux, absence de fonds de pension, souligne-t-il. La vraie urgence serait de remodeler les marchés européens de capitaux."*

Le Journal Officiel de la République française a publié le 30 décembre 2005 un décret réglementant certains investissements étrangers en France.²⁴ Ce texte prévoit onze secteurs d'activités dans l'économie française dans lesquels un investissement étranger ne peut se réaliser sans une autorisation préalable du gouvernement : le secteur des jeux d'argent (au nom de la lutte contre le blanchiment d'argent), la sécurité, les biotechnologies et la production d'antidotes (au nom de la lutte anti terroriste), le matériel d'interception et de communications, la sécurité des systèmes informatiques, les technologies duales (c'est-à-dire pouvant être utilisées tant pour des applications civiles que militaires), la cryptologie, les marchés classifiés « secret défense » et l'armement.

Ce texte concerne toute entreprise française dans les secteurs considérés, qu'elle soit petite ou grande, cotée ou non cotée et quel que soit l'avis des actionnaires en place. Par contre, des secteurs tels que l'énergie, l'agroalimentaire ou la métallurgie ne figurent pas sur la liste. La presse rapporte que la Commission européenne est intervenue auprès du gouvernement français afin de limiter la portée du projet initial de décret, celui-ci ayant été jugé contraire aux règles communes de libre circulation des biens et des capitaux sur le marché européen²⁵. Certains redoutent aussi que l'effet pervers de ce décret soit de limiter les sources de financement des PME innovantes qui ont du mal à se développer dans un contexte économique difficile²⁶.

²⁴ Décret n° 2005-1739 du 30 décembre 2005 réglementant les relations financières avec l'étranger et portant application de l'article L. 151-3 du code monétaire et financier (http://lexinter.net/Legislation/decret_du_30_decembre_2005.htm)

²⁵ Notamment FOLLOROU, J., "La Commission européenne contraint le gouvernement à corriger son décret sur le patriotisme économique", *Le Monde*, 12 janvier 2006.

²⁶ KHAN, A., 'La France veut protéger dix secteurs jugés stratégiques', *Le Monde*, 2 septembre 2005.

6.3. Aux États-Unis

Aux États-Unis, le « *Committee on Foreign Investment in the United States* » (CFIUS) est chargé depuis 1975 de protéger douze secteurs dits stratégiques de l'économie américaine. Présidé par le secrétaire au trésor, ce comité rassemble treize agences du gouvernement américain.

Cette instance doit déterminer si l'acquisition d'une entreprise américaine par un propriétaire étranger « *menace d'affaiblir la sécurité nationale* ». En trente années d'existence, ce comité n'a cependant interdit qu'une seule transaction. Actuellement, le CFIUS ne s'oppose qu'à des investissements étrangers dans les technologies classifiées ou bien, interdites à l'exportation.

Plusieurs sénateurs américains voudraient réformer en profondeur ce comité et élargir sa mission à la défense des « *besoins à long terme des USA en matière d'énergie* » ainsi qu'à la « *sécurité économique* »²⁷.

7. SYNTHÈSE DES POINTS DE VUE RECUEILLIS

On peut synthétiser les réponses des différents interlocuteurs du Comité permanent R de la manière qui suit. Ces points de vue seront précédés par les positions développées par la Sûreté de l'État, dans la mesure où ce service s'est exprimé sur la question.

7.1. Comment définir les éléments essentiels du potentiel scientifique ou économique d'un pays comme la Belgique ?

7.1.1. Le point de vue de la Sûreté de l'État

La Sûreté de l'État a proposé que le potentiel économique du pays soit défini comme suit : « *l'infrastructure et le savoir-faire à protéger et à défendre susceptibles de promouvoir une augmentation relative et soutenue de la production du travail et du capital* » .

En ce qui concerne le potentiel scientifique, la Sûreté de l'État propose la définition suivante : « *l'infrastructure, la technologie et le savoir-faire à protéger et à défendre en matière de recherche et de développement qui sont les garants et le moteur de l'accroissement du stock de 'know-how' et qui génèrent des prestations réellement innovatrices* ».

La Sûreté de l'État préfère cependant la définition de secteurs et de domaines prioritaires à l'énumération nominative de structures et d'organisations économiques et scientifiques. Une telle énumération ne parviendrait jamais à être exhaustive et à rester actualisée. Il convient pourtant de dresser une liste de secteurs d'activités à protéger dans le domaine scientifique et économique. A cette fin, la Sûreté de l'État utilise trois critères : la valeur ajoutée, l'emploi, la capacité de réguler le marché et les connaissances « *kennis en marktregerend vermogen* ».

La Sûreté de l'État a donc proposé de considérer comme prioritaires les domaines d'activité suivants :

²⁷ X., 'Washington, contrôle des investissements étrangers', *Intelligence On Line*, 2005, novembre, n° 510, p. 5.

- les entreprises publiques autonomes (loi du 21 mars 1991) ;
- les organismes d'intérêt public (loi du 21 mars 1991) ;
- les entreprises vitales pour les besoins de la population (eau, gaz, électricité, carburant, transport...);
- les entités scientifiques et économiques qui déploient des activités innovantes d'une haute valeur ajoutée ou qui occupent une position concurrentielle élevée sur le marché mondial.

La Sûreté de l'État vise ici les entreprises, les centres de recherche publics ou privés, les universités, spin-off, hautes écoles, services publics ainsi que d'autres structures supranationales, internationales, fédérales et régionales qui développent des technologies de pointe. Sont notamment visés la technologie spatiale, l'aéronautique, la santé, l'énergie, l'informatique, les télécommunications, l'environnement, la biotechnologie, la chimie et le secteur nucléaire.

7.1.2. Les points de vue des interlocuteurs du Comité permanent R

Les points de vue des interlocuteurs du Comité permanent R peuvent être résumés comme suite :

- Monsieur VANDENBORRE (administration des douanes) : « On pourrait définir le potentiel scientifique comme la capacité des scientifiques à développer de nouvelles techniques et nouveaux produits dans les deux processus précités afin d'agir de façon plus effective et/ou plus efficace. (...) Les éléments essentiels du potentiel économique comprennent la capacité à produire des biens et des services ainsi que celle des opérateurs à participer au commerce international ».
- Monsieur DE BUYSER, (S.A. ASTRID) : « *Il est difficile de répondre à la question de savoir si l'infrastructure et le savoir-faire de cette société (ASTRID) doivent relever de la définition du « potentiel scientifique et économique du pays », étant donné l'absence d'une définition claire. Nous pouvons toutefois souligner son intérêt dans le cadre de la sécurité nationale* ». MARC DE BUYSER estime par conséquent que l'ensemble de l'infrastructure et des connaissances techniques de sa société doit bénéficier d'une protection particulière vu l'importance de ces différents systèmes pour la communication nécessaire des services de secours et de sécurité du pays.
- Madame VEN (FEB) : « *L'intérêt de la Recherche et du Développement ne peut manquer de figurer dans la description du potentiel scientifique et économique d'un pays. L'excellence dans la recherche et le développement constitue en effet une réponse à la concurrence des pays à faibles salaires ; elle nous permet de placer la productivité et le potentiel de développement à son plus haut niveau. (...) D'autres ingrédients traditionnels comptent aussi à côté de la Recherche et du Développement, à savoir l'infrastructure du pays. Il s'agit bien sûr de ses transports et, plus généralement, de ses capacités logistiques telles que le réseau routier, les chemins de fer et, très important en Belgique, de ses installations portuaires. Des réseaux industriels d'électricité et de télécommunication bien développés sont d'un intérêt capital pour le potentiel économique d'un pays.* »
- Monsieur DE MESMAEKER (expert du Comité) propose la définition suivante du PSE : « *L'ensemble des connaissances, du savoir-faire, des structures et des moyens matériels qui permettent de générer une prospérité économique par la création et le maintien dynamique à long terme d'une valeur ajoutée et d'emplois*».

7.2. Qui sont les moteurs de ce potentiel scientifique et économique ?

7.2.1. Le point de vue de la Sûreté de l'État

Pour la Sûreté de l'État, le moteur de l'économie, c'est la Recherche et le Développement.

7.2.2. Les points de vue des interlocuteurs du Comité permanent R

En ce qui concerne les moteurs du potentiel scientifique et économique, le Comité permanent R reprend les éléments les plus importants du point de vue de ces interlocuteurs .

- Monsieur VANDENBORRE, (administration des douanes), estime que ces moteurs peuvent notamment être les suivants : « un climat économique mondial favorable, des centres de recherche bien équipés, une tendance à l'innovation au sein de la population, la stimulation du climat des entreprises, de bonnes infrastructures et la création d'un environnement où les dernières techniques informatiques peuvent être exploitées et appliquées ».
- Monsieur QUADEN, (Banque nationale) : « *Le bon fonctionnement du système financier et des grandes infrastructures financières belges est indispensable à l'activité économique du pays et même au-delà de nos frontières, compte tenu de l'imbrication du système belge dans des réseaux internationaux, liée notamment à la localisation sur notre territoire de plusieurs infrastructures transfrontalières. (...) Leur protection ainsi que celle de la continuité du service qu'elles rendent devraient assurément être rangées au rang de priorité pour la préservation du potentiel économique du pays. (...) La Banque (nationale) est elle-même fortement impliquée dans la surveillance de ce domaine d'activité. Une de ses missions légales est en effet de contribuer à la stabilité financière et, à ce titre, elle est plus spécifiquement chargée de l'oversight des systèmes de paiements et de règlement titres* ».
- Monsieur QUADEN, cite les systèmes de paiement bancaires nationaux et internationaux tels que ELLIPS, CEC et NBB Clearing, ainsi que Banksys, Euroclear (y compris le CIK), SWIFT, Mastercard Europe et ISABEL. Il plaide également pour que l'on ne néglige pas certaines infrastructures privées essentielles telles que l'aéroport de Bruxelles-national sous le contrôle de BIAC.
- Selon Madame VEN (FEB), la protection du potentiel scientifique et économique du pays relève essentiellement d'une politique générale en matière économique, juridique et sociale. « *Pour que les entreprises puissent se développer et traduire leurs idées innovantes en croissance économique, profit et emploi, une politique économique de soutien doit être menée. L'esprit d'entreprise doit être stimulé, les charges sur les entreprises doivent être limitées au maximum et la sécurité juridique doit être assurée*».
- Pour Monsieur DE MESMAEKER (expert du Comité permanent R), la création à plus long terme d'une Valeur ajoutée et d'Emplois requiert plusieurs facteurs constitutifs et environnants qu'il qualifie d'« infrastructure de base » :
 - un environnement social structuré, ce qui signifie que l'État (ordre juridique, ordre public & sûreté, principales institutions...) doit fonctionner correctement ;
 - des équipements de base qui répondent aux besoins primaires (aliments et boissons, soins médicaux et assistance...) ;
 - des services disponibles, en termes d'équipements d'intérêt général (énergie, télécommunications, poste, transport, infrastructure financière...).

L'État a aussi d'autres possibilités de stimuler le PSE par la création d'un climat économique favorable, d'un régime financier stimulant afin d'attirer les chercheurs étrangers, des incitations à convertir des résultats de recherches scientifiques utilisables en un produit ou service... .

7.3. Quelles menaces visent ce potentiel scientifique et économique ?

Le Comité permanent R a eu son attention attirée par cet avertissement donné à la Belgique par la Commission européenne le 12 janvier 2006²⁸ . Même si elle figure aujourd'hui à la sixième place des pays le plus innovant au sein de l'Union européenne, la Belgique pourrait perdre à l'avenir cette position en raison d'investissements insuffisants en recherche et développement, du désintérêt pour les études scientifiques, ainsi que de la faiblesse du capital à risque dans notre pays.

La Belgique arrive en sixième place, derrière la Suède, la Finlande, la Suisse, l'Allemagne et le Danemark, en tête d'un groupe de pays dont les performances en matière d'innovation sont jugées « moyennes » par la Commission. « *En termes de tendance de performance, la Belgique est en retard pour la moitié des indicateurs, ce qui laisse présager des problèmes* », avertit le rapport.

Celui-ci met le doigt sur la faiblesse des investissements publics et privés en matière de recherche et développement (R & D). Le désintérêt pour les études scientifiques, l'insuffisance des dépenses dans les technologies de l'information et de la communication, de même que la timidité du capital à risque sont d'autres facteurs défavorables cités par la Commission européenne.

7.3.1. Le point de vue de la Sûreté de l'État

La Sûreté de l'État identifie les menaces suivantes :

- les activités émanant de groupements idéologiques, sectaires, terroristes ou criminels ;
- les attentats ou sabotages visant la destruction physique d'infrastructures ;
- la déstabilisation de l'économie par la corruption, le blanchiment et l'introduction de capitaux provenant d'activités criminelles ;
- les activités clandestines de puissances étrangères (l'espionnage économique) ou d'entreprises étrangères (l'espionnage de concurrence) qui peuvent nuire aux intérêts belges dans le domaine scientifique et économique ;
- les activités commerciales de recueil, de traitement et d'analyse d'informations (ou courtage d'informations) qui peuvent porter atteinte au potentiel scientifique et économique ;
- la fabrication et la diffusion d'informations comme moyen de désorganisation dans les secteurs d'activité d'intérêt essentiel pour le bon fonctionnement des institutions fédérales et régionales, les universités, les écoles supérieures, les institutions de recherche et les entreprises : ceci vise les campagnes organisées de désinformation et d'influence (le lobbying) dans le but de porter atteinte au potentiel scientifique et économique ;

²⁸ Chaque année, la Commission européenne présente un rapport annuel qui évalue les progrès réalisés par chaque pays membre vers la mise en oeuvre des objectifs du sommet de Lisbonne en mars 2000. Les chefs d'États et de gouvernements y avaient décidé de faire de l'UE l'économie de la connaissance la plus innovante d'ici 2010 (X., "La Belgique tancée par l'Europe", *La Libre Belgique*, 13 janvier 2006).

- le site Web du SPF Justice mentionne également « *les tentatives étrangères de contrefaçon de la haute technologie qui procure à la Belgique un avantage économique sur d'autres pays* ».

La Sûreté de l'Etat fait référence à la situation canadienne.

L'espionnage économique est défini comme étant 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.²⁹

L'espionnage de concurrence (qu'on appelait autrefois espionnage industriel) est défini comme 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.³⁰

La Sûreté de l'État estime que l'espionnage de concurrence entre deux entreprises belges ne fait pas partie de ses compétences³¹ mais elle reconnaît que la frontière entre entreprises belges et non belges est souvent difficile à déterminer vu que beaucoup d'entreprises ont à présent un caractère multinational. L'intérêt pour une affaire devra donc être examiné au cas par cas.

Les membres du personnel d'une entreprise peuvent aussi être des cibles potentielles s'ils ont connaissance de secrets de fabrication, d'informations sensibles ou stratégiques ou encore d'inventions à haute valeur ajoutée. Ces personnes pourraient être les victimes de chantages, d'agressions ou d'usurpations d'identité.

7.3.2. Les points de vue des interlocuteurs du Comité permanent R

- Monsieur VANDENBORRE, (administration des douanes) : « Pour le moment, les plus grosses menaces se situent au niveau du terrorisme et de la sécurité mondiale. Toutefois, les menaces ne se limitent pas aux aspects purement terroristes mais comprennent également les aspects économiques, sociaux et environnementaux. Outre ces menaces générales, chaque participant à la vie économique peut également être confronté à des menaces liées à sa situation spécifique en raison, par exemple, d'une concurrence déloyale à la suite d'un abus de son savoir-faire, de secrets commerciaux, de relations commerciales, etc. L'obtention d'informations sur un procédé commercial spécifique par des concurrents peut avoir un impact négatif sur la position d'une entreprise sur le marché, entraînant une faillite dans le pire des cas, et peut donc nuire au potentiel économique d'un pays ».
- Monsieur POULLET, (CRID NAMUR) : « *Les risques liés à la digitalisation de l'information et à sa circulation sur des infrastructures de communication constituent une préoccupation importante vu les possibilités pour des puissances étrangères de capter de tels messages.* »
- Monsieur DE MARET, (ULB) : « *Le 'hacking' et le vol en vue d'obtenir des informations confidentielles sur des collaborations industrielles doit être évalué.* »

²⁹ Cette définition est celle donné par le Service canadien de Renseignement de Sécurité, dans "Série d'aperçus", 1998, mai, n° 6.

³⁰ *Idem.*

³¹ Voir Comité permanent R, *Rapport général d'activités 2000*, Bruxelles, 2001, chapitre 7, page 117 (www.comiteri.be).

- Madame VEN insiste elle aussi sur les menaces qui visent les réseaux de télécommunication, surtout pour les PME innovantes qui investissent énormément dans la R&D: virus, spam, vols de données, perte de confidentialité, sabotage du système informatique, etc. « *La sécurité informatique est un 'must' et les entreprises doivent en être rendues conscientes* ».
- La littérature consultée par le Comité permanent R confirme à ce propos que le patrimoine scientifique des laboratoires de la planète est souvent stocké dans les mémoires d'ordinateurs très vulnérables à des attaques ciblées ou aux virus. Ces mémoires constituent une immense bibliothèque mondiale mal protégée. La protection du potentiel scientifique se doit donc d'être attentive à la sécurisation des systèmes informatiques et des réseaux d'informations.
- Pour Monsieur DE MESMAEKER (expert du Comité), « *alors que les menaces telles que le terrorisme et le sabotage sont clairement visibles et malveillantes, la reprise du contrôle d'une infrastructure vitale par un acteur étranger peut, par exemple, constituer une menace potentielle, surtout lorsque cette infrastructure vitale occupe une position dominante sur le marché. Un acteur étranger pourrait en effet torpiller une infrastructure vitale au détriment des intérêts nationaux, que ce soit par opportunité économique ou par une stratégie consciente.* ».

7.4. A quelles difficultés se heurte la protection du potentiel économique et scientifique de notre pays ?

- Selon Madame VEN (FEB), la difficulté de définir le rôle des services de renseignement dans une libre économie de marché, caractérisée de surcroît par une globalisation croissante, ne doit pas certainement constituer un obstacle à leur action. Il faut bien sûr être attentif à ce que leur intervention soit conciliable avec les principes de base de la libre entreprise. De même, la difficulté de collaborer avec des services étrangers, dont les intérêts nationaux ne sont pas nécessairement les mêmes que les nôtres, ne doit pas non plus entraver leur action.
- Monsieur VANDENBORRE, (administration des douanes) : « *En ce qui concerne les problèmes de protection du potentiel scientifique et économique, l'on peut dire ce qui suit du point de vue des Douanes :*
 - *En raison du flux croissant de marchandises, il est devenu difficile de réaliser des contrôles efficaces sans perturber les flux commerciaux légitimes.*
 - *Des mesures peuvent être facilement appliquées aux flux de marchandises en vue de protéger le potentiel scientifique et économique mais si ces menaces découlent d'une opération non liée à des marchandises, telle que la diffusion et le transfert de connaissances, l'impact est beaucoup plus faible ».*

7.5. Comment attribuer un caractère national au potentiel scientifique et économique du pays ?

7.5.1. Le point de vue de la Sûreté de l'État

Entre autre dans une interview³² avec l'administrateur général de la Sûreté de l'État, rappelant que son service ne bénéficiait pas encore d'une définition claire de la notion de patrimoine économique et scientifique, posait notamment la question suivante : « *Devons-nous défendre une entreprise étrangère dont le siège est en Belgique ?* »

Où les intérêts et investissements de sociétés belges à l'étranger ? Il y a là un manque de clarté qui doit être comblé par le politique. » L'administrateur général envisageait enfin que dans quelques années, la défense des intérêts économiques des États pourrait être gérée au niveau européen et non plus national.

7.5.2. Les points de vue développés par les interlocuteurs du Comité permanent R

- Pour Madame VEN (FEB), la Belgique est un petit pays très ouvert au cœur de l'Europe. Cette situation rend son économie particulièrement dépendante des développements qui se produisent dans le reste de l'Union européenne. La Belgique a des relations économiques très étroites avec ses voisins directs mais aussi avec le reste du monde. Ces relations ne se limitent pas à des liens commerciaux, l'actionnariat de beaucoup d'entreprises y est en tout ou en partie détenu par des groupes étrangers. Le réseau Internet renforce cette tendance à la globalisation puisqu'il permet de trouver très facilement des partenariats étrangers.
- La Fédération des Entreprises de Belgique (FEB) considère 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.
- Monsieur QUADEN, (Banque nationale) : « *L'économie belge est caractérisée par un degré d'ouverture considérable et sa capacité à attirer ou retenir des investissements étrangers est déterminante pour l'évolution de sa prospérité, et notamment de l'emploi dans notre pays. De ce point de vue, la capacité des autorités à assurer un bon niveau de sécurité économique peut jouer un rôle dans la décision de localiser une activité en Belgique plutôt qu'ailleurs* ». M. QUADEN se rallie donc au point de vue exprimé par la Fédération des entreprises de Belgique selon lequel doit être considérée comme belge toute entreprise implantée sur le territoire national et qui y crée de la valeur ajoutée, quelle que soit la nationalité de ses actionnaires ou de ses dirigeants.
- Pour Monsieur VANDENBORRE, (administration des douanes), le caractère national d'un bien est subordonné à son caractère communautaire européen.

³² X., 'Interview avec l'administrateur général Dassen', *l'Écho*, 5 juin 2003,

- Monsieur DE MESMAEKER (expert du Comité) affirme de manière pragmatique que le PSE est national s'il contribue à créer de la richesse matérielle en Belgique. « Cette conception élude dès lors la question (complexe et difficile à répondre) de savoir ce qu'est exactement une entreprise ou organisation « belge » (localisation du centre de décision ?, nationalité de la direction ?, nationalité des membres du conseil d'administration ?, origine du capital ?...), en affirmant que ce sont les bénéficiaires (à long terme) des activités économiques qui déterminent si une entité contribue de manière significative aux intérêts de l'État. (...) Ce qui signifie également que les activités menées à l'étranger qui créent une valeur ajoutée en Belgique font partie du PSE belge. En outre, il convient d'interpréter « l'intérêt belge » dans le sens large du terme et sous un angle spatio-temporel. (...) Notons que, dans un contexte belge, où les intérêts économiques sont de plus en plus régionalisés, l'on peut se demander si le PSE doit également être examiné sous cet angle. »

7.6. Comment définir le secret en matière économique, scientifique et technologique et situer sa place dans une économie caractérisée par les mutations technologiques, la circulation de l'information et son ouverture internationale ?

- Monsieur VANDENBORRE, (administrations des douanes) DISTINGUE LE POINT DE VUE DES ENTREPRISES ET CELUI DES AUTORITÉS : « Du point de vue des entreprises, cette définition sera davantage axée sur le commercial (savoir-faire, techniques de production, relation commerciale, etc.). Par contre, du point de vue des autorités, elle sera davantage liée au respect des lois (informations confidentielles à fournir notamment aux parquets, aux greffes des cours, des tribunaux et de toutes les juridictions ; institutions ou établissements publics...). L'Administration des douanes et accises est confrontée aux deux aspects car les informations concernant l'importation, l'exportation et le transit de marchandises peuvent comprendre des données entrant en ligne de compte pour l'un des aspects ou pour les deux ».
- Le professeur COOLS (Université de Gand et la Vrije Universiteit Brussel) et le recteur VAN CAMP (VUB) estiment que la recherche scientifique universitaire doit en principe pouvoir être valorisée dans l'intérêt de la communauté. La publication de recherches financées par les autorités publiques peut toutefois être reportée si leur produit fait l'objet de droits de propriété intellectuelle. Cette protection doit permettre aux universités de recevoir une indemnisation équitable en cas de valorisation de leurs découvertes. Une gestion relativement close des recherches dotées d'un potentiel scientifique et/ou économique peut s'effectuer dans l'intérêt de la nation.
- Cette conception rejoint celle de Monsieur DE MESMAEKER qui estime que lorsque le savoir et le savoir-faire ont été accumulés grâce aux deniers publics, le gouvernement doit être autorisé d'imposer des mesures contraignantes en la matière. Par contre « S'ils ont été acquis sans l'aide de l'État, toute mesure coercitive est bien sûr inadmissible et serait même contre-productive à l'égard des efforts que les organisations sont disposées à consentir en Belgique pour acquérir un savoir et un savoir-faire. Concernant ce dernier point, seul un incitant positif s'avérerait constructif. »

7.7. Comment la Sûreté de l'État doit-elle prendre sa mission en charge dans cette matière ?

7.7.1. Le point de vue de la Sûreté de l'État

La Sûreté de l'État estime devoir orienter son action prioritaire sur la protection des « connaissances vulnérables ». Le 31 mai 2001, la Sûreté de l'État a adressé une note au Comité ministériel du renseignement et de la sécurité. Ce document contenait une série de propositions relatives à la définition du potentiel scientifique et économique, à l'établissement de priorités, à la détermination des menaces qui visent ce potentiel, ainsi qu'une description des missions qui devaient incomber à la Sûreté de l'État en cette matière.

Outre la recherche, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou qui pourrait menacer les éléments du potentiel économique et scientifique, la Sûreté de l'État se proposait de collaborer et d'échanger des informations en la matière avec les autorités judiciaires, les administrations fédérales, les entreprises privées et les particuliers, conformément aux articles 14, 16 et 19 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

A cet égard, la Sûreté de l'État se déclarait disposée à mener des actions de sensibilisation à l'égard des victimes potentielles en participant, par exemple, à des forums de concertation et d'information avec les autorités chargées de leur protection. La Sûreté pourrait ainsi présenter des analyses globales et des évaluations de la menace ou procéder à la prévention et au traitement de cas ponctuels.

Un rapport interne de la Sûreté de l'État daté du 20 septembre 2001 conclut que sa mission principale en matière de protection du potentiel scientifique et économique doit être essentiellement d'ordre préventif : il s'agit de connaître les détenteurs de « connaissances vulnérables » (« *kwetsbare kennis* ») et de les sensibiliser à l'égard des menaces d'appropriation qui peuvent se produire à leur rencontre.

«La Sûreté de l'État doit se positionner comme une institution vigilante de sensibilisation. Elle doit donc évoluer et s'insérer dans les structures existantes qui ont été mises en place dans le tissu économique en vue de soutenir et de canaliser le caractère innovant des activités scientifiques et économiques (les connaissances vulnérables). C'est ainsi qu'elle peut rester en phase avec la notion évolutive de potentiel économique et scientifique. De plus, elle occupe une place stratégique pour se tenir informée des besoins éventuels et remédier aux problèmes ».

Dans l'interview déjà mentionnée, l'administrateur général de la Sûreté de l'État situe les trois missions de la Sûreté de l'État en cette matière de la manière suivante :

- Une mission d'avertissement des autorités d'un éventuel danger lié aux intérêts économiques et scientifiques ; et Monsieur DASSEN de souligner à cet égard que la privatisation d'infrastructures comme les égouts ou l'électricité, qui sont susceptibles de passer aux mains d'étrangers, n'est pas sans risque ;
- Une mission de prévention et de stimulation de la vigilance à l'égard des autorités régionales et des universités de manière à ce que les attitudes de préservation de la confidentialité de la Recherche et Développement deviennent une habitude ;
- Une mission d'enquête à l'égard des actes criminels qui ont été commis en la matière.

Dans un article³³, Monsieur ROBIN LIBERT, Conseiller général et Directeur de l'analyse à la Sûreté de l'État, précise que cette mission d'avertissement et de prévention peut notamment porter sur :

- la sécurité en ce qui concerne le personnel,
- la protection physique,
- la sécurisation des matières classifiées, des communications et du courrier électronique.

Et même, la Sûreté de l'État a aussi pour tâche de signaler des manœuvres de concurrence déloyale ou des tentatives d'infiltrations d'organisations criminelles. Monsieur LIBERT évoque la possibilité de fournir aux entreprises des informations sur des personnes. Mais il reconnaît aussitôt que l'exploitation de ce type d'information n'est pas encore juridiquement encadrée. Monsieur LIBERT évoque également la fourniture de conseils juridiques et l'assistance spécialisée aux membres du personnel qui feraient l'objet de pressions ou d'agressions afin d'en soutirer de l'information. Il propose également d'élargir le champ des enquêtes de sécurité au personnel des entreprises essentielles pour l'intérêt général, par exemple celles visées par la directive SEVESO.

7.7.2. Les points de vue développés par les interlocuteurs du Comité permanent R

- Selon le professeur COOLS, (Université de Gand et Vrije Universiteit Brussel), la Sûreté de l'État doit, par principe, s'abstenir de toute intervention susceptible de restreindre la diffusion de connaissances scientifiques dès lors que celles-ci contribuent à l'épanouissement de l'humanité. L'intervention de ce service ne peut se justifier que si la recherche scientifique est financée par les pouvoirs publics d'une part, est couverte par un droit de propriété intellectuelle. Si la recherche est financée par des fonds privés, la Sûreté de l'État ne pourrait intervenir qu'à la demande des « propriétaires ».
- Le recteur VAN CAMP (VUB) situe aussi l'intervention de la Sûreté de l'État dans le domaine de la protection de la propriété intellectuelle, des procédures de brevet de l'université et de l'accès au campus.
- Monsieur VANDENBORRE (administration des douanes) insiste sur la nécessité de l'information pour son service : *« la protection de la chaîne logistique et le contrôle en temps réel impliquent que les douanes disposent d'informations sur les flux de marchandises, les flux de données liées aux flux de marchandises et les transactions financières, et ce, depuis le départ de l'envoi chez le fabricant jusqu'à l'arrivée chez le destinataire »*.

³³ LIBERT, R., "De vrijwaring van het Wetenschappelijke en Economische Potentieel" dans PETERMANN, S. et CLAES, W. (eds.), *Les services de renseignements en Belgique et les nouvelles menaces*, Politeia, Bruxelles, p. 145 e.s.

- Selon Madame VEN (FEB), les services de renseignement peuvent jouer un rôle crucial dans cette matière : *«La difficulté de définir leur rôle dans une libre économie de marché, caractérisée de surcroît par une globalisation croissante, ne doit pas certainement constituer un obstacle. Il faut bien sûr être attentif à ce que leur intervention soit conciliable avec les principes de base de la libre entreprise. De même, la difficulté de collaborer avec des services étrangers, dont les intérêts nationaux ne sont pas nécessairement les mêmes que les nôtres, ne doit pas entraver leur action. Les principes de base du libre marché et de la dérégulation n'empêche aucunement que les services de renseignement jouent un rôle de soutien à la politique générale en avertissant des dangers potentiels. Par leur analyse des tendances et des menaces actuelles, aussi bien nationales qu'internationales, ils contribuent grandement à la détermination des actions à entreprendre dans le cadre de la politique générale.»*

Comme déjà mentionné, Madame VEN cite la mise en place d'une procédure d'alerte rapide dans le cadre de la plate-forme permanente de concertation sur la sécurité des entreprises. Ce système permet de signaler des agissements suspects au sein d'entreprises dans le cadre de menaces terroristes. Ceci doit se passer d'une manière très confidentielle, selon que la menace concerne un secteur, une activité ou une entreprise spécifique. En cette matière, la confidentialité est une condition nécessaire de la bonne collaboration entre l'autorité et le secteur privé.

Elle estime aussi que les services de renseignement pourraient créer une très grande valeur ajoutée en s'engageant dans des actions de sensibilisation du monde économique. Une information sur les menaces pouvant viser les entreprises ainsi que sur les « trucs » pour s'en protéger permet à celles-ci de mieux prendre leurs responsabilités concernant la sécurité de leurs intérêts économiques et scientifiques.

Il va de soi, selon Madame Ven, qu'une action efficace exige une meilleure collaboration entre services de renseignement nationaux. Un premier pas en ce sens pourrait être réalisé dans le cadre d'une future politique européenne de sécurité. La nature changeante des menaces et la montée du terrorisme offre déjà un terrain suffisant de collaboration.

- Selon Monsieur DE MESMAEKER, *«le rôle premier de la Sûreté de l'État devrait dès lors consister à identifier les organisations pertinentes pour le PSE (parce qu'elles font partie de l'infrastructure vitale et/ou qu'elles disposent d'un savoir et d'un savoir-faire précieux), à les sensibiliser aux menaces potentielles et à les informer sur les mesures de précaution éventuelles. En outre, il s'avérerait utile que la Sûreté de l'État entreprenne également des analyses de tendances afin d'informer le gouvernement et, avec l'accord de ce dernier, de sensibiliser les acteurs économiques pertinents. En matière d'analyses de tendances, la Sûreté de l'État peut collaborer avec des institutions spécialisées dans l'analyse économique et qui disposent de collaborateurs hautement spécialisés dans ce domaine. Nous pensons ici plus particulièrement à la Banque nationale et au Bureau du plan. L'apport de la Sûreté de l'État peut simplement consister à (faire) examiner les tendances observées avec toute l'attention requise pour le PSE et avec une saine méfiance à l'égard des intentions dissimulées ou malveillantes.»*

8. CONCLUSIONS

8.1. Les conclusions du rapport d'expertise

« En réponse à la question concernant la manière dont le comité ministériel du renseignement et de la sécurité pourrait définir les éléments essentiels du potentiel scientifique et économique (PSE), nous pouvons citer :

- un objectif fondamental de l'État réside dans le souci de préserver le bien-être social collectif de la population belge ;
- ce bien-être social collectif est notamment atteint en appliquant les mécanismes de redistribution à la richesse économique générée ;
- la richesse économique résulte de la production de valeur ajoutée et d'emplois ;
- cette valeur ajoutée et ces emplois résultent, pour leur part, de l'activation du potentiel scientifique et économique ;
- les principaux composants du potentiel scientifique et économique sont :
 - *l'infrastructure sociale et économique vitale,*
 - *l'exploitation économique du Savoir et du Savoir-faire,*
- en matière de protection du PSE, la Sûreté de l'État s'intéressera de préférence aux actions malveillantes clandestines et ciblées à l'encontre de ce PSE ;
- d'un point de vue pratique, la Sûreté de l'État pourrait entreprendre :
 - *des analyses de tendances, afin d'informer l'État et, avec l'accord de ce dernier, de sensibiliser les acteurs économiques pertinents,*
 - *l'édification d'un réseau relationnel avec les organisations pertinentes pour le PSE, avec pour objectif :*
 - *la sensibilisation*
 - *l'information*
 - *la surveillance et le contrôle concernant les matières régies par la loi.*

Parmi les facteurs de réussite clés lors de la mise en œuvre de cette stratégie de protection, citons :

- une approche constructive :
 - *à l'exception des habilitations de sécurité qui ont bien sûr un caractère coercitif, le rôle de la Sûreté de l'État doit être ressenti comme pertinent et comme un service par tous les acteurs, et surtout par les acteurs non gouvernementaux ;*
 - *une approche contraignante ou bureaucratique aurait un effet contre-productif, surtout dans une économie ouverte*

- une bonne intégration et une collaboration avec les structures existantes :
 - *en matière d'analyses de tendances, il convient d'exploiter au maximum l'expertise existante (Banque nationale, Bureau du plan, entreprises, partenaires sociaux...)*
 - *lors de l'établissement et l'exploitation du réseau relationnel, il convient de collaborer au mieux avec les structures existantes. Du côté de l'État, il s'agit principalement du Centre de Crise, du SGRS... Du côté des entreprises, la Plateforme de concertation permanente sur la protection des entreprises aujourd'hui institutionnalisée constitue un instrument prêt à l'emploi. À partir de là, d'autres acteurs professionnels peuvent également être approchés, notamment : la communauté des ingénieurs, les responsables de Sécurité, les juristes d'entreprise, les auditeurs internes, les gestionnaires de risques... »*

8.2. Les conclusions du Comité permanent R

On rencontre les notions de potentiel scientifique et économique ou de potentiel socio-économique dans différents textes de lois et arrêtés royaux. Sans être autrement définies, ces notions s'inscrivent parmi d'autres intérêts fondamentaux de la Nation ou de la population dont l'État entend se porter garant.

Ces notions témoignent de secteurs d'activités du secteur privé sur lesquels l'État cherche à conserver une certaine maîtrise dans l'intérêt général. À côté de l'ordre public, la tranquillité, la salubrité et la sécurité publique, la souveraineté nationale, les institutions publiques établies par la Constitution et les lois, l'intégrité du territoire national, le potentiel socio-économique du pays est placé parmi les « *intérêts vitaux de la Nation* » ou les « *besoins essentiels de la population* ».

La dimension socio-économique n'est elle-même pas absente de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité puisque son article 7 mentionne les activités des organisations criminelles qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique.

Dans les courriers adressés au Comité permanent R, de même que dans les rapports et ouvrages qu'il a consultés, les éléments suivants ont été cités comme composants du potentiel scientifique et économique du pays :

- l'approvisionnement vital en eau et en énergie ;
- la capacité des scientifiques à rechercher et à développer de nouvelles techniques et productions ;
- la capacité des opérateurs à produire des biens et des services ainsi que celle de participer au commerce international ;
- le bon fonctionnement du système financier et des grandes infrastructures financières ;
- les infrastructures de transport (chemins de fer, aéroports, réseau routier...) et les capacités logistiques ;
- la sécurité et la fiabilité des systèmes d'information et de communication ;
- l'état de bien-être socio-économique en général.

En conclusion, la défense des éléments d'un patrimoine économique, technique ou scientifique ne devrait-elle être l'affaire que de ceux auxquels ils appartiennent ?

Les services de renseignement peuvent y contribuer, jamais y pourvoir à la place de son détenteur. Cette défense doit s'adapter à tout moment aux menaces et aux multiples formes des attaques. La vulnérabilité des systèmes d'information et de communication des entreprises semble être aujourd'hui une préoccupation majeure.

Faut-il définir préalablement le potentiel scientifique et économique pour établir des secteurs prioritaires ? La démarche adoptée par les services de renseignement étrangers semble être empirique. Ils s'occupent d'abord des secteurs qui paraissent les plus menacés par l'espionnage de services étrangers ou par l'infiltration de la criminalité organisée. La fonction d'alerte et de sensibilisation des milieux économiques et scientifiques semble être celle la plus attendue de la part des services de renseignement.

Le renforcement du secret ne semble donc pas la meilleure solution en ce qui concerne le potentiel scientifique à moins qu'il ne soit financé par les deniers publics. Le secret ne doit être utilisé qu'à bon escient. Sa mise en oeuvre réduit la libre discussion et ralentit l'efficacité de la recherche. C'est aux scientifiques eux-mêmes qu'il appartient de trouver les solutions qui leur conviennent.

8.3. Quelques constatations

Première constatation

La difficulté de dégager une définition claire et, surtout, unanime. En effet, les points de vue que l'on peut adopter sur la définition du PSE sont en effet totalement différents selon que l'on met l'accent sur l'intérêt privé ou public. Cette discussion débouche dès lors rapidement sur une approche purement politique du sujet dans laquelle il n'appartient pas au Comité permanent R d'intervenir.

Deuxième constatation

Les services ont moins besoin d'une définition théorique que d'une délimitation de leurs champs d'actions. Pour le Comité ministériel du renseignement et de la sécurité, il s'agit en définitive de pouvoir indiquer la mission exacte qui doit être confiée aux services ainsi que les priorités dans ce domaine.

Troisième constatation

Plusieurs autres services publics et administrations fédérales et/ou régionales sont actifs sur ce terrain. Chacune de ses administrations dispose de compétences spécifiques, de telle sorte que, dans cette matière, la collaboration, la coordination et la répartition des tâches est une nécessité. Le rôle éventuel de coordination et de collaboration que la Sûreté de l'Etat pourrait jouer en la matière devrait faire l'objet d'une réflexion. Il n'est resté pas moins vrai que ce service n'est pas le seul concerné par la protection du potentiel scientifique et économique (sans parler de la relation avec le secteur privé).

Un exemple concret à retenir dans cet ordre d'idée est l'affaire EPSI évoquée dans le présent rapport annuel.

L'absence du SGRS dans ce débat est étonnante. La loi organique des services de renseignement et de sécurité lui confère pourtant la mission de rechercher, d'analyser et de traiter le renseignement relatif à toute menace de nature militaire contre le potentiel économique du pays, une telle menace étant considérée comme une menace contre l'intégrité du territoire national (article 11, § 1^{er} et § 2, 1^o). Le SGRS dispose d'une expertise dans ce domaine grâce à son contrôle spécifique sur les entreprises fournissant la Défense nationale, dans le cadre des enquêtes de sécurité et de la gestion des informations et des brevets classifiés.³⁴

Le fait que la Sûreté de l'État et le SGRS aient chacun une compétence dans cette matière doit inciter ces deux services à collaborer activement sur le sujet.

Ces trois premières constatations sont partagées par l'organe de contrôle parlementaire des services de renseignement britanniques. En parlant de la notion de « *UK's economic well-being* », le Comité britannique (*Intelligence and Security Committee*) fait le commentaire suivant : « *this is an important topic, with a large number of departments and governments organisations having interest in it. We note that there is not a common definition across Whitehall of what constitutes economic well-being and we believe that, because of the number of interested bodies, there is a clear need for more co-ordination on the setting of priorities and requirements* ».³⁵

Dernière constatation

La recherche de l'efficacité d'un service public ne peut pas aboutir exclusivement à des considérations théoriques et, surtout, il ne faut pas succomber à la tentation d'imaginer des directives qui figurent déjà dans la loi fondamentale. En gardant les différentes données de l'étude à l'esprit, le Comité permanent R a dès lors réexaminé la question en partant des principes généraux et de plusieurs dispositions spécifiques de la loi organique.

8.4. Une autre approche

Plusieurs dispositions générales qui s'appliquent à chaque activité d'un service de renseignement belge découlent de la loi organique : il s'agit toujours d'une MENACE émanant d'un PHÉNOMÈNE³⁶ ; l'intérêt global de l'ensemble de la société est toujours en jeu ; l'action des services de renseignement, en collaboration avec les autres acteurs concernés, doit avoir pour but d'informer les autorités compétentes afin de leur permettre d'adapter leur politique ou de prendre des mesures nécessaires en connaissance de cause . Il s'agit toujours d'une approche défensive. D'autres services étant également actifs sur le terrain, cette action nécessite donc un échange d'informations.

L'objet de la menace

A la question de savoir ce qui doit être protégé il ne faut pas se laisser égarer par l'opposition entre les intérêts privés ou publics à protéger.

Finalement, il y a deux valeurs de base qui sont établis dans la société.

Cela concerne d'un côté l'état de droit et de l'autre le bien-être socio-économique. Ces deux éléments sont la base de la qualité de la vie et de la société .

³⁴ Comité permanent R, *Rapport général d'activités 2003*, Bruxelles, 2004, pp. 117-118 (www.comiteri.be).

³⁵ Intelligence and Security Committee (UK), *Annual report 2004-2005*.

³⁶ L'on entend par « menace » une activité humaine malveillante par opposition à un phénomène naturel.

La nature de la menace

Mais quelle est précisément la mission d'un service de renseignement face à cette menace ? Il suffit de reprendre l'article 8, 1 a) et g) de la loi organique pour comprendre où se situe le « CRÉNEAU » que ces services peuvent occuper, étant donné, d'une part, les moyens et possibilités limités des services de renseignement belges et, d'autre part, les missions et compétences des autres services.

Il s'agit ici de l'espionnage (l'obtention ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter) et de l'ingérence (la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins).

Une double mission : informer et sensibiliser

Bien que la mission première d'un service public consiste à remettre des rapports au politique, il est également recommandé, dans cette matière, de conférer aux services un rôle de sensibilisation à l'égard des secteurs visés.

Plusieurs enquêtes du Comité permanent R ont démontré que notre pays se caractérisait historiquement tant par une ouverture qui ne tient pas ou peu compte de l'intérêt de pays tiers pour notre savoir-faire, que par une méfiance à l'encontre des missions et du fonctionnement de nos services de renseignement. Il y a donc place ici pour un partenariat entre les secteurs privé et public lorsque les intérêts privés et publics convergent. Ceci conforte dès lors une conception DEFENSIVE de la mission des services de renseignement belges en matière de protection du potentiel scientifique et économique.

Une proposition de description de la mission

La mission des services de renseignement à l'égard du PSE consiste à obtenir, analyser et signaler aux autorités compétentes des informations relatives à l'espionnage et l'ingérence (tels que visés par l'article 8, 1 a et g de la loi organique), lorsque ces derniers mettent en péril le maintien du bien-être socio-économique, ainsi qu'à sensibiliser les entreprises de ce secteur aux dangers de l'espionnage et l'ingérence et aux mesures à prendre.

En application de l'article 33, alinéa 5 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement, la ministre a organisé plusieurs échanges de vues avec le Comité permanent R et la Sûreté de l'Etat. A la suite de quoi, le Comité permanent R a amendé ses conclusions le 26 avril 2006.

La discussion n'est pas encore terminée et fait l'objet de nouveaux entretiens avec les acteurs les plus importants.

CHAPITRE 2	ASSISTANCE A LA REDACTION DU PROJET DE LOI RELATIF A L'ANALYSE DE LA MENACE
-------------------	--

Depuis 2004, le Comité permanent R a collaboré étroitement au projet du Gouvernement visant à créer un organe de coordination pour l'analyse de la menace. Cette collaboration se situe dans le prolongement de la recommandation des Commissions de la Chambre des Représentants et du Sénat chargées du suivi du Comité Permanent de contrôle des services de renseignements et de sécurité.

Cette commission, sur indication du Comité permanent R, a constaté qu'un problème structurel se posait quant à l'échange d'informations essentielles entre tous les services publics. Les commissions de suivi insistent par conséquent sur une meilleure communication entre les deux services de renseignements avec une reconnaissance des compétences spécifiques de chaque service. Par ailleurs, elles insistent quant à la coordination de l'information aux autorités compétentes. Cette coordination devrait également avoir lieu avec les autres services concernés.

En 2005, à nouveau, divers membres du Comité permanent R ont intensivement collaboré à cet important projet. Particulièrement pour ce qui concerne le volet "contrôle", qui sera assuré par les Comités permanents R et P, le Comité permanent R a été très actif pour ce qui est de la rédaction des projets de textes.

1. APERÇU ET ÉTAT DES LIEUX DES PROCÉDURES JUDICIAIRES

Lors du séminaire organisé par le Sénat le 12 juillet 2005³⁷, il a été demandé au Comité permanent R de suivre les procès actuellement en cours au niveau européen à l'encontre des « listes terroristes ». En outre, il a été demandé si le Comité permanent R pouvait examiner cette problématique et les conséquences de la mention sur une telle liste à la lumière des droits fondamentaux de l'homme.

En ce qui concerne ce dernier aspect, le Comité permanent R se bornera à soulever un certain nombre de remarques générales. La question des « listes terroristes » est en effet toujours pendante au Tribunal de première instance des Communautés européennes et (au stade de l'appel) à la Cour de Justice à Belgique. Selon toute vraisemblance, la Cour européenne des droits de l'homme devra une nouvelle fois³⁸ se pencher sur l'affaire.³⁹ Le Comité permanent R se limitera à brosser un état des lieux en date du 17 janvier 2006. Des jugements ont déjà été prononcés à plusieurs niveaux (le Tribunal de première instance des Communautés européenne, la Cour européenne des droits de l'homme et (au niveau national) le Tribunal de première instance de Bruxelles). Le Comité donnera également un bref aperçu des questions judiciaires soulevées et de la décision et des motivations des juridictions.

Pour une bonne compréhension, le Comité permanent R souhaite préciser que cette note porte uniquement sur les listes établies suite aux résolutions de l'ONU. D'autres listes qui résultent d'initiatives internationales ne sont pas abordées⁴⁰. Dans une quatrième section, nous répondrons brièvement à la question de savoir si une liste nationale s'avère ou non nécessaire.

L'on part généralement du principe qu'il existe deux types de « listes terroristes ONU » : la liste qui se fonde sur la Résolution 1267 de l'ONU et celle qui se base sur la Résolution 1373 (également appelée *Clearing House List*). D'un point de vue purement juridique, l'on pourrait voir les choses autrement et parler de trois listes.

³⁷ *La genèse et la mise en oeuvre des listes terroristes - Het ontstaan en de toepassing van de terroristische lijsten*. Le 17 janvier 2006, les Commissions des Relations extérieures et de la Défense du Sénat et la Commission des Relations extérieures de la Chambre ont tenu une séance d'audition sur *Les critères d'établissement de la liste des organisations terroristes de l'Union européenne*. Cette séance s'est toutefois déroulée à huis clos, de telle sorte que le Comité permanent R n'en connaît pas les résultats

³⁸ La Cour a déjà été saisie à deux reprises d'une affaire portant sur des listes terroristes (voir plus loin à la section 2.B.). Le couple belge Sayadi-Vinck a annoncé à la presse qu'il se pourvoierait également devant la Cour européenne (*De Standaard*, 13 juillet 2005 et *La Gazet van Antwerpen*, 7 et 8 janvier 2006).

³⁹ Lors de la rédaction de ce rapport d'activités on a appris que le Comité des droits de l'homme des Nations Unies se penchera sur la question (*La Libre Belgique*, 1 juin 2006).

⁴⁰ Lors du séminaire organisé au Sénat, il a été dit que les services de renseignement et de police participants utilisent également une liste terroriste au sein du *Working group on terrorism*.

En fait, deux listes se fondent sur cette dernière résolution de l'ONU : une liste mentionnant uniquement des personnes juridiques ou citoyens de l'Union européenne (UE) (à l'égard desquels seule une collaboration policière et judiciaire est prévue⁴¹) et une liste reprenant des personnes juridiques ou citoyens non ressortissants de l'UE (à l'égard desquels le gel des avoirs est également possible). Nous parlerons dès lors de la « Liste 1267 » qui résulte de la Résolution 1267, la « Liste 1373a » qui résulte de la Résolution 1373 et s'applique uniquement aux ressortissants de l'UE et la « Liste 1373b » pour les ressortissants hors UE.

1.1. Liste 1267

Le 15 octobre 1999, le Conseil de sécurité des Nations unies adoptait la Résolution 1267 (1999), qui imposait des sanctions économiques aux Talibans, en plus d'un embargo sur les armes et d'une interdiction de vol. Les États furent obligés de geler les fonds et autres moyens financiers ou économiques des Talibans. La Résolution 1333 (2000) du 19 décembre 2000 élargit ces sanctions à Oussama Ben Laden et aux individus et entités qui lui sont associés. Ces deux « résolutions fondamentales » ont été régulièrement rappelées et approfondies⁴².

Ces résolutions donnèrent naissance au « Comité des sanctions » dans le giron des Nations unies. Cet organe décide si une personne ou organisation doit être soumise aux sanctions qui découlent de la Résolution 1267 et des résolutions qui en découlèrent.

La Charte des Nations unies oblige les membres de l'ONU à exécuter ses décisions directement ou via les institutions internationales auxquelles ils appartiennent. C'est ainsi que le Conseil de l'Europe prit l'initiative de mettre en exécution cette obligation internationale par le biais de la Position commune 2001/154/PESC (26 février 2001) et du Règlement 467/2001 (6 mars 2001)⁴³. Ce règlement imposait notamment le gel de tous les avoirs et autres moyens financiers d'un certain nombre de personnes physiques ou morales, d'entités ou d'organisations désignées nommément. Il incombe à la Commission européenne d'actualiser cette liste. Ce qu'elle fait en suivant le « Comité des sanctions » : la Commission européenne modifie « sa » liste chaque fois que ce comité adapte la liste⁴⁴. En Belgique, les SPF des Finances et des Affaires économiques sont chargés de l'exécution des mesures prises. Ils centralisent les déclarations que les banques sont tenues de leur transmettre⁴⁵.

⁴¹ Le Traité CE n'offre aucun fondement justifiant la prise de "mesures de gel" au niveau de l'UE à l'encontre de ressortissants et d'organisations de l'UE.

⁴² Résolution 1363 (2001) du 30 juillet 2001, Résolution 1390 (2002) du 16 janvier 2002, Résolution 1452 (2002) du 20 décembre 2002 (cette résolution permet aux États – moyennant intervention du Comité des sanctions – de ne pas geler les avoirs des intéressés, c'est-à-dire l'argent leur permettant de couvrir les dépenses de base ou des frais exceptionnels), Résolution 1455 (2003) du 17 janvier 2003, Résolution 1456 (2003) du 20 janvier 2003, Résolution 1526 (2004) du 30 janvier 2004 et Résolution 1617 (2005) du 29 juillet 2005. Ces résolutions peuvent être consultées à l'adresse suivante www.un.org/documents/scres.htm.

⁴³ À l'heure actuelle, c'est le Règlement 881/2002 du 27 mai 2002 du Conseil, qui a abrogé le Règlement 467/2001, qui est d'application.

⁴⁴ Ce qui s'est déjà produit à plus de 60 reprises.

⁴⁵ La conformité du nom d'un titulaire de compte avec les personnes ou entités figurant sur la liste est contrôlée par la Sûreté de l'État et la police fédérale (*Questions et Réponses*, Chambre, 2004-2005, 27 juin 2005, 15753 (Question N° 859 Depoortere)). Jusqu'à présent, les banques belges ont bloqué environ 14 comptes sur la base de cette liste, et ce, pour un montant total de 6 348 € (Groupe d'action financière, "Synthèse du 3^e rapport d'évaluation mutuelle de la lutte anti-blanchiment de capitaux et contre le financement du terrorisme. Belgique", 10 juin 2005, www.fatf-gafi.org, point 10).

Cependant, la Belgique dispose également d'une réglementation en la matière. La loi du 11 mai 1995 relative à la mise en œuvre des décisions du Conseil de sécurité de l'Organisation des Nations unies autorise le Roi à mettre en exécution, par un arrêté délibéré en Conseil des ministres, les décisions contraignantes de l'ONU. C'est ce que le Roi fit par l'Arrêté royal du 17 février 2000 relatif aux mesures restrictives à l'encontre des Talibans d'Afghanistan. Cet arrêté stipule que le ministre des Finances est compétent pour organiser et prendre toute mesure visant à assurer la mise en œuvre du gel des avoirs et autres moyens financiers. L'Arrêté ministériel du 15 juin 2000 portant exécution de l'Arrêté royal du 17 février 2000 inclut une liste des personnes et/ou entités visées et reprend la liste de l'ONU. A l'instar de la liste « européenne », la liste « belge » est régulièrement adaptée selon la liste de l'ONU.

Plusieurs procédures juridiques ont été introduites contre cette (ces) liste(s), et ce, tant à l'échelle européenne que nationale.

1.1.1. Tribunal de première instance des Communautés européennes

Cinq actions ont été introduites devant le Tribunal de première instance des Communautés européennes contre la méthode de travail de l'UE⁴⁶. Les principaux arguments invoqués par les différents requérants sont les suivants :

Violation des articles 60, 249 et 301 du Traité CE

Les requérants ont argumenté que par le Règlement 467/2001, le Conseil a franchi les limites de ses compétences. Ils ont tenté de démontrer que le Conseil n'est pas compétent pour imposer des sanctions à des particuliers et organisations et s'est rendu coupable d'un abus de pouvoir. En outre, le Conseil et la Commission auraient délégué au Comité des sanctions le pouvoir de décider quelles personnes et organisations figurent sur la liste.

Article 3 CEDH

Le gel des avoirs peut engendrer des situations inhumaines.

Article 6 CEDH

La plupart des requérants pouvaient difficilement accepter que le Conseil et la Commission n'aient pas examiné les raisons qui ont amené le Comité des sanctions à les placer sur la liste. Ils n'ont pas non plus eu la possibilité de prendre connaissance des raisons de cette décision et n'ont pas pu faire connaître leur point de vue. Les requérants se sentaient lourdement sanctionnés sans avoir pu se défendre. Il s'agit dès lors d'une atteinte au principe de droit fondamental d'une bonne administration de la justice.

Article 8 CEDH

Plusieurs requérants ont invoqué que la mention sur une « liste terroriste » est une immixtion dans la vie privée et familiale.

⁴⁶ Affaire T-306/01 (Abdirisak Aden et autres) ; affaire T-318/01 (Omar Mohamed Othman) ; affaire T-315/01 (Yassimn Abdullah Kadi) ; affaire T-253/02 (Chafiq Ayadi) et affaire T-49/04 (Faraj Hassan). Ces affaires peuvent être suivies à l'adresse www.curia.eu.int

Article 13 CEDH

Plusieurs individus et groupes ont non seulement eu du mal à accepter le fait de n'avoir jamais été entendus avant d'être mentionnés sur la liste. Ils se sont également plaints de n'avoir droit à aucun recours effectif devant une instance judiciaire indépendante et de ne pas être dès lors à même de se pourvoir contre les constatations factuelles sur lesquelles reposent les mesures.

Article 1- Premier protocole CEDH

Il est logique que le droit à la jouissance paisible de sa propriété soit invoqué lorsque des avoirs sont gelés et donc soustraits à la jouissance des personnes.

Le principe de proportionnalité

Enfin, ils ont argumenté que le règlement va à l'encontre des principes fondamentaux du droit communautaire, et plus particulièrement les principes de subsidiarité, de proportionnalité et du respect des droits de l'homme. Les États membres de l'UE sont les mieux placés pour déterminer quelles mesures sont proportionnelles ou non ; l'on ne peut pas simplement se fonder sur les constatations du Comité des sanctions. Il est également disproportionné de priver un particulier de tout revenu et assistance financière.

Le Tribunal de première instance des Communautés européennes de Belgique s'est toutefois peu intéressé à ces arguments. Dans deux arrêts de principe datant du 21 septembre 2005 et prononcés dans les affaires T-306/01 et T-315/01, il reconnaît la force juridique de la « Liste 1267 ».

Ses motivations sont détaillées ci-après en raison de leur importance.

- La compétence du Conseil pour imposer des sanctions économiques à des particuliers

Le Traité CE permet au Conseil d'imposer des sanctions économiques et financières à des pays tiers, lorsqu'une position commune adoptée par l'Union européenne au titre de la politique étrangère et de sécurité commune (PESC) le prévoit. Le Tribunal juge que le Conseil est également compétent, dans des conditions similaires, pour imposer des sanctions économiques et financières (comme le gel des fonds) à des particuliers, dans le cadre de la lutte contre le terrorisme international.

- La primauté du droit de l'ONU sur le droit communautaire

Le Tribunal constate que, selon le droit international, les obligations des États membres de l'ONU en vertu de la Charte des Nations unies l'emportent sur toute autre obligation, y compris sur leurs obligations au titre de la Convention européenne des droits de l'Homme et au titre du Traité CE. Cette primauté s'étend aux décisions du Conseil de sécurité. Bien qu'elle ne soit pas membre de l'ONU, la Communauté doit être considérée comme liée elle aussi par les obligations résultant de la Charte des Nations unies. La Communauté ne peut violer les obligations incombant à ses États membres en vertu de la Charte ni entraver leur exécution.

– L'étendue du contrôle de légalité exercé en l'espèce par le Tribunal

Le Tribunal relève que le règlement attaqué se borne à mettre en œuvre, au niveau de la Communauté, des décisions du Conseil de sécurité. Tout contrôle de la légalité de ce règlement impliquerait donc que le Tribunal examine, de façon indirecte, la légalité des décisions en question. Or, compte tenu de la règle de primauté énoncée ci-dessus, ces décisions échappent en principe au contrôle juridictionnel du Tribunal et celui-ci n'est pas autorisé à remettre en cause, fût-ce de manière indirecte, leur légalité au regard du droit communautaire ou des droits fondamentaux. Au contraire, le Tribunal est tenu, dans toute la mesure du possible, d'interpréter et d'appliquer ce droit d'une manière qui soit compatible avec les obligations des États membres au titre de la Charte des Nations unies.

Néanmoins, le Tribunal est habilité à contrôler la légalité du règlement attaqué et, de manière indirecte, la légalité des décisions du Conseil de sécurité que ce règlement met en œuvre, au regard des règles supérieures du droit international général relevant du *jus cogens*, entendu comme un ordre public international auquel ni les États membres, ni les instances de l'ONU ne peuvent déroger. En font partie, notamment, les normes impératives visant à la protection universelle des droits fondamentaux de la personne humaine.

– Les droits fondamentaux des requérants protégés par le *jus cogens*

Le Tribunal de première instance constate que le gel des fonds ne viole pas *in casu* les droits fondamentaux des requérants, tels qu'ils sont protégés par le *jus cogens*. En effet, le règlement attaqué prévoit expressément la possibilité de dérogations, à la demande des intéressés, pour rendre accessibles les fonds nécessaires à des dépenses de base. Ces mesures n'ont donc ni pour objet ni pour effet de soumettre les requérants à un traitement inhumain ou dégradant. Les requérants n'ont pas non plus été arbitrairement privés de leur droit à la propriété, pour autant que ce droit soit protégé par le *jus cogens*. En effet, le gel des fonds constitue un aspect de la lutte légitime des Nations unies contre le terrorisme international et est une mesure conservatoire qui, à la différence d'une confiscation, ne porte pas atteinte à la substance même du droit de propriété des intéressés sur leurs actifs financiers, mais seulement à leur utilisation. De plus, les résolutions du Conseil de sécurité prévoient un mécanisme de réexamen périodique du régime général des sanctions et une procédure permettant aux intéressés de soumettre leur cas, par l'intermédiaire de leur État, au Comité des sanctions pour réexamen.

Quant aux droits de la défense, le Tribunal constate qu'aucune norme du *jus cogens* ne paraît exiger une audition personnelle des intéressés par le Comité des sanctions. S'agissant d'une mesure conservatoire limitant la disponibilité des biens, le respect des droits fondamentaux des intéressés n'impose pas non plus que les faits et éléments de preuve retenus à leur charge leur soient communiqués, dès lors que le Conseil de sécurité estime que des motifs intéressant la sûreté de la communauté internationale s'y opposent.

Le Tribunal juge que les institutions communautaires n'étaient pas davantage tenues d'entendre les intéressés, étant donné qu'elles ne disposaient d'aucune marge d'appréciation dans la mise en œuvre des sanctions décidées par le Conseil de sécurité.

Quant au droit à un recours juridictionnel effectif, le Tribunal relève que, dans le cadre du recours introduit par les requérants, il exerce un entier contrôle de la légalité du règlement attaqué quant au respect, par les institutions communautaires, des règles de compétence ainsi que des règles de légalité et des formes substantielles qui s'imposent à leur action. Il contrôle également la légalité du règlement, notamment sous l'angle de son adéquation formelle et matérielle, de sa cohérence interne et de sa proportionnalité par rapport aux résolutions du Conseil de sécurité. Le Tribunal contrôle encore la légalité du règlement et, indirectement, la légalité des résolutions du Conseil de sécurité, au regard du *jus cogens*.

Comme énoncé précédemment, le Tribunal refuse de contrôler indirectement la conformité des résolutions du Conseil de sécurité avec les droits fondamentaux tels qu'ils sont protégés par l'ordre juridique communautaire, de vérifier l'absence d'erreur d'appréciation des faits et des éléments de preuve que le Conseil de sécurité a retenus à l'appui des mesures adoptées, ou encore, de contrôler indirectement l'opportunité et la proportionnalité de ces mesures. Le Tribunal reconnaît que les requérants ne disposent d'aucune voie de recours juridictionnel dans cette mesure (seule une juridiction internationale chargée de statuer sur les recours dirigés contre les décisions individuelles du Comité des sanctions pourrait y remédier). Néanmoins, cette lacune dans la protection juridictionnelle des requérants n'est pas en soi, selon le Tribunal, contraire au *jus cogens*. Le droit d'accès aux tribunaux n'est pas absolu. En l'espèce, il se heurte à l'immunité de juridiction dont bénéficie le Conseil de sécurité. L'intérêt des requérants à voir leur cause entendue sur le fond par un tribunal n'est pas suffisant pour l'emporter sur l'intérêt général essentiel qu'il y a à ce que la paix et la sécurité internationales soient maintenues face à une menace clairement identifiée par le Conseil de sécurité, toujours selon le Tribunal.

Cet arrêt de principe a fait l'objet d'un seul pourvoi⁴⁷.

1.1.2. Tribunal de première instance de Bruxelles (11 février 2005)

Un juge belge a également dû se prononcer sur la légalité de la mention de personnes sur la « Liste 1267 ». Deux ressortissants belges qui figuraient sur cette liste ont demandé, d'une part, à ce que leur nom soit supprimé de l'Annexe à l'Arrêté ministériel du 31 janvier 2003 modifiant l'Arrêté ministériel du 15 juin 2000 portant exécution de l'Arrêté royal du 17 février 2000 et, d'autre part, à ce que les autorités belges insistent auprès du Comité des sanctions de l'ONU pour que leur nom soit supprimé de la liste de l'ONU.

Le juge a uniquement accédé à cette dernière demande : la Belgique doit signaler au Comité des sanctions qu'après deux ans et demi d'enquête, le tribunal n'a pas encore procédé à une mise en accusation et demande dès lors la radiation des deux noms.

⁴⁷ Affaire T-315/01 (Yassin Abdullah Kadi) (aujourd'hui : C-402/05).

1.2. Liste 1373a

Peu de temps après les attaques du 11 septembre 2001, le Conseil de sécurité des Nations unies vota la Résolution 1373 (2001). Cette dernière oblige notamment les Etats à geler les fonds et les moyens financiers et économiques de toutes les personnes qui ont commis, ont tenté de commettre ou ont facilité des actes terroristes. Elle est donc plus étendue que la précédente.

Les États membres de l'Union européenne ont également traduit cette résolution en un certain nombre d'instruments juridiques visant à geler les actifs financiers de personnes et entités formellement citées ET à améliorer la collaboration policière et judiciaire. Il s'agit de la Position commune 2001/931/PESC du Conseil du 27 décembre 2001 relative à l'application de mesures spécifiques en vue de lutter contre le terrorisme et (en exécution de celle-ci) du Règlement (CE) 2580/2001 du Conseil du 27 décembre 2001 concernant l'adoption de mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le terrorisme.

La Position commune donne *de facto* lieu à la « Liste 1373a »⁴⁸ et le Règlement, à la « Liste 1373b » (*infra*).

Ces deux listes répertorient des personnes qui ont commis ou tenté de commettre un acte de terrorisme ou y ont participé. Des informations ou éléments de dossier doivent démontrer qu'une instance (judiciaire) compétente a pris une décision en ce sens contre la personne concernée (p. ex. : introduction d'une enquête ou de poursuites sur la base de preuves ou d'indices sérieux et crédibles ou d'une condamnation)⁴⁹. L'Union européenne établit ces listes à l'unanimité. Cette dernière est également requise pour supprimer un nom des listes. Les listes sont actualisées tous les six mois. Contrairement à la « Liste 1276 », il ne s'agit donc pas ici de reprendre une liste de l'ONU.

Les conséquences de la mention sur la « Liste 1373a » se limitent à une obligation pour les Etats membres de veiller à une collaboration policière et judiciaire optimale eu égard aux personnes ou groupes concernés^{50 51}.

Plusieurs actions ont été intentées à l'encontre de cette liste, tant devant le Tribunal de Belgique que devant la Cour de Strasbourg.

⁴⁸ C'est-à-dire les personnes ou groupes dont le nom est précédé d'un astérisque sur la liste de la Position commune.

⁴⁹ Le point de vue belge concernant la mention ou non de personnes ou entités sur l'une de ces listes est exprimé, au niveau de l'UE, par notre représentation permanente. Celle-ci est conseillée par la Sûreté de l'État, le SGRS, le GIA et la police fédérale.

⁵⁰ Pour ces personnes (privées ou morales) ressortissantes de l'UE, le gel des avoirs n'est donc pas possible. Il faut pour cela un fondement dans le droit interne.

⁵¹ Étant donné que la "Liste 1373a" découle, d'un point de vue juridique, d'un accord intergouvernemental (il s'agit en effet d'une Position commune émise dans le cadre de la politique étrangère et de sécurité commune) et que tous les pays doivent être d'accord avec la mention ou la suppression d'un nom, l'on pourrait affirmer que chacun des 25 États membres de l'UE applique une liste "nationale" propre.

1.2.1. Tribunal de première instance des Communautés européennes

Cinq procédures ont été introduites contre la « Liste 1373a »⁵².

Les arguments invoqués par les requérants ne divergent en fait pas de ceux soulevés contre la « Liste 1267 » : aucune contestation possible, pas de consultation du dossier, décision non motivée, violation du principe de subsidiarité, le traité de l'UE n'autorise pas la prise de telles décisions, violation de la vie privée, droit à un procès équitable, liberté d'expression et d'association et enfin droit à la propriété.

Jusqu'à présent, le Tribunal s'est prononcé sur trois affaires⁵³ : les deux premières demandes ont été déclarées irrecevables le 7 juin 2004 et la troisième, le 18 novembre 2005. Le Tribunal dut en effet constater que la liste concerne en grande partie une question intergouvernementale qui a résulté d'une position commune au titre de la PESC (deuxième pilier) et porte sur une matière du troisième pilier (collaboration policière et judiciaire). Au regard de ces constatations, le Tribunal estime ne pas être compétent pour émettre un jugement.

Un recours a été introduit contre les deux premières décisions auprès de la Cour de Belgique⁵⁴.

1.2.2. Cour européenne des Droits de l'homme

Les deux premières associations qui furent déboutées à Belgique et deux de leurs porte-parole s'étaient auparavant adressés à la Cour de Strasbourg. Ils ont invoqué pour principal argument qu'ils avaient été publiquement décrits par les quinze États membres de l'UE comme une organisation terroriste, sans connaître les motivations de cette décision et sans avoir pu s'y opposer. Comme ils s'estimaient victimes directes et potentielles du règlement de l'UE, ils ont également allégué des violations aux articles 3, 6, 8 (uniquement pour les porte-parole), 10, 11 et 13 de la CEDH et à l'article 1 du premier Protocole de la CEDH.

Déjà le 23 mai 2002, la Cour déclarait leur requête irrecevable, et ce, principalement pour deux raisons. Premièrement, elle affirma que le Traité exige qu'un plaignant soit réellement concerné par la violation qu'il invoque ; une action contre une violation potentielle d'un droit fondamental n'est recevable que dans des circonstances exceptionnelles.

Deuxièmement, elle statua que l'appel à une meilleure collaboration policière et judiciaire à l'égard de groupes et personnes mentionnés sur la liste n'octroie aucune compétence supplémentaire aux autorités et que les intéressés ne sont qu'indirectement concernés⁵⁵.

⁵² Affaire T-228/02 (Organisation des Modjahedines du peuple d'Iran) ; affaire T-333/02 (Gestoras Pro Amnistia) ; affaire T-338/02 (Segi e.a.) ; affaire T-327/03 (Fondation Al-Aqsa) et affaire T-299/04 (Selmani).

⁵³ D'abord dans les affaires T-333/02 (Gestoras Pro Amnistia) et T-338/02 (Segi e.a.), puis dans l'affaire T-299/04 (Selmani).

⁵⁴ Ces appels sont connus sous les numéros C-354/04 et C-355/04

Selon la Cour, le fait qu'une organisation soit répertoriée sur une liste avec des pays impliqués dans le terrorisme peut être « embarrassant », mais ne suffit pas pour conclure à une violation des droits fondamentaux.

Les porte-parole des deux associations s'étaient en outre appuyés sur l'article 8 de la CEDH. La Cour déclare brièvement que le nom de ces personnes n'apparaît pas sur la liste en question et qu'il ne peut donc s'agir d'une violation. Cette déclaration peut offrir une possibilité aux plaignants qui y sont mentionnés à titre personnel.⁵⁶

1.3. Liste 1373b

Cette troisième liste, qui porte sur des ressortissants hors UE, n'appelle pas seulement à une collaboration policière et judiciaire efficace dans les questions pénales. Elle va même beaucoup plus loin : les comptes bancaires ou autres moyens économiques doivent être gelés. Le gel est une mesure administrative mise en œuvre par les banques ou institutions financières qui communiquent toutes les informations pertinentes au ministre des Finances.

La « Liste 1373b » est une véritable liste UE. Elle se fonde sur le droit communautaire, et notamment sur le Règlement 2580/2001. En Belgique, ce règlement (et donc indirectement la Résolution 1373 de l'ONU) est exécuté par l'Arrêté royal du 2 mai 2002 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le terrorisme et par l'Arrêté ministériel du 17 juin 2002 portant exécution de l'Arrêté royal précité⁵⁷.

Jusqu'à présent, six actions ont été introduites contre la mention sur cette liste auprès du Tribunal de première instance de Belgique^{58 59}.

⁵⁵ Ce raisonnement ne tient bien sûr plus debout lorsque certains pays décident individuellement d'assortir la mention sur une telle liste de conséquences plus importantes. Par exemple, les Pays-Bas veulent/voudraient interdire les organisations qui figurent sur les listes terroristes et pénaliser la participation aux activités de ces organisations (Proposition de loi portant approbation de la Convention européenne adoptée le 24 avril 1986 à Strasbourg en matière de reconnaissance de la personnalité juridique des organisations internationales non gouvernementales, et concernant l'introduction de certaines règles relatives à des organisations mentionnées sur une liste terroriste et d'autres organisations dont le but ou les activités sont contraires à l'ordre public (n° 28 764).

⁵⁶ Dans un avis récent, la Commission de protection de la vie privée part implicitement du principe que la mention de personnes sur des "listes noires" constitue une ingérence au titre de l'article 8 de la CEDH (avis n° 09/2005 du 15 juin 2005 qui porte principalement sur les listes établies par des personnes privées ou morales). Dans ce cadre, la commission renvoie à l'article 22 de la Constitution qui (contrairement à l'article 8 de la CEDH) exige une base légale formelle pour toute immixtion. Le Comité permanent R adhère totalement à l'analyse de la Commission de protection de la vie privée.

⁵⁷ Par souci de complétude, soulignons le fait que l'Arrêté royal du 2 mai 2002 portant exécution du Règlement 2580/2001 reposait encore sur la loi du 11 mai 1995, en l'absence de législation qui octroie au pouvoir exécutif la compétence pour la mise en œuvre des mesures décidées par le Conseil de l'Union européenne. Dans l'intervalle, le Moniteur belge du 13 juin 2003 publiait la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'États, de certaines personnes et entités. Cette loi confère au Roi le pouvoir de prendre, par arrêté délibéré en Conseil des ministres, les mesures nécessaires à la mise en œuvre de certaines actions ou positions communes et des règlements adoptés par le Conseil de l'Union européenne.

⁵⁸ Affaire T-206/02 (Congrès national du Kurdistan), affaire T-228/02 (Organisation des Modjahedines du peuple d'Iran), affaire T-229/02 (Osman Oclalan), affaire T-47/03 (José Maria Sison), affaire T-327/03 (Fondation Al-Aqsa) et affaire T-299/04 (Selmani). Trois de ces procès portent aussi sur la "Liste 1373a".

⁵⁹ Pour ce que nous avons pu vérifier, aucune action n'a été intentée en Belgique contre la mention dans cette liste. En revanche, aux Pays-Bas, la Fondation Al-Aqsa a saisi (sans succès) le juge des référés ('s-Gravenhage, 3 mai 2003 et 3 juin 2003, www.rechtspraak.nl).

Les mêmes arguments ont une nouvelle fois été avancés. Il fut en outre également invoqué que la mention sur la liste restreint la libre circulation des finances et la liberté de mouvement.

Le 15 février 2005, le Tribunal prononça l'irrecevabilité de deux affaires⁶⁰. Il ne faut toutefois pas en conclure que cette liste n'est pas discutable pour le juge européen. L'irrecevabilité est motivée par le fait que les requérants (chacun pour une raison spécifique) n'avaient pas d'intérêt direct dans cette action. Les personnes ou groupes qui sont bel et bien cités conservent la possibilité que le Tribunal se déclare compétent pour l'aspect « gel des avoirs », qui relève du « premier pilier ». Un pourvoi a été introduit pour l'une des deux affaires⁶¹.

Le 19 novembre 2005, la Cour déclara irrecevable une autre demande, et ce, alors que le requérant apparaissait bien sur la liste concernée. La demande était toutefois introduite tardivement⁶².

Par souci de complétude, nous mentionnons encore que l'un des plaignants avait également intenté une action par laquelle il demandait la consultation des documents sur lesquels se fonde sa mention sur la liste. Cette demande fut elle aussi rejetée⁶³.

2. DE LA PERTINENCE D'UNE LISTE BELGE

Parallèlement aux listes de l'ONU, plusieurs pays utilisent également des listes nationales auxquelles ils associent des conséquences juridiques spécifiques⁶⁴. En Belgique, ce n'est pour l'instant pas le cas⁶⁵. Le *Groupe d'action financière*, qui regroupe actuellement 31 pays, insiste sur la création d'une telle liste⁶⁶.

Il s'avère en effet aujourd'hui que notre pays ne peut procéder au gel des avoirs de deux catégories de personnes ou entités : celles établies dans l'UE et celles situées hors de l'UE mais pour lesquelles aucune unanimité n'existe parmi les États membres.

⁶⁰ Affaire T-206/02 (Congrès national du Kurdistan) et affaire T-229/02 (Osman Oclalan).

⁶¹ Affaire T-229/02 (Osman Oclalan), aujourd'hui C-229/05.

⁶² Affaire T-299/04 (Selmani).

⁶³ Affaire T-110/03 (José Maria Sison).

⁶⁴ Aux États-Unis, la liste "TEL" (*Terrorism Exclusion List*) a été établie sur la base du Patriot Act, de la liste FTO (*Foreign Terrorist Organizations*) et de la liste dressée par la *Maison-Blanche* au titre de l'*Executive Order 13224*.

Au Royaume-Uni, le *Home Secretary* dispose d'une liste. En vertu de la *Part II* du *Terrorism Act 2000*, le *Secretary of State* a la possibilité d'interdire des groupes impliqués dans le terrorisme. Pour être supprimée de la liste, une personne ou entité doit en faire la demande au *Secretary of State* et, le cas échéant, peut interjeter appel auprès de la *Proscribed Organizations Appeal Commission* (POAC).

Les Pays-Bas doivent toujours se prononcer sur la proposition de loi portant approbation de la Convention européenne adoptée le 24 avril 1986 à Strasbourg en matière de reconnaissance de la personnalité juridique des organisations internationales non gouvernementales, et concernant l'introduction de certaines règles relatives à des organisations mentionnées sur une liste terroriste et d'autres organisations dont le but ou les activités sont contraires à l'ordre public (n° 28 764). Cette proposition a pour but de permettre au juge de mettre hors la loi des corporations étrangères dont l'objectif ou les activités sont contraires à l'ordre public. En outre, les corporations ou personnes juridiques mentionnées sur les listes 1267, 1373a et 1373b (voir plus loin) seraient interdites de plein droit. La collaboration avec ces organisations doit être punissable.

⁶⁵ Chez nous, la Sûreté de l'État, dans le cadre de sa mission générale, tient également des listes de groupements extrémistes et terroristes à suivre. La mention sur ces listes n'est toutefois pas assortie de mesures administratives (p. ex. : dissolution, liquidation ou gel des avoirs) ou judiciaires particulières.

⁶⁶ *Groupe d'action financière*, "Synthèse du 3^e rapport d'évaluation mutuelle de la lutte anti-blanchiment de capitaux et contre le financement du terrorisme. Belgique", 10 juin 2005, www.fatf-gafi.org, point 9.

Le fait que cette liste n'existe pas pour l'instant ne signifie bien sûr pas que notre pays soit totalement impuissant. Étant donné que le financement du terrorisme constitue un délit autonome depuis 2003 (article 141 du Code pénal), il est toujours possible de procéder à la saisie ou confiscation des deniers et avoirs.

3. CONCLUSION

L'analyse des décisions judiciaires montre clairement que des personnes ou des groupes qui veulent s'opposer au fait et à la manière dont leur nom a été ajouté à l'une des listes terroristes disposent de peu de moyens juridiques pour mettre à néant cette décision.

Seule une action politique et diplomatique semble possible⁶⁷.

La question n'est toujours pas tranchée. Le Tribunal et en cas d'appel la Cour de Luxembourg doivent encore se prononcer sur plusieurs questions de principe. Selon toute vraisemblance, la Cour de Strasbourg sera également appelée à statuer sur cette matière de même que le Comité des droits de l'homme des Nations Unies.

⁶⁷ Nous pensons ici aux actions menées par les parlementaires en faveur du retrait de l'*Organisation des Modjahedines du peuple d'Iran* de la liste terroriste (cf. p. ex. la proposition de résolution sur le régime en Iran et l'opposition à celui-ci, Sénat, 2004-2005, 3-1065/1 et la proposition de résolution adoptée concernant la situation politique en Iran et ses relations avec l'Union européenne, Sénat, 2004-2005, 3-1057/7).

CHAPITRE 4 : ETUDE JURIDIQUE COMPARÉE PORTANT SUR CERTAINS ASPECTS DE L'INTERACTION ENTRE LES SERVICES DE RENSEIGNEMENT ET LA JUSTICE

Dans son rapport annuel 2004⁶⁸, le Comité permanent R publiait une étude intitulée "INTERACTION ENTRE LES SERVICES DE RENSEIGNEMENT ET LES AUTORITÉS JUDICIAIRES", dans laquelle il décrivait en détail la situation belge dans cette matière vaste et complexe, formulait quelques recommandations provisoires et jetait les bases d'une étude juridique comparée. Cette étude fut confiée, courant 2005, au professeur D. Van Daele de l'*Instituut voor Strafrecht* de la faculté de droit de la *Katholieke Universiteit Leuven*. Il lui fut demandé de répondre à quatre (grandes) questions en s'intéressant à la situation en vigueur aux Pays-Bas, en France et en Allemagne. Il s'agissait des questions suivantes :

1. OBLIGATION OU POSSIBILITÉ DE TRANSMETTRE AUX AUTORITÉS JUDICIAIRES DES INFORMATIONS RELATIVES À UN DÉLIT

En Belgique, les membres des services de renseignement doivent informer les autorités judiciaires de tout crime ou délit dont ils ont connaissance dans l'exercice de leur fonction, même si l'infraction n'est pas directement liée à leurs missions et même s'ils n'ont pas été témoins du fait.

Outre cette obligation, les services de renseignement ont également la possibilité de communiquer aux autorités judiciaires d'autres données potentiellement importantes. Il s'agit, par exemple, d'informations potentiellement intéressantes au démarrage proactif d'une enquête.

Existent-ils aux Pays-Bas, en France et en Allemagne une obligation similaire ? Ou s'agit-il seulement d'une possibilité ? Dans ce cas, qui prend la décision et sur quels critères ? Dans le cas d'une obligation, les instances poursuivantes, le suspect ou le juge peuvent-ils obliger les services de renseignement à communiquer certaines informations (p. ex. perquisition et saisie) ?

2. POSSIBILITÉ DE FOURNIR UNE "ASSISTANCE TECHNIQUE"

En Belgique, les services de renseignement peuvent prêter une "assistance technique" à la justice. En fait, ils interviennent dans le cadre d'enquêtes, sans qu'il soit toutefois clairement déterminé jusqu'où ils peuvent aller. La situation est-elle similaire aux Pays-Bas, en France et en Allemagne et quelle est la marge de manœuvre (les services de renseignement disposent-ils dans ce cas de compétences policières ? Peuvent-ils rassembler activement des données ? Peuvent-ils se servir de leurs propres compétences ?...) ?

⁶⁸ Comité permanent R, *Rapport général d'activités 2004*, Brussel, 2005, pp. 110-141.

3. UTILISATION EN JUSTICE DE DONNÉES QUE LES SERVICES DE RENSEIGNEMENT ONT OBTENUES LÉGALEMENT PAR DES MÉTHODES AUXQUELLES LA JUSTICE NE PEUT PEUT-ÊTRE PAS RECOURIR

Comment sont utilisées dans les pays concernés les données que les services de renseignement ont récoltées à l'aide de leurs méthodes (particulières) (p. ex. les écoutes téléphoniques) et sont transmises à la justice, alors que la justice elle-même n'aurait probablement jamais pu trouver ces informations ? Cette question est-elle régie par la loi ou est-elle problématique ?

4. LES DONNÉES DES SERVICES DE RENSEIGNEMENT COMME MOYEN DE PREUVE OU COMME INFORMATION DE DÉPART OU D'ORIENTATION

Existe-t-il des règles relatives à l'utilisation de données provenant des services de renseignement comme preuve dans des affaires criminelles ? Ces données peuvent-elles servir de preuve valable ou peuvent-elles uniquement être utilisées comme information pour démarrer ou orienter une enquête judiciaire ? Doivent-elles toujours figurer au dossier répressif ou sont-elles totalement ou partiellement protégées ? Dans ce cas précis, qui juge du bien-fondé de la collecte et de la fiabilité et de la valeur des données ? Existe-t-il à cet égard différents régimes selon la nature ou la provenance des données (données classifiées ; données provenant de services de renseignement étrangers, d'informateurs ou de membres de services de renseignement) ?

Début avril 2006, le rapport d'enquête détaillé et richement documenté fut remis au Comité permanent R. Cette étude fera l'objet d'une publication séparée au cours de l'année 2006. Afin de pouvoir formuler des recommandations concrètes à propos de l'interaction entre les services de renseignement et les autorités judiciaires, le Comité permanent R va examiner ce rapport en profondeur. Il agrémente, le cas échéant et si possible, le débat de quelques exemples provenant d'autres pays que les trois pays étudiés et alimentera la discussion d'informations récentes recueillies en Belgique. Ce rapport d'enquête et les recommandations concrètes-y afférentes seront transmis à la Commission de suivi du Sénat dans le courant de l'année 2006.

CHAPITRE 5 : LE CONTRÔLE DEMOCRATIQUE DES SERVICES DE RENSEIGNEMENT – SEMINAIRE

« Les attaques terroristes en Europe et dans le reste du monde ont donné lieu à l'élargissement des moyens d'action des services de renseignement. Cependant, le monde politique ne peut bien entendu pas limiter son attention à l'augmentation des moyens et des compétences de ces services. Il doit sans aucun doute veiller aussi à ce qu'un contrôle parlementaire réel soit instauré sur leur fonctionnement. »

C'est sur cette idée qu'un séminaire intitulé « *Contrôle démocratique des services de renseignement* » a été organisé par le Sénat et par le Comité permanent de contrôle des services de renseignements.

Le vendredi 16 septembre 2005, sous la présidence de Madame LIZIN, présidente du Sénat et présidente de la Commission parlementaire de suivi, un panel composé d'universitaires, d'hommes politiques et de spécialistes de différentes nationalités a brossé un tableau des modalités de contrôle qui existent dans différents pays européens, tels que la Belgique, l'Allemagne, la France, les Pays-Bas et le Royaume-Uni. Ces personnes ont en outre proposé un aperçu des réalisations et des projets concernant le travail de renseignement au niveau européen. Une question a d'emblée été soulevée : un contrôle démocratique par le Parlement européen est-il déjà nécessaire, et dans quelle mesure ?

Des experts belge (M. DELEPIÈRE, président du Comité permanent de contrôle des services de renseignement), allemand (M. MAIER, Ministerialdirektor, Sekretär des Parlamentarisches Kontrollgremium), français (M. LACOSTE, Amiral e.r.), anglais (M. GILL, professeur en « Politics and Security » à l'université John Moores de Liverpool) et néerlandais (M. FASSEUR, membre de la commission de contrôle des services de renseignement et de sécurité) ont présenté la manière dont leur pays respectif règle le contrôle démocratique des services de renseignement et de sécurité. Ces présentations ont permis de constater que le contrôle parlementaire de services de renseignement et de sécurité est exercé de manière différente dans chaque pays. Tout le monde est cependant d'accord sur le fait que le contrôle démocratique peut contribuer à l'acceptation et à la légitimation du travail des services de renseignement. Un contrôle démocratique efficace place les services de renseignement au milieu d'un système démocratique visant à garantir les libertés des citoyens, notamment dans leurs relations avec les autorités. Ce contrôle peut tout aussi bien viser le respect de la légalité que du cadre administratif l'efficacité.

M. BORN (Geneva Centre for the democratic control of armed forces) a expliqué comment ce contrôle démocratique doit de préférence prendre forme sur le plan du contenu en se fondant sur de meilleures pratiques (« best practices »).

Outre les mécanismes de contrôle nationaux, on observe également une attention croissante au niveau international pour le contrôle démocratique des services de renseignement et de sécurité. M. ALMEDA (chef d'unité des coopérations policières et de la lutte antiterroriste à la Direction Justice Liberté et Sécurité de l'Union) et Mme MASTENBROEK (membre du Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures) ont successivement donné leur vision sur l'internationalisation croissante du contrôle démocratique.

Les exposés des orateurs de ce colloque seront rassemblés dans le rapport « Contrôle démocratique des services de renseignement » qui sera réalisé dans le courant de l'année 2006.

TITRE 7

LES ACTIVITÉS DU COMITÉ PERMANENT R EN TANT QU'ORGANE DE RECOURS

Pour le Comité permanent R, l'année 2005 aura été marquée du sceau d'une modification notable de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité¹, loi remaniée en profondeur par la loi du 3 mai 2005² : non seulement le contentieux de l'organe a été élargi au recours contre les attestations et avis de sécurité négatifs ou faisant l'objet d'une absence de décision, mais encore la composition de l'instance de recours a, elle aussi, été modifiée.

Auparavant, l'organe de recours se composait des trois membres du Comité permanent R. Depuis l'entrée en vigueur de la nouvelle loi, à la date du 7 juin 2005, cet organe se compose des présidents du Comité permanent R, du Comité permanent P et de la Commission de la Protection de la Vie privée ; le président du Comité permanent R en assure la présidence, tandis que le Comité permanent R continue d'assurer la fonction du greffe.

Les recours contre les nouvelles attestations et nouveaux avis de sécurité ainsi que ceux à l'encontre des habilitations de sécurité intentés après le 7 juin 2005 ne sont donc plus traités par l'organe de recours rattaché au Comité permanent R. Seules les affaires en cours sont menées à leur terme et les activités du nouvel organe de recours ne sont pas reprises dans le présent rapport d'activités.

¹ Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, *M.B.*, 7 mai 1999 ; err. 24 juin 1999.

² Loi du 3 mai 2005 modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations de sécurité, *M.B.*, 27 mai 2005.

CHAPITRE 2**ACTIVITÉS DE L'ANCIEN ORGANE DE RECOURS**

En 2005, l'ancien organe de recours a encore traité 14 recours, dont voici le relevé commenté :

N°	AUTORITE DE SECURITE	DECISION
1	ANS	Incompétent
2	SGR	Non fondé
3	ANS	Irrecevable
4	ANS	Enquête à parachever et nouvelle décision (l'habilitation est accordée)
5	SGR	Enquête à parachever et nouvelle décision (l'habilitation n'est pas accordée)
6	ANS	Renonciation au recours
7	SGR	Recours fondé, habilitation de sécurité accordée
8	SGR	Recours fondé, habilitation accordée
9	SGR	Recours fondé, habilitation accordée
10	SGR	L'enquête doit être parachevée et une nouvelle décision prise (résultat inconnu)
11	SGR	Recours fondé, habilitation accordée
12	SGR	Recours irrecevable
13	SGR	Recours non fondé
14	SGR/ANS	Recours non fondé

Comme on peut le voir, la majorité des recours sont intentés à l'encontre des décisions du Service général de Renseignement et de Sécurité (SGR), qui effectue les enquêtes de sécurité et décide d'octroyer ou non les habilitations de sécurité pour les forces armées, le personnel du département de la Défense nationale, ainsi que pour les entreprises collaborant avec ce département.

Dans cinq cas, l'habilitation a en fin de compte été accordée, soit par décision de l'organe de recours, soit à l'issue d'une enquête complémentaire imposée, suivie d'une nouvelle décision de l'autorité de sécurité.

La situation de 2005 est comparable à beaucoup d'égards à celle de l'année précédente : on observe une surreprésentation des recours intentés contre les décisions du SGR, tout en relevant une proportion similaire de recours fondés et non fondés. Deux problèmes majeurs ont toutefois disparu. Tout d'abord, il y a le départ des membres de la police fédérale qui assuraient les enquêtes de sécurité au sein du SGR, mission à présent reprise par des membres du personnel du SGR lui-même. Par ailleurs, le Comité permanent R n'a plus été approché ou informé au sujet d'entreprises actives dans le secteur de la Défense nationale suite à des plaintes au sujet d'enquêtes refusées ou durant beaucoup trop longtemps et qui faisaient en sorte que ces entreprises subissaient une forme de préjudice concurrentiel.

Par contre, on continue de relever des refus d'octroi d'habilitation de sécurité pour des militaires qui, suite à une mission à l'étranger, ont entamé une relation affective stable avec une personne étrangère ne séjournant pas encore depuis assez longtemps en Belgique (de cinq à dix ans) pour que l'on puisse, conformément aux prescriptions, effectuer une enquête satisfaisante et dont le pays d'origine n'a pas conclu de traité avec la Belgique. Le ministre de la Défense a d'ores et déjà adhéré au point de vue du Comité permanent R, qui veut que cette seule circonstance est insuffisante pour refuser une habilitation. Toutefois, le refus peut s'avérer fondé si, par exemple, le passé de la famille de la personne étrangère et le contexte encadrant celle-ci ou encore le pays d'origine peuvent être considérés comme constitutifs d'un risque certain pour la sécurité. Cette catégorie de motifs de refus ou de retrait de l'habilitation de sécurité constitue, conjointement avec l'usage de drogues, un important groupe au sein des recours introduits contre les décisions du SGR.

Un dernier élément ne peut être ignoré, à savoir l'arrêt de la Cour d'arbitrage du 25 janvier 2006¹, arrêt rendu suite à une question préjudicielle posée à la Cour dans le cadre d'un recours intenté auprès du Comité R. Cette question, ici résumée de manière succincte, concernait les aspects suivants :

- le caractère de l'organe de recours (qui était toujours le Comité R à l'époque) ;
- l'impossibilité d'aller en appel d'une décision prise par le Comité R en tant qu'organe de recours ;
- la possible restriction du droit de consultation du dossier de sécurité pour le plaignant et son conseil concernant des éléments mettant en jeu la sécurité nationale.

La Cour d'arbitrage s'est penchée de manière attentive sur la problématique et est parvenue aux conclusions suivantes :

- en tant qu'organe de recours, le Comité permanent R est un organe juridictionnel collégial doté d'un pouvoir juridictionnel complet lui permettant d'exercer un contrôle indépendant sur les décisions prises en matière d'habilitations de sécurité
- l'absence de possibilité de recours n'est pas un principe général ou impératif, sauf dans les affaires pénales ;
- la restriction du droit de consultation du dossier de sécurité n'est pas constitutive d'une violation de la protection des droits de l'homme incluse dans la Constitution ou la CEDH si, précisément, l'organe de recours, en tant que juge indépendant et impartial, est en mesure de soulever les intérêts de l'intéressé et l'intérêt général.

Cet arrêt, qui porte toujours sur la législation ancienne mouture, revêt donc une importance fondamentale, y compris pour l'organe de recours dans sa nouvelle composition.

¹ Cour d'arbitrage, 25 janvier 2006, arrêt n° 14/2006, *M.B.*, 23 mars 2006, p. 16765 et.svt.
Voir également : www.arbitrage.be

TITRE 8

LA COMPOSITION ET LE FONCTIONNEMENT DU COMITE PERMANENT R

|

|

Le président Jean-Claude DELEPIÈRE, ses conseillers, Gérald VANDE WALLE et Walter DE SMEDT, ainsi que le président suppléant et ses membres, respectivement messieurs PRIGNON, MARIQUE et DE SMET, ont accompli la dernière année complète de leur mandat. Il est clair que la composition de la direction du Comité permanent R n'a pas changé par rapport à 2005.

Au moment de la rédaction du présent rapport d'activités, il est connu que monsieur DELEPIÈRE a mis son mandat à la disposition du Sénat. Monsieur RAPAILLE a été nommé en tant que nouveau président du Comité permanent R suite à une décision du Sénat du 30 mars 2006. Monsieur DEJEHANSART a été désigné en tant que président suppléant.

Comme annoncé dans le précédent rapport annuel¹, le Comité permanent R a engagé trois nouvelles personnes pour le Service d'enquêtes. Le Service d'enquêtes, dirigé par monsieur Paul VANDER STRAETEN, compte à nouveau cinq membres.

Les quatre enquêteurs sont détachés de la police intégré (deux de la police fédérale, un d'une zone de police locale) et du SPF Justice. Pour la première fois, le Service d'enquêtes compte désormais en son sein une enquêtrice.

En ce qui concerne le personnel administratif, un documentaliste a été engagé en 2005. Les collaborateurs administratifs sont dès lors à présent au nombre de neuf.

Après la levée de l'arrêt provisoire des engagements, le cadre administratif sera davantage renforcé en 2006 avec les recrutements précédemment approuvés par la Chambre, notamment en raison des modifications de la législation et de la charge de travail y afférente concernant l'organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.²

¹ Comité permanent R, Rapport d'activités 2004, Bruxelles, 2005 p. 144 et suiv.

² Voir Titre 7 – Les activités du Comité permanent R concernant l'organe de recours

Il y a régulièrement des confusions entre le Comité Permanent R et la Commission chargée du suivi du Comité Permanent R. La Commission du suivi exerce le contrôle sur le fonctionnement du Comité Permanent R, vérifie la prise en considération des dispositions de la loi et du règlement d'ordre intérieur. La Commission du suivi se réunit notamment pour (a) examine, avant publication et en présence des membres de chaque Comité Permanent, les rapports annuels des Comités Permanents (b) examine les projets de budgets des Comités Permanents, (c) exercer le contrôle sur le fonctionnement du Comité Permanent dans les cas prévus par les articles 52 à 55 de la loi du 18 juillet 1991 portant sur le contrôle des services de police et de renseignement (MB, 26 juillet 1991).

Au côté de la présidente du Sénat, Madame LIZIN, font également partie de la Commission concernée, Monsieur VANDENHOVE, Madame DEFRAIGNE, Monsieur VANDENBERGHE et Monsieur WILLE.

Outre l'exercice de ses activités légales – entre autre des enquêtes de contrôle, des enquêtes judiciaires,... - qui constituent le *core business* du Comité permanent R, le Comité R investit une partie de son temps et de ses moyens dans le fonctionnement de sa propre institution. Il accorde une attention particulière aux activités qui relèvent du domaine du fonctionnement interne, des affaires du personnel, du budget, du soutien matériel et logistique, de la sécurité, ... Vu sa moindre importance, cette partie ne sera que brièvement abordée.

Par son statut autonome, le Comité permanent R, qui dépend, il est vrai, du Parlement, doit prendre lui-même toutes les dispositions relatives à sa propre gestion.

Une tendance remarquée et croissante est que le Parlement, et plus particulièrement la Chambre des représentants, sous les traits de la Commission de la comptabilité présidée par monsieur DE CROO, a de plus en plus tendance à soumettre au même régime les diverses institutions à dotation qui dépendent du Parlement. Ce constat a déjà été mentionné dans un précédent rapport³ dans le cadre de la présentation des moyens et des comptes et s'étend aujourd'hui à d'autres domaines, tels p. ex. celui de la réglementation de certains coûts.

Comme auparavant, le Comité permanent R souligne qu'il se soumet sans problème à toutes les consignes et mesures de contrôle requises. Il demande seulement que l'on tienne compte des spécificités de sa mission et de la taille limitée de son organisation.

³ Comité permanent R, *Rapport d'activités 2004*, Bruxelles, 2005, pp.145 et suivantes

Une dotation d'un montant de 2 480 865 millions d'euros a été approuvée pour l'exercice 2004.

Cette année s'est clôturée avec un boni de 560 939,55 euros, qui seront remis à la disposition du Parlement après approbation par la Chambre des représentants et rapport de contrôle de la Cour des comptes.⁴

Pour 2005, une dotation de 2 700 000 millions d'euros a été octroyée.

Au moment de la rédaction de ce rapport d'activités, l'exercice 2005 n'était pas encore officiellement clôturé en raison de l'absence de plusieurs factures importantes, qui n'ont donc pas pu être réglées.

Tout semble néanmoins indiquer que 2005 se clôturera également par un excédent important, essentiellement en raison de la durée du recrutement qui est également en partie due à l'arrêt temporaire des engagements. Cet effet se ressentira encore en 2006. Ensuite, le boni se réduira structurellement.

⁴ Voir aussi : Chambre des Représentants, Cour d'arbitrage, Conseil supérieur de la Justice, Commissions de nomination pour le notariat, Cour des comptes, Comités permanents de contrôle des services de police et de renseignements, médiateurs fédéraux et Commission pour la protection de la vie privée: les comptes de l'année budgétaire 2004; les ajustements des budgets de l'année budgétaire 2004 et 2005; les propositions budgétaires pour l'année budgétaire 2006, rapport fait au nom de la commission de la comptabilité, 8 décembre 2005, DOC 51 2139/002.

CHAPITRE 5	LES RELATIONS AVEC DES ORGANES DE CONTRÔLE ETRANGERS
-------------------	---

1. LA RENCONTRE AVEC L'AUTORITE DE CONTRÔLE NÉERLANDAISE

Les 13 et 14 avril 2005, une délégation du Comité permanent R fut reçue à La Haye par la « Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten » (CTIVD).

Le 1^{er} juillet 2003, cet organe de contrôle néerlandais a débuté ses travaux. L'établissement de la Commission est réglé par la loi sur les services de renseignement et de sécurité entrée en vigueur le 29 mai 2002.⁵

Depuis la création de cette autorité de contrôle néerlandaise, les deux institutions ont eu divers contacts formels et informels.

Après une visite du CTIVD à Bruxelles en 2004, le Comité permanent R fut invité à venir visiter La Haye.

Les sujets suivants étaient notamment à l'ordre du jour :

- une présentation du fonctionnement des deux institutions ;
- les modifications et projets de modification de la législation en matière de renseignement ;
- les conséquences de la menace du terrorisme et de l'extrémisme pour le contrôle ;
- la problématique de la relation des services de renseignement avec les autorités judiciaires ;
- les relations avec d'autres organes de contrôle étrangers et la création d'un collège d'organes de contrôle européens.

En outre, il y a eu des rencontres avec l'ambassadeur belge à La Haye et le coordinateur néerlandais des services de renseignement et de sécurité. Ce dernier a pour mission la concertation régulière entre les ministres concernés pour ce qui est des services de renseignement et de la préparation des politiques de coordination (art. 4, 3a Wiv)⁶ et la coordination de l'exécution des tâches des services de renseignement (art. 4, 3b Wiv).

Ces discussions ont été très utiles à tous égards pour le Comité permanent R, puisque ces deux organes de contrôle parlementaires ont un mandat similaire dans deux pays voisins aux nombreuses similitudes.

⁵ Voir *Nederlands staatsblad (Stb.)*, 2002, 148 (ensuite cette loi a été modifiée par la loi du 23 avril 2003, Stb. 212) (abrégé Wiv). Voir aussi : Jaarverslagen van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (WWW.ctivd.nl). En ce qui concerne le Règlement d'ordre van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, nous nous référons à leur récent rapport annuel 2005-2006, pp; 33 et suivantes.

⁶ *Nederlands Staatsblad (Stb.)*, 2002, 148

L'échange d'informations, ayant pour but d'améliorer le fonctionnement et donc la qualité du contrôle, repose sur une confiance et une discrétion mutuelles.

2. LA PARTICIPATION AU COLLOQUE DU « COMITÉ CANADIEN DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT ET DE SÉCURITÉ »

Ayant confronté sa propre expérience à celle d'autres organes de contrôle étrangers, le Comité permanent R attire l'attention sur l'existence d'une problématique récurrente : quelle que soit la structure mise en place, l'exercice d'un contrôle sur les services de renseignement et de sécurité est une source de tension constante qui donne lieu à des prouesses d'équilibre entre le caractère secret des missions d'une part, et la garantie de la transparence due envers le Parlement, les autorités politiques et le public d'autre part.

Les 18 et 19 mai 2005 se tint, à Ottawa (Canada), un symposium international intitulé : « *Making national security accountable: international perspectives on intelligence review and oversight* », avec e.a. le contrôle des services nationaux de renseignement et de sécurité et l'exercice d'équilibre dont question ci-dessus comme sujet de discussion. Ce symposium était organisé par le *Canadian Center of Intelligence and Security Studies*, la *Norman Patterson School of International Affairs*, la *Carlton University* et le comité canadien de surveillance des activités de renseignement de sécurité. Ce dernier comité est mieux connu chez nous sous sa dénomination française « *Comité de surveillance des activités de renseignement de sécurité* », et fut, en tant qu'un des premiers organes externes de contrôle des services de renseignement, une source d'inspiration pour la législation qui vit le jour en 1991 en Belgique. Ce symposium fut d'ailleurs organisé à l'occasion du 20^e anniversaire de cette organisation collègue canadienne.

De plus, cette conférence s'inscrit dans un cycle de réunions biennales similaires entre organes de contrôle, cycle pour lequel des rendez-vous ont déjà été fixés en juin 2007 aux Pays-Bas. Ci-après nous développeront les divers exposés. Malgré la diversité et parfois la contradiction parmi les différents orateurs, nous tentons de proposer ici une synthèse thématique.

2.1. Le contrôle des services de renseignement et de sécurité

Un nombre important d'orateurs a présenté une typologie des différentes formes de surveillance et de contrôle des services de renseignement et de sécurité. Ce qui étonne est le fait que le contrôle et la législation sur laquelle il se fonde sont relativement récents et s'intègrent dans le cadre du démantèlement post-guerre froide. C'est le cas tant pour la législation sur le contrôle que pour la législation ou la modification de la législation relative aux missions et moyens des services de renseignement.

Plusieurs orateurs reconnaissent un nouvel équilibre nécessaire afin de rétablir la balance après que les services de renseignement et de sécurité aient reçu des moyens et missions bien plus vastes pour lutter contre le terrorisme international. La question de savoir si cet équilibre a réellement été atteint a dès lors été maintes fois soulevée. La situation varie bien sûr selon les divers pays, tout comme l'avis des experts en la matière d'ailleurs.

D'une manière générale, nous avons pu constater qu'un contrôle particulier des services de renseignement et de sécurité, quand il existe, n'est pas une compétence exclusive. Il est presque partout combiné à une responsabilité politique.

Cela peut aller de la responsabilité politique du gouvernement et des ministres compétents, du contrôle interne par le service de renseignement, du contrôle par le pouvoir judiciaire, aux habilitations octroyées par les instances judiciaires (warrants), en passant par le contrôle parlementaire exercé par une commission spéciale (temporaire ou permanente) de ce parlement ou le contrôle confié à un organe externe indépendant.

Lorsqu'un organe de ce dernier type existe, il est généralement considéré comme la forme la plus prononcée de contrôle des services de renseignement.

La première conclusion que nous pouvons tirer est que le contrôle des services de renseignement et de sécurité n'opère pas d'un vide juridique ou social mais au contraire est indissociable - dans un jeu subtil – à d'autres formes de contrôle.

L'existence d'un organe de contrôle indépendant est toutefois peu significative en soi. Tout dépend bien sûr du mandat de cette institution, de sa composition, de la possibilité de prendre des initiatives et de mener des enquêtes. La question de savoir dans quelle mesure l'organe de contrôle peut imposer son contrôle au service de renseignement et de sécurité est bien entendu primordiale.

La complexité de cette situation et la différence entre les pays sont bien sûr liées à la nature et aux missions des services de renseignement proprement dits. Même si les participants à ce symposium provenaient de démocraties parlementaires, les divers services de renseignement respectifs n'ont évidemment pas les mêmes dimensions et mandats. Les principales différences résident dans la question de savoir si le service dispose également d'un mandat policier (comme le FBI par exemple) et, plus encore, s'il remplit une mission offensive. Une mission leur est toutefois commune : « defending democracy against internal and external menaces without destroying democracy ».

A l'opposé des services de renseignement et de sécurité, se trouvent les représentants des pouvoirs législatif et exécutif. Cette relation entre ces derniers et l'organe de contrôle ne coule pas non plus de source ; plusieurs orateurs soulignent le danger que peuvent présenter des informations sensibles dans des mains politiques. Le contrôle exercé par des politiques ne vise pas des résultats politiques mais a pour but de déterminer ce que les services de renseignement doivent faire ou non. Enfin, la relation avec les autorités judiciaires peut également poser problème. Non seulement, les services de renseignement et les autorités judiciaires n'emploient pas du tout les mêmes méthodes de travail. En outre, les services de renseignement estiment souvent que les représentants des tribunaux n'y connaissent pas grand-chose en matière de renseignement, tandis que les autorités judiciaires pensent que les tribunaux doivent faire leur travail et que les services de renseignement n'ont aucune prérogative.

A l'intersection de tous ces acteurs, l'organe de contrôle doit s'acquitter d'une tâche ardue, ce qui fit d'ailleurs dire à un orateur : « review is an art, not a science ».

Malgré la diversité des services de renseignement et de leurs organes de contrôle respectifs, deux systèmes plus ou moins distincts semblent exister. Ils suivent, et ce n'est pas un hasard, la même orientation dans la séparation entre le « common law », d'une part, et le droit continental européen, d'autre part. La tradition anglo-saxonne a en effet davantage recours à l'inspection interne, aux habilitations spéciales de juges et au contrôle exercé par le Parlement, sans organe de contrôle indépendant. Sans pouvoir parler de modèle européen commun, certaines similitudes entre des pays tels que la Suède, la Norvège, les Pays-Bas et la Belgique existent.

Pour rendre la situation encore plus complexe, nous ne pouvons à un moment précis brosser un tableau complet sans reconnaître le rôle majeur de la vaste communauté internationale du renseignement. Ce réseau de services des différents pays est nécessaire au bon fonctionnement des services mais peut également être utilisé pour esquiver le contrôle.

Cette dernière remarque s'applique tant aux services de renseignement qu'aux départements et gouvernements, qui se servent, souvent à bon mais parfois aussi à mauvais escient, du réseau international pour dissimuler ou blanchir des informations.

A cet égard, de nombreux orateurs soulignent la relation particulière entre l'organe de contrôle et les services de renseignement. Cette relation repose sur une entente efficace dans laquelle une tension saine peut exister entre les deux acteurs. Les services nourrissent une certaine réticence à l'égard du contrôle, et ce, non par mauvaise volonté mais généralement parce qu'ils sont convaincus de remplir leur mission.

2.2. Le contrôle des services de renseignement à l'heure des menaces terroristes

Il est largement répandu que les services de renseignement sont confrontés, depuis la fin de la guerre froide, à un autre ennemi que les Soviétiques ainsi qu'à d'autres menaces. Ce présent ennemi est toutefois plus difficile à identifier et à contrôler. Ainsi, par exemple, le terrorisme revêt de nouveaux aspects internationaux, sociaux, ethniques et religieux. Aujourd'hui, il apparaît également de plus en plus clairement que ce danger ne vient pas exclusivement de l'étranger mais est implanté dans notre (nos) propre(s) communauté(s), que ce soit sous la forme de l'action, du recrutement ou du soutien logistique et financier.

Cette menace exerce une pression non négligeable sur les dirigeants et les services de renseignement. Le contrôle ne doit pas représenter une entrave à l'efficacité et l'utilité de ces services. La principale mission du service de renseignement consiste à informer correctement les autorités et le public à propos d'éventuelles menaces. L'organe de contrôle doit suivre ce processus de très près. Cela suppose donc qu'il doit s'intéresser tant au respect des droits de l'homme qu'à la gestion et à la qualité de l'analyse.

Ces deux éléments sont trop souvent considérés comme opposés.

Les exemples étrangers de services qui furent soumis à de fortes pressions pour neutraliser les menaces démontrent, dans certains cas, qu'une utilisation inappropriée des moyens a un effet contre-productif. Ainsi, la focalisation sur certains groupes culturels ou ethniques de la société rend ces mêmes groupes plus sensibles à la radicalisation et au recrutement.

Ces remarques critiques ne contredisent pas l'opinion de la plupart des représentants d'organes de contrôle, qui estiment que les services de renseignement doivent bénéficier de moyens suffisants pour remplir leur difficile mission.

2.3. Remarques finales

Sans toutefois pouvoir parler de réelles conclusions, se dégage un consensus à l'égard des éléments suivants,.

Une première constatation est que, dans le modèle d'une démocratie et d'un État de droit fortement ancrés, le pouvoir exécutif doit être soumis à un contrôle.

En outre, de nombreux exemples montrent clairement que malgré leur dévouement, leur professionnalisation et leurs moyens supplémentaires, les services de renseignement ne sont pas à l'abri d'un échec, par exemple en ne parvenant pas à identifier ou à s'attaquer à temps à une menace ou en traitant injustement des citoyens. Compte tenu des pressions accrues qui résultent de la priorité donnée à la menace terroriste, un contrôle efficace des services de renseignement et de sécurité est dès lors primordial.

Le contrôle des services de renseignement prend diverses formes selon les pays. Le modèle d'un organe de contrôle externe est surtout en vogue sur le continent européen. Ce système présente pour principal avantage de pouvoir rester dans le « circle of secrecy » et de pouvoir ainsi vérifier toutes les informations et acquérir un savoir-faire. En outre, contrairement aux inspections internes, par exemple, il reste indépendant des services et du pouvoir exécutif.

Quelle que soit sa forme, le contrôle est une mission délicate.

Vis-à-vis des services de sécurité et de renseignement et du pouvoir exécutif, l'organe de contrôle doit veiller à ne pas prendre la place du service de renseignement ou de sa direction et à ne pas devenir l'instrument du gouvernement.

D'autre part, le contrôle doit être efficace et tenir compte du fait que d'autres facteurs interviennent dans ce secteur, tels que par exemple le réseau international de services de renseignement et d'autres services de police et de renseignement, y compris des services privés.

De plus, les organes de contrôle n'ont pas le monopole du contrôle. Ils partagent cette tâche avec les organismes de contrôle internes, les instances des pouvoirs exécutifs, judiciaire et, last but not least, législatif. Le rôle du secteur privé et, plus particulièrement, des médias ne doit pas non plus être sous-estimé.

Enfin, la place de l'individu - le citoyen - ne peut pas être négligée. S'il est bien loin de toutes ces considérations, pour lui, la sécurité, les droits de l'homme et la crédibilité de l'État de droit sont bel et bien des valeurs importantes.

CHAPITRE 6 PARTICIPATION DU COMITÉ PERMANENT R A DES SEMINAIRES, JOURNEES D'ETUDE ET COLLOQUES

1. JOURNÉE D'ÉTUDE SUR LE RÔLE DES ORGANISATIONS INTERNATIONALES DANS LA LUTTE CONTRE LE TERRORISME

La journée d'étude consacrée au rôle des organisations internationales dans la lutte contre le terrorisme a été organisée le 17 mai 2005 par la Commission du suivi du Comité permanent R, conjointement avec le *World Anticriminal and Antiterrorism Forum (WAAF)*, une organisation non-gouvernementale internationale composée de parlementaires et d'anciens ministres de pays comme l'Allemagne, la Russie, l'Israël, la Belgique, les États-Unis, ...

Le but de cette journée était d'examiner le rôle spécifique et les possibilités d'action des différentes organisations internationales contre le terrorisme. Des représentants de l'Union européenne, les Nations Unies, l'OTAN et l'OSCE, ainsi que des experts, y ont pris la parole. Ces exposés ont été suivis d'échanges de vues entre les participants.

2. RAPPORT DE LA CONFÉRENCE SUR « INFORMATION OPERATIONS »

La conférence sur 'Information operations' qui s'est tenue à Malvern (Grande Bretagne) les 4, 5 et 6 juillet 2005, a particulièrement attiré l'attention du Comité permanent R, d'une part pour la relation supposée entre le sujet et le secteur des renseignements et, d'autre part, pour la présence d'un officier de l'armée belge en tant qu'orateur.

2.1. Qu'entend-on par 'information operations' ?⁷

Lors d'"information operations' (dénommé ci-après IO) on peut imaginer qu'une unité militaire en mission de maintien de la paix qui met sur pied une campagne de renseignement axée sur la population civile locale. Durant cette campagne, cette unité expose son objectif et appelle la population à déposer les armes. A cette fin, cette unité entre en contact avec la population, utilise des tracts, émissions de radio,

Le champ d'action d'une IO est toutefois beaucoup plus étendu et porte même parfois un autre nom.

Certains pays parlent de PSYOPS (« psychological operations ») ou STRATCOM (« strategic communications »). Pour les uns, ces dénominations sont des synonymes, alors que pour les autres, elles désignent une toute autre réalité.

Nous retiendrons dans ce qui suit le concept plus neutre et plus vaste d'OI et mentionnerons la définition retenue par les États-Unis : « *les actions entreprises en vue de nuire aux informations et systèmes d'information de l'ennemi tout en défendant ses propres informations et systèmes d'information (Joint Pub 3-13, rédigé en 1998)* ».

⁷ ARMISTEAD, E.L., (ed:), *Information operations : warfare and the Hard Reality of Soft Power*, United States, Brassey's Inc., 2004, 277 p.

Un grand nombre de techniques ou d'actions principalement mais pas exclusivement militaires correspondent à cette définition.

- actions militaires visant notamment la destruction (p. ex. : des lignes de communication ennemies) ;
- leurre de l'ennemi ;
- cyberattaques et défense contre les cyberguerres ;
- attaques électroniques ;
- opérations psychologiques (psyops) ;
- divulgation d'informations à la presse et au public (public affairs, public information) ;
- sécurité des opérations ;
- infosec et contre-espionnage ;
- contacts avec les autorités civiles et la population de la zone concernée.

Ces composantes de l'IO peuvent se manifester tant sur le plan stratégique, opérationnel que sur le plan tactique.

Ces tâches ne sont pas l'apanage des organisations militaires. Les dirigeants politiques (avec leur stratégie et capacité de renseignement), la diplomatie et les partenaires privés (tant les entreprises militaires privées que les ONG), sans oublier les médias, peuvent jouer un rôle dans ce domaine.

Les critiques affirment dès lors que cette description est tellement vaste qu'elle ne peut servir de définition.

D'autres pays se basent davantage sur le terme PSY-OPS qui est considéré comme une activité plus ciblée. La Défense belge est favorable à l'utilisation des IO comme philosophie et des PSYOPS comme l'un des éléments qui contribuent à l'ensemble des IO.

La définition britannique des PSYOPS s'énonce comme suit : « *activités planifiées, culturellement sensibles, conformes à la vérité (...) qui poursuivent des objectifs politiques et militaires en influençant les attitudes et comportements* ».

En règle générale, l'on considère que par le biais de l'appareil politique et militaire propre, qui en principe se trouve sur la même longueur d'onde, on usera de techniques PSYOPS pour influencer la population de la zone d'action, les parties en présence et le commandement de l'ennemi, de manière à ce qu'ils se plient un maximum aux souhaits propres avec, pour objectif principal, la garantie de la protection de ses propres troupes et la création d'une situation sûre et tranquille dans la zone d'opération.

Ces activités varient bien sûr selon le lieu et la culture (voir infra). Cela peut, par exemple, signifier que l'on tente de gagner la population à sa cause ou de préserver sa neutralité, de mettre sous pression le commandement de l'adversaire, (par exemple pour qu'il s'avoue vaincu ou fasse des concessions) et, dans le même temps, fournir à ses propres troupes et aux puissances alliées des informations, et tout cela, sans la moindre contradiction.

2.2. Contexte historique

Avant que le concept d'IO (ou similaire) ne soit accepté - ce qui varie d'un pays à l'autre - des renseignements étaient utilisés lors de situations de crise ou de guerres également. Pendant la Deuxième Guerre mondiale, tant les alliés que l'Allemagne nazie usèrent fréquemment de la propagande. La science (les sciences naissantes de la communication et de la psychologie), les arts et même le divertissement furent placés sous le signe de la guerre.

Durant la Guerre Froide, l'on assista également à une lutte du renseignement visant la conquête des esprits, par exemple par la création de stations de radio qui essayaient sans cesse d'affaiblir les régimes ennemis.

Certains théoriciens font même référence au guerrier chinois Sun Tzu qui, il y a environ trois mille ans, reconnaissait l'importance des connaissances et informations, tant de l'ennemi que de ses propres capacités.

On peut se poser la question de savoir comment il se fait, surtout dans les milieux militaires, qu'une sorte de battage publicitaire convainc pays après pays d'adopter le nouveau concept et de déployer des moyens spécifiques dans cette optique ?

Plusieurs facteurs sont à l'origine de ce phénomène. Nous en énumérons quelques-uns ci-après, pas nécessairement par ordre d'importance.

Tout d'abord, une révolution technologique a bouleversé le secteur des communications et de l'informatisation, dont les applications touchent tous les domaines (également ceux de l'armement et des techniques de renseignement, e.a. SIGINT, IMINT, OSINT...) ainsi que les moyens de communication eux-mêmes.

Ensuite, le rôle croissant des médias, notamment dû aux progrès techniques, a lui aussi radicalement changé la donne. Prenons, par exemple, la guerre du Vietnam pour laquelle il est communément admis (à tort ou à raison) que les États-Unis ont perdu la guerre en raison des médias. Depuis lors le rôle du quatrième pouvoir n'a cessé de croître.

En raison de cet état de fait, l'appareil militaire est devenu très prudent à tous égards et tente si pas de contrôler les médias (par des « embedded journalists »), d'au moins les gagner à leur cause. Il est cependant un fait que le gouvernement, du moins des pays démocratiques, ne peut plus contrôler les informations.

Ces évolutions sont encore accentuées par la rapidité avec laquelle les informations sont échangées avec la zone opérationnelle. CNN et Al Jazeera ont fait entrer la guerre dans les foyers. Conséquence : les commandants militaires ou politiques, qui s'entourent de plus en plus (par obligation) de porte-parole, spécialistes des médias et conseillers juridiques, doivent faire des déclarations quelques heures après un incident survenu de l'autre côté de la planète, alors que les troupes qui sont sur place ne sont parfois pas encore en mesure d'avoir une vision complète de la situation.

Autre fait tout aussi important : les missions militaires et la façon dont la guerre est menée évoluent en raison du nombre croissant de missions pacifistes qui favorisent visiblement un rôle plus actif des puissances intervenantes.

Un glissement perceptible s'opère également dans l'organisation de l'ennemi. Il apparaît qu'il s'agit de moins en moins souvent d'une force armée nationale d'un État plus ou moins organisé. Au contraire, on a de plus en plus souvent affaire à des milices, rebelles, guerriers, terroristes....

L'on peut également ajouter que malgré sa nouvelle organisation, l'ennemi n'utilise pas moins les moyens de renseignement et de communication. La Belgique a pu expérimenter le rôle perfide joué par une radio telle que celle des « Mille Collines » dans la crise du Rwanda. Les insurgés et terroristes irakiens utilisent à leur tour de manière très réfléchie les chaînes de télévision et Internet pour montrer et justifier leurs actions violentes. Les IO sont en fait devenues incontournables pour ne pas céder devant les opérations d'information de l'ennemi. Remarquons que les attaques du 11 septembre visaient des objectifs symboliques et médiagéniques.

Enfin et sans vouloir être complets, relevons que les IO organisées à la place de ou parallèlement à des actions militaires énergiques produisent des résultats, et ce, souvent en engendrant moins de frais et en faisant moins de victimes que les formes classiques de la guerre.

Un exemple d'IO réussie : l'opération militaire « Tempête du désert » menée en Irak après l'invasion du Koweït. Les troupes de la coalition purent vaincre assez facilement les unités irakiennes après que celles-ci furent non seulement surprises par une manœuvre tactique (préparée et combinée à une déception), mais aussi anéanties au sens propre comme au figuré par des bombardements de munitions et de propagande, et cela, pendant que les moyens de communication et d'observation des Irakiens étaient détruits.

2.3. Les IO sur le plan politique et éthique

Le déploiement de moyens militaires et surtout leur objectif suscitent généralement d'intenses débats politiques et juridiques à connotation éthique.

La mise en œuvre de « moyens modérés », comme l'on pourrait qualifier les OI, peut ne poser aucun problème par rapport à des arguments plus fermes.

Lors de cette conférence, presque tous les représentants militaires ont souligné l'importance de l'utilisation de renseignements véridiques. L'on parle d'informations « blanches » par opposition aux informations « noires » ou « grises ». Pour eux, seules des informations correctes peuvent être utilisées si non la crédibilité des actions et de ceux qui ont fourni les informations est perdue.

Les critiques, qui avaient aussi leur place à la conférence, veulent mettre en doute cette thèse. Parfois, la pensée occidentale a décrit la vérité comme inaccessible et l'opinion selon laquelle la perception est primordiale est de plus en plus présente. Dans un tel état d'esprit, l'on ose alors « user avec parcimonie de la vérité » lorsque c'est pour 'la bonne cause'. Ils mettent dès lors en garde contre la manipulation qui doit influencer l'adversaire ET convaincre l'observateur neutre et la nation. C'est pourquoi l'un des orateurs a évoqué le 'langage Orwellien' utilisé lors des opérations militaires.

Pour ces raisons, l'OTAN a explicitement opté pour une directive (MC-422) dans le but de différencier les opérations d'information (IO) et les informations publiques (IP). Les IO sont considérées comme un moyen d'influencer les politiciens de la partie adverse, tandis que les PI ont pour objectif d'apporter des informations ouvertes, fiables et actuelles. Ces deux concepts ont de nombreux points communs, mais la distinction doit être clairement établie afin de protéger et garantir la crédibilité des informations publiques. En aucun cas, celles-ci ne peuvent être subordonnées à des experts en communication spin doctors ou en PSYOPS.

L'un des orateurs donna un exemple qui démontre le caractère délicat de cette relation. En Irak, un porte-parole militaire (U.S.) a annoncé à CNN une offensive contre la ville de Fallujah trois semaines avant la date. Son intention était-elle d'informer ou d'attirer les insurgés dans la ville et donc dans un piège ?

Le point de vue de l'OTAN semble en forte contradiction avec la politique américaine récente en la matière qui a mis à exécution le concept de communication stratégique. STRATCOM, à son tour, est défini comme étant « *la transmission de thèmes et messages gouvernementaux intégrés et coordonnés qui aident les intérêts et la politique des États-Unis par des efforts interdépartementaux synchronisés soutenus par la diplomatie, les informations gouvernementales et les opérations d'information militaires, et ce, en concertation avec d'autres actions de nature économique, politique, informative et militaire.* »⁸ L'accent est mis sur le fait qu'il s'agit uniquement 'd'informations blanches' et que la déception militaire, par exemple, porte sur un autre domaine.

Cette discussion, qui est loin d'être close, pourrait bien mettre au jour une différence de principe entre les alliés de l'OTAN. La question est de savoir si dans cette société d'information globalisée, il est encore possible de maintenir une distinction entre IO et IP ? Les points de vue divergents entre les autorités militaires et politiques du monde entier ne disparaissent-ils pas ? Ce qui est sûr, c'est que même l'approche la plus objective tant de l'information publique que des opérations d'information sont déterminées par les objectifs et les moyens dans un contexte politique.

Cette relativisation pourrait conduire à ce que les informations ne soient plus un reflet de la vérité. Pour la Défense belge, l'Information publique implique une reproduction fidèle des informations. L'objectif premier des PSYOPS consiste à protéger ses propres troupes et à créer une situation calme et sûre dans la zone d'opération. Les PSYOPS OTAN, ratifiés par la Belgique, donnent toujours la « vérité ». Sachant que la « vérité absolue » n'existe pas, il est clair que « la vérité » est elle aussi liée à la perception. Il fut toutefois souligné que les PSYOPS OTAN belges ne feront jamais de la désinformation.

2.4. L'application des Information Opérations dans les zones actuellement en guerre ou en crise

Les applications actuelles des IO ont été illustrées par deux exemples concrets très différents.

Commençons par un résumé très sélectif de l'exposé du lieutenant-colonel Salamonowicz de la composante Air belge. Cet officier de réserve remplaçait l'orateur annoncé, le major Segers, officier d'état-major pour ACOS Ops & Trg, Concepts & Plans, Cel PSYOPS.

⁸ (Définition de travail approuvée par le président des chefs d'état-major en septembre 2004, traduction libre)

Depuis 2000, l'officier de réserve travaille dans le secteur des PSYOPS. Il souligna le fait que les Belges ne parlent pas de « PSYOPS » mais « d'opérations d'information » (OI), conformément à la volonté de la Défense, qui estime que le concept de « PSYOPS » a encore une connotation négative.

Tout d'abord, l'orateur attira l'attention sur les capacités militaires très différentes d'un pays à l'autre. Pour un petit pays comme le nôtre, cette différence se répercute bien sûr aussi sur nos capacités et ambitions en matière d'OI. Pourtant, comme le dit Salamonowicz, « Good things may also come in small packages ». Cette discipline militaire trouva son origine en Belgique dans le drame du Rwanda où, comme expliqué ci-dessus, les opposants à la pacification et aux opérations de maintien de la paix utilisèrent entre autres la campagne de haine de la tristement célèbre station de radio « Mille Collines ».

Au fil des ans, cette discipline militaire est devenue un véritable module PSYOPS, mais aux ambitions modestes. Sur le plan opérationnel, ces ambitions portent sur des opérations d'évacuation non offensives et sur un soutien modulaire d'une puissance médiane. Sur le plan tactique, l'armée belge est en mesure d'offrir un soutien PSYOPS modulaire aux troupes terrestres déployées. Un module PSYOPS se compose d'éléments planification, de développement de produit, de radio et enfin d'équipes PSYOPS tactiques (Tactical PSYOPS teams – TPT dans le jargon de métier) dans la zone d'opération. Quant aux capacités, l'armée belge aspire à cinq modules permanents composés de personnels actifs et de réserve.

A titre d'exemple récent, l'orateur décrit la collaboration des PSYOPS au programme de coopération militaire (PMP) au Congo. Pour cela, il s'appuya sur le cycle standard des OI qui part d'une

- situation finale souhaitée
- la question de savoir comment les IO peuvent contribuer à cet objectif

1. *Quels sont les thèmes principaux ?*

Ici, la Belgique participait à la reconstruction d'une force militaire unifiée qui doit apporter la garantie d'une pacification durable ;

2. *Quels sont les objectifs des IO ?*

Un premier objectif consistait à créer les conditions de l'exécution réussie de la mission. Cet objectif fut étendu à des buts plus spécifiques, tels que limiter l'influence de la propagande ennemie, créer une image positive du contingent belge dans la région, promouvoir une armée congolaise professionnelle qui respecte les droits de l'homme,...

3. *Quels sont les groupes cibles des IO ?*

Comme c'est souvent le cas dans les opérations d'information, il y a différents groupes cibles: la population locale, les soldats de la nouvelle force militaire congolaise (1^{re} brigade), sans oublier les chefs locaux ;

4. *Quels sont les moyens déployés ?*

Il s'agit tant des moyens humains (cinq personnes) que matériels (haut-parleurs, imprimantes) ;...

5. *Quelles sont les méthodes utilisées ?*

Elles sont également très variées : entretiens avec les composantes de la population, impression d'une bande dessinée, diffusion de messages radio, intervention de troupes de théâtre de rue locales, « parrainage » d'événements sportifs, etc....

Pendant et après chaque opération, l'efficacité des opérations est évaluée et les leçons à tirer sont identifiées. Comme dans presque toutes les autres opérations, l'on souligne de nouveau l'importance de la connaissance de la situation par les responsables des PSYOPS et les autres troupes déployées où, par exemple, est mise en évidence l'importance d'une bonne communication avec les « chefs de coutumes », en plus bien sûr du contact avec la population en général.

Une autre situation se déroule en Irak, où les troupes américaines recourent activement aux IO pour lutter contre les insurgés/terroristes pour atteindre l'objectif du gouvernement américain. Comme expliqué ci-dessus, ces opérations sont mises en œuvre selon le concept de « strategic communications ».

Les porte-parole et commandants dans les QG et centres de presse ne sont pas les seuls concernés par ces opérations. La preuve en est donnée par la participation d'un ancien militaire, qui a conseillé et même évalué sur le terrain les IO des alliés et autorités irakiennes pour le compte de la société Rand corporation⁹ et ce, grâce à un contact étroit avec la population locale. Notons que dans ce domaine, la sous-traitance de tâches à des entreprises privées est également une réalité.

Son histoire, qui fut en grande partie confirmée par d'autres orateurs expérimentés dans cette campagne, est nuancée. Il va de soi que les moyens déployés n'ont rien à voir avec l'exemple belge et que des centaines de projets sont menés qui peuvent être considérés comme autant de batailles pour l'information.

Certains projets portent sur le court terme et d'autres sont plus permanents, mais sont toujours en confrontation avec les IO très efficaces de l'ennemi. Ici aussi, la connaissance du champ d'action joue un rôle clé inévitable dans la diffusion d'un message crédible et l'utilisation des erreurs de l'ennemi. Ce spécialiste laissa les définitions de côté et examina surtout les résultats. Ils ne lui donnèrent pas toujours entière satisfaction, malgré plusieurs succès, tels que p. ex. la guerre de l'information autour de l'offensive de Fallujah. Outre l'utilisation de la communication vis-à-vis de la presse internationale et américaine, les opérations portent également sur le soutien des médias pro-occidentaux. Surtout l'opération relative aux élections en Irak revêt un caractère important car elle fut couronnée de succès.

L'orateur souligna également la difficulté, par exemple, de sensibiliser la population à un système démocratique lorsque la majorité de cette même population ne connaît pas ces concepts et ignore même de quoi il s'agit. Il attira également l'attention sur la crainte des services occidentaux à l'égard de l'utilisation du thème de la religion, alors qu'il joue précisément un rôle clé, du moins lorsqu'il est utilisé avec prudence et sous les conseils des experts locaux.

⁹ Pour plus d'info, voir www.rand.org

Il insista également sur l'importance de l'élément visuel et d'un message simple (« sticky message ») et reconnut son utilisation souvent réussie par la partie adverse qui montre notamment à la population des images d'attaques réussies délivrant un message très simple (« occupation bad »).

2.5. Information Operations et renseignements

Terminons par quelques réflexions sur le lien entre les IO et le travail de renseignement. Il est étonnant de constater que de très nombreux spécialistes de cette discipline relativement nouvelle proviennent du secteur des services de renseignement. Cela semble pourtant logique puisque les renseignements et les IO se fondent tous deux sur l'utilisation d'informations.

Nous pouvons même affirmer que les renseignements précèdent chronologiquement les OI. Comme indiqué ci-dessus, les opérations d'information sont tributaires, durant leur phase de planification, de bonnes informations. Ce principe s'applique à tous les aspects des OI (tels que la destruction des moyens de communication ennemis, l'anticipation des commandants ennemis...). Les différentes sources des services de renseignement - qu'elles soient humaines, techniques ou publiques - recèlent un trésor d'informations et sont indispensables à la planification et l'exécution des IO.

Comme nous l'avons souligné plusieurs fois, la connaissance de la culture locale de l'ennemi ou de la zone d'action joue ici un rôle primordial et des renseignements de qualité peuvent faire la différence. Il existe également des différences. Par exemple, dans les IO (et ce n'est pas très fréquent lors de la collecte classique d'informations), il est très important de bénéficier d'une connaissance approfondie de ses propres objectifs et ce, tant au niveau militaire que politique, ce qui n'est pas toujours évident. On peut également remarquer que les IO font davantage appel à d'autres domaines de connaissance et spécialistes en la matière, tels que psychologues, sociologues, ethnologues, linguistes, spécialistes des médias...

Comme les IO subissent, selon les règles de l'art, une évaluation des conséquences et une appréciation globale, l'on pourrait supposer que le secteur des renseignements reçoit également un feed-back.

Puisque lors de cette conférence il n'a pas été mis l'accent sur les services de renseignement, cet aspect n'a pas été abordé. Il ne s'agit donc que d'une supposition toutefois étayée par les organigrammes des différentes structures d'IO de divers pays où l'on remarque chaque fois que les services de renseignement participent structurellement ou au moins fonctionnellement aux opérations d'information.

Idéalement, un échange de vues permanent devrait en fait avoir lieu entre les disciplines du renseignement et celles des IO.

Les IO peuvent dès lors être simplement considérées comme un client des services de renseignement. Un client relativement nouveau mais de plus en plus important des services de renseignement - surtout mais pas exclusivement - militaires. Bien que l'existence de l'essence même de ce que l'on nomme OI aujourd'hui fût déjà connue autrefois, les modifications sociales susmentionnées influencent également le travail des services de renseignement, dont la mission ne consiste pas à se fournir en informations. En revanche, leurs recherche et traitement des informations devront de plus en plus répondre aux besoins de ce nouveau client.

Nous pouvons imaginer que la frontière théorique entre les deux est très mince, voire inexistante dans certains cas. La production de renseignements est en effet une activité qui influence déjà en soi la réalité et dont le résultat, adapté à l'IO, influence le jugement de ses propres commanditaires.

Cela peut également comporter quelques dangers, du moins en théorie. Alors que nous avons déjà évoqué les relations éthiques et politiques des IO, le secteur des renseignements est également lié à un certain contexte social et politique en grande partie incontournable, mais qui risque également d'engendrer la production de rapports politiquement corrects, au mépris d'éléments objectifs.

S'il s'avérait que les renseignements sont manipulés, l'on pourrait tomber dans un cercle vicieux où les renseignements et les informations divulguées se renforcent mutuellement dans une certaine vision politique. Le pire scénario consisterait dès lors à ce que la déception, basée sur des renseignements manipulés, vise finalement sa propre opinion publique. C'est justement pour éviter pareille situation que l'OTAN interdit clairement de prendre sa propre opinion publique comme cible des programmes de PSYOPS.

Par souci de clarté, nous devons préciser que les participants et orateurs de cette conférence reconnaissent sans exception la primauté de la politique et de la démocratie. Lorsqu'en outre, l'on évoque les dangers de manipulations politiques, l'on pense au danger d'abus provenant d'une idéologie (de parti) politique spécifique.

Tant la phase de renseignement que les opérations d'information (respectivement input et output de l'information) doivent dès lors être soumises à une évaluation critique permanente, d'abord par les services concernés.

Ce danger est bien entendu moindre dans une société démocratique ouverte qui ne fait pas l'objet de menaces sévères ou de conflits.

2.6. Conclusions

L'importance croissante de l'information¹⁰ (d'aucuns parlent même d'une domination) est indéniable. Elle constitue dès lors un facteur toujours plus crucial dans la conquête ou le maintien du pouvoir. Tous les aspects de la vie et de la société (tels que la culture, l'économie ou la politique) le ressentent très clairement.

Il n'y a donc rien d'étonnant à ce que l'information revête un rôle de plus en plus grand dans l'entreprise militaire. Alors qu'auparavant, le renseignement était axé, pour les dirigeants militaires et politiques, sur l'obtention d'informations relatives aux capacités et intentions de l'ennemi, l'on remarque depuis quelques décennies que ces dirigeants utilisent de nouvelles techniques de renseignement pour soutenir leurs actions.

Nous ne voulons pas dire que les messages publicitaires remplacent les armes ou que les slogans tels que « *l'information est une arme* » il est indéniable que les autorités militaires - qui se montrent traditionnellement méfiantes à l'égard de la divulgation d'informations, a fortiori aux médias - utilisent de plus en plus l'information et les médias pour atteindre leurs objectifs en combinaison avec d'autres moyens.

¹⁰ Voir Toffler A., *The third wave*, London, Pan Books, 1980.

Étant donné les liens entre les opérations d'information et le travail de renseignement et étant donné le fait que le secteur des renseignements même se retrouve lui aussi dans une société d'information, il est très probable que cela ait, aujourd'hui et demain, une influence sur le fonctionnement des services de renseignement. De prime abord, cela semble être une affaire pour les services de renseignement militaires, mais cela ne doit pas se limiter à ce secteur, d'autant plus lorsqu'il est constaté, par exemple, que la lutte contre le terrorisme est une mission pour tous les services de renseignement, tant localement qu'à l'étranger. L'information à l'échelle nationale devient en ce sens aussi de plus en plus importante.

Il est quasiment impossible d'évaluer ce phénomène, pas seulement à cause des données faisant suite à une première exploration du thème, mais surtout parce qu'il concerne des activités très variées dans différentes situations.

Alors que l'on évoque ici les possibilités au moins théoriques de manipulation des informations - dans le sens de l'utilisation d'informations non conformes à la vérité -, il faut toutefois également souligner que ces dangers sont reconnus (cf. la doctrine de l'OTAN en la matière) et - que les spécialistes militaires présents à une conférence comme celle-ci ne craignent pas le débat et la critique notamment des scientifiques et journalistes.

Cette situation présente un défi pour les services de renseignement : ils doivent, peut-être plus qu'auparavant, prendre conscience, sans divulguer des informations confidentielles, du fait qu'ils opèrent dans une société d'information ; ce qui fait une différence évidente, tant pour leur collecte d'informations que pour la réalisation de leurs produits finis, c'est-à-dire les informations au profit de différentes autorités.

3. SÉMINAIRE SUR LES « LISTES TERRORISMES ».

La commission du Sénat chargée du suivi du Comité permanent R a pris l'initiative d'organiser un séminaire de travail le 12 juillet 2005 sur la genèse et la mise en œuvre des listes terroristes.

La Commission souhaitait plus particulièrement analyser les points suivants :

- Quelle procédure doit être respectée avant qu'une personne et/ou une organisation ne puissent figurer sur une liste terrorisme ?
- Une liste terrorisme a été adoptée en exécution des résolutions du Conseil de Sécurité des Nations Unies. Existe-t-il d'autres listes, au niveau national ou international, qui sont utilisées par les autorités publiques en Belgique ?
- De quelle manière la communication et la coordination peuvent-elles être assurées entre les différentes autorités publiques qui travaillent sur base des listes terrorismes ?
- Quelles sont les conséquences concrètes pour les personnes et/ou les organisations qui figurent sur une liste terrorisme ?
- Quelles sont les conséquences sur les droits fondamentaux des personnes dont le nom figure sur une liste terroriste ? Disposent-elles d'un droit de recours contre la décision de les répertorier sur une liste terrorisme ?

Outre les membres des deux commissions de suivi et du Comité permanent R et du Comité permanent P, des membres de la Sûreté de l'Etat, du SGRS, ainsi que des experts français et belges ont également été invités.

Au cours de ce séminaire, les membres de la commission sénatoriale ont demandé au Comité permanent R d'examiner plus avant cette problématique sous l'angle juridique national et international.¹¹

4. LE COLLOQUE 'MILITARY SATELLITES'

Un membre du Comité permanent R a participé les 5 et 6 juillet 2005 à Toulouse (France) à la conférence « Military satellites » organisée par l'association britannique International Quality and Productivity Center (IQPC Ltd).

Cette participation a permis au Comité permanent R de se tenir au courant des derniers développements des programmes européens de satellites militaires d'observation et de télécommunication, notamment les programmes Hélios 1 et Hélios 2.

Le recours à des systèmes d'observation spatiale tel qu'Hélios permet d'observer - en toute indépendance et en tout lieu - sans risquer de violer l'espace aérien des pays observés.

Le système Hélios est ainsi devenu un élément primordial pour le renseignement et les opérations militaires. En complément de systèmes terrestres, les satellites apportent une couverture mondiale et permanente. L'imagerie est au cœur du dispositif terrestre mais elle est également utilisée par les bases aériennes ou la Marine nationale.

Le système Hélios 1 est opérationnel depuis 1995 à l'issue du lancement du premier satellite Hélios 1A. Il a fonctionné avec deux satellites de 1999, année de la mise en orbite d'Hélios 1B, jusqu'au 21 octobre 2004. A cette date, le satellite Hélios 1B a été désorbité à la suite de problèmes techniques, après les cinq années de fonctionnement prévues. Depuis lors, le système fonctionne sur un satellite au profit des pays partenaires et au prorata de leur participation : la France (78,9 %), l'Italie (14,1 %) et l'Espagne (7 %).

Cette coopération dans le cadre du programme Hélios constitue une première pierre de l'édification d'une Défense européenne dans le domaine spatial. Ce projet se caractérise par la synergie qui existe entre le programme civil d'observation de la Terre Spot et les enjeux militaires, tant pour des raisons technologiques qu'économiques.

Un nouveau pas sera franchi dans la synergie civile-militaire avec le programme dual Pléiades. Pour la première fois, utilisateurs civils et militaires pourront partager un même système d'observation.

Lancé le 18 décembre 2004, Hélios 2 doit renforcer et améliorer les capacités existantes d'Hélios 1 et ce tant en matière de résolution que de délai d'accès à l'information et de capacité de prises de vue. Le nouveau système permet également le ciblage, le guidage, la préparation de missions et la vérification des dommages de combat. Il est réalisé dans le cadre d'un partenariat entre la France (95 %), la Belgique (2,5 %) et l'Espagne (2,5 %).

D'autres États européens, membres de l'Union européenne ou de l'Otan, ont fait connaître leur intérêt concernant le système Hélios 2, en particulier l'Italie et la Grèce avec qui les discussions pour une éventuelle participation ont commencé.

¹¹ Voir ci-dessus Titre 6 – Etude et activités - Chapitre 3 – Listes terroristes

La France a mis en oeuvre une politique destinée à fédérer l'ensemble de ses partenaires autour d'une vision commune de l'utilisation militaire de l'espace. Simultanément à la rédaction d'un document définissant 'un besoin opérationnel commun' en observation spatiale, aujourd'hui signé par les chefs d'état-major des Armées français, allemand, espagnol, italien, belge et grec, il existe plusieurs projets de coopération dans le domaine de l'observation spatiale (optique et radar).

La Belgique a signé, le 13 juillet 2001, un arrangement de coopération relatif à sa participation au développement et à l'utilisation du système Hélios 2 à hauteur de 2,5 %. Un arrangement particulier, signé le 31 mars 2003 par la France, l'Espagne, l'Italie et la Belgique autorise en outre la fourniture d'images Hélios 1 à la Belgique, à des fins de formation à l'imagerie spatiale.

L'Allemagne n'a pas d'accès au système Hélios 1. Un arrangement de coopération, relatif à la fédération des systèmes Hélios 2 et SAR-LUPE, a été signé par les ministres de la Défense français et allemand le 30 juillet 2002. Dans le cadre de cette coopération, la France fournit des droits d'accès à l'Allemagne sur son système Hélios 2 en contrepartie de droits d'accès fournis à la France sur le système allemand SAR-LUPE. Celui-ci comprend cinq satellites d'observation radar SAR dont le premier exemplaire devrait être lancé en février 2006. La constellation devrait être complète dans le courant du second semestre 2007. La durée de vie prévue du système, avec quatre satellites opérationnels au minimum, est de dix ans.

L'avantage du satellite radar est de pouvoir fournir des images malgré une couverture nuageuse. Ceci est particulièrement utile pour l'observation des zones humides de l'Afrique Centrale. Mais ces images demandent beaucoup plus d'expertise technique pour être interprétées.

Le major Luc PETERS, responsable renseignements « capability design », ACOS STRAT, était l'un des orateurs de ce séminaire. Son exposé insistait sur la complémentarité de l'imagerie spatiale par rapport aux autres sources de renseignement. Pour obtenir une bonne analyse d'une image spatiale, il faut avoir recours à d'autres informations y compris OSINT, HUMINT, COMINT, ...

5. LES RENCONTRES POUR L'INNOVATION, LA COMPÉTITIVITÉ ET LA CONNAISSANCE

Le 29 septembre 2005, un membre du Comité permanent R et un enquêteur ont assisté aux journées de rencontre « Innovation, compétitivité et connaissance » à Paris organisé par la revue « *Veille Magazine* »¹² autour des thèmes « [l'Intelligence économique](#) » et « [la veille](#) ».

Deux membres de la Sûreté de l'État ainsi qu'un membre du SGRS participaient à cette conférence témoignant d'intérêt que chaque service porte à la protection du potentiel scientifique et économique

Cette participation s'inscrit dans le cadre de l'élaboration d'une proposition de définition du potentiel scientifique et économique¹³.

¹² La revue française *Veille Magazine* publie des articles relatifs à l'intelligence économique et à la gestion des connaissances.

¹³ Voir titre 6 – Etude et activités, Chapitre 1 – L'Etude sur le potentiel scientifique et économique

Ces journées de rencontre étaient organisées en collaboration avec l'Intelligence Collective, Coopération et Efficacité (ICCE). Ce fut en outre la première fois qu'un événement du genre organisé en France se consacrait à « ...*la maîtrise stratégique des informations et des connaissances ainsi que l'innovation au cœur des enjeux technologiques, économiques et organisationnels de chaque entreprise.* »¹⁴

Pour le Comité permanent R et le Service d'enquêtes, la participation à cet événement fut l'occasion de découvrir la situation française concernant l'intelligence économique et, plus particulièrement, les solutions, les technologies et les méthodes qui sont développées dans ce domaine.

Parallèlement au « *Forum IE2005* », entièrement dédié aux renseignements économiques et à la 'veille', se tenaient également un séminaire portant sur les '*Dynamiques offensives et conquêtes de marchés*', ainsi qu'un forum intitulé '*Forum KM&EC2005*' (sur la gestion des connaissances et '*l'efficacité collective*').

Sont relatées ci-dessous les présentations entendues lors du « *Forum IE2005* ».

Les orateurs suivants ont particulièrement retenu l'attention des membres du Comité permanent R :

Le professeur QIHAO MIAO (Chine).

Le professeur QIHAO MIAO est considéré comme l'un des promoteurs de l'intelligence économique (également appelé intelligence compétitive, IC) en Chine. La révolution économique chinoise axée sur l'ouverture au marché mondial a déclenché une explosion de la demande pour l'intelligence compétitive. Le professeur MIAO pense que ceci doit devenir une priorité pour son pays s'il a pour but de devenir un grand acteur économique mais aussi un acteur puissant dans un monde globalisé.

Le professeur MIAO propose aux entreprises occidentales une formule qu'il baptise « co-pétition », c'est-à-dire une relation dans laquelle les acteurs sont à la fois partenaires et compétiteurs. Sa philosophie en la matière consiste à passer de « l'art de la guerre » tel que défini par l'antique général Sun Tsu à la co-pétition. Il s'agit de surpasser l'adversaire sans lui faire la guerre.

Monsieur CHABASSE, co-fondateur de l'ONG Handicap International :

Commentant le succès de la campagne internationale qu'il a menée contre les mines anti-personnelles, monsieur CHABASSE veut démontrer l'influence que peuvent prendre les ONG dans l'élaboration des règles internationales. Les ONG sont devenues des lieux de contre-pouvoir (des « *stakeholders* »). Ceci peut entraîner des répercussions sur le monde économique et avoir un effet déstabilisant sur des entreprises. Les capacités de mobilisation de l'opinion publique développées par les ONG s'appuient souvent sur un haut degré d'expertise et de connaissances techniques qu'il ne faut pas négliger. Monsieur CHABASSE souligne le fossé qui existe dans l'image que les entreprises se font des ONG et réciproquement. Ces acteurs devront pourtant arriver à se comprendre et à dialoguer les uns avec les autres dans la mise en oeuvre des stratégies de développement durable. C'est ce à quoi il s'emploie dans sa fonction actuelle de conseiller auprès des entreprises sur la relation avec le monde associatif.

¹⁴ *Veille Magazine*, n° 87, octobre 2005, p. 3.

Madame REVEL, Iris Action

Les règles et les normes développées par l'Union européenne peuvent profondément affecter les processus de production économique. L'influence normative et le lobbying se développent donc afin d'influencer les processus d'élaboration des règles internationales. Le lobbying cherche à favoriser des intérêts privés, les ONG cherchent à promouvoir des intérêts éthiques et humanitaires. Il est nécessaire, selon Madame REVEL de réguler ces activités.

Elle souligne l'apparition de nouvelles formes de droit qui peuvent aussi influencer le monde économique. C'est ce qu'elle appelle les « soft laws » c'est-à-dire une série de principes non obligatoires (chartes, labels, codes éthiques, etc.) qu'on s'engage à respecter en matière de production économique, de respect de l'environnement, de commerce équitable, Les ONG jouent un rôle très important dans l'élaboration de ces nouvelles règles.

Monsieur BREESE, conseiller en propriété intellectuelle.

Nous vivons dans une société où la source de richesse est de plus en plus immatérielle. La connaissance (le capital intellectuel) représente 65 à 85 % de la valeur d'une entreprise. Dans le contexte de la société de l'information, existe le risque pour une entreprise de perdre la maîtrise des informations échangées avec les clients, les concurrents, les autorités, Pour monsieur BREESE, il est nécessaire que l'État protège les droits de propriété intellectuelle. Or on assiste actuellement à un puissant travail de lobby de la part des milieux libertaires pour remettre en question ces droits intellectuels (voir la problématique du brevetage des logiciels vs logiciels libres). Il y a contestation de toute forme de protection du secret.

Monsieur BREESE cite la législation américaine sur les « *trade secrets* » comme modèle à suivre. Il démontre les lacunes des législations actuelles en France et en Europe sur la protection des secrets. Il regrette le manque de sensibilité du monde politique et économique français à cette problématique.

Monsieur BESSON, contrôleur général à la Direction Centrale française des Renseignements Généraux (DCRG), chargé de mission à l'IE, spécialement délégué pour l'intelligence économique.

Monsieur BESSON répond à la question : « quels services les services de renseignement d'État peuvent-ils rendre aux entreprises ? »

Pour Monsieur BESSON, les services de renseignement de l'État ont une mission de service public qui est d'informer les autorités de l'État, non les intérêts privés.

Les services d'État n'ont pas à se substituer aux entreprises défaillantes qui négligent de mettre en place une cellule d'intelligence économique en leur sein. L'IE est un concept qu'il appartient aux entreprises de mettre en œuvre, pas aux services de renseignement. Ceci ne doit pas empêcher que les uns et les autres se rencontrent. Il existe toutefois entre eux de nombreuses barrières qui rendent ces rencontres difficiles : différence de culture et de mentalité...

En France, c'est la DST qui a pour mission d'entretenir des contacts avec les entreprises, non les Renseignements Généraux. Les RG informent l'État de toute menace ou vulnérabilité via les préfets et le ministère de l'Intérieur. Les informations intéressant le monde des entreprises sont orientées vers la Délégation générale à l'Intelligence Économique. Les préfets sont chargés de la mise en œuvre des politiques régionales d'IE.

Un chef d'entreprise confronté à une menace (espionnage, sabotage, extorsion, etc.) peut s'adresser indistinctement au préfet de son département, à la DST, aux RG ou à la Gendarmerie. La confidentialité lui est garantie.

Un représentant de la DST

Le représentant de la DST rappelle les missions de la DST dans cette matière : le contre-espionnage, le contre-terrorisme, la protection du patrimoine et la lutte contre la prolifération. Depuis 1981, la DST accorde une assistance aux entreprises, aux labos et aux communautés territoriales confrontées à l'espionnage économique.

Les contacts avec les entreprises et les labos sont quotidiens. Ils consistent essentiellement en séances d'information et briefing de sensibilisation sur les dangers et vulnérabilités des entreprises (sécurité physique, fiabilité des personnes, sécurité des systèmes d'information, ...). Cela représente quelque 600 conférences touchant +/- 35.000 personnes par an. Ce dialogue avec les chefs d'entreprises n'est pas facile parce que sensible mais il est franc. C'est un véritable partenariat qui a été réalisé avec les entreprises et les labos. Les informations que la DST en retire (ponctuelles ou générales) remontent vers les ministères concernés. Sur le terrain, il y a collaboration avec les RG et la Gendarmerie. La DST collabore aussi avec la DGSE qui est représentée au sein de la délégation générale à l'IE.

La DST surveille les séjours d'étudiants et de stagiaires étrangers dans les établissements à accès restreints.

Le général e.r. SCHAEFFER, ancien attaché de défense en Asie.

Le général retraité SCHAEFFER devint consultant dans une firme privée. Il déclare que les militaires peuvent aussi être associés à l'IE. Il énumère les services que les attachés militaires français à l'étranger peuvent rendre aux entreprises. C'est essentiellement dans le secteur de l'armement qu'ils peuvent renseigner les entreprises françaises sur les besoins des armées étrangères et sur les appels d'offre.

Monsieur DOUBLET, chef d'entreprise.

Monsieur DOUBLET dirige une PME « High Tech » dans la région Nord-Pas de Calais. S'il se félicite des initiatives prises dans sa région en matière d'IE, il déplore par contre l'absence d'approche globale de l'IE de la part du gouvernement. Il critique l'obligation faite aux entreprises de publier leurs comptes « *ce qui permet à nos concurrents étrangers de tout savoir de nous !* ». Monsieur DOUBLET explique qu'il a plusieurs fois consulté les DCRG, notamment pour préparer un voyage en Chine, à propos de l'espionnage économique américain en France et lorsque son entreprise a été victime d'un vol d'ordinateur.

Monsieur CARAYON

Monsieur CARAYON, député, répéta que l'intelligence économique est « une politique publique ».

Eu égard au contenu de la politique à mettre en œuvre en matière d'intelligence économique, monsieur CARAYON réitéra les recommandations déjà formulées lors d'interventions passées¹⁵, à savoir :

- « une politique de compétitivité qui favorise la recherche et permet l'accompagnement des entreprises dans la conquête de marchés mondiaux ; accompagnement par l'identification commune d'enjeux stratégiques et la mutualisation des expertises et des informations publiques et privées ;
- une politique de sécurité économique qui protège le périmètre stratégique de l'économie nationale ;
- une politique d'influence, notamment auprès des organismes où s'élaborent désormais les normes qui règlent la vie économique ;
- enfin une politique de formation. »

Il aborda également le champ d'application de la politique en matière d'intelligence économique.

En bref, il répéta l'argumentation qu'il avait déjà précédemment exposée :

« Cette politique publique d'intelligence économique concerne plus particulièrement les marchés qui ne sont pas seulement créateurs de valeur mais également générateurs d'influence et de puissance, - ceux par exemple de l'aéronautique et de l'espace, de l'armement, de l'énergie, de la pharmacie et de la génétique, des réseaux, des technologies de l'information, des télécommunications et de la sécurité. Dans ces marchés, que j'appelle "stratégiques", ce ne sont pas la qualité ou le prix des produits et services qui font la différence mais bien l'accompagnement politique des Etats qui permet de les conquérir. »

Dernier point qui attira notre attention était son avis selon lequel aucun critère objectif – mais bien des critères subjectifs - ne peut déterminer si une entreprise est française ou non.

À la fin de son exposé, monsieur CARAYON insista sur l'importance du « patriotisme économique » et souligna le fait que cette politique ne prône pas un mur de Berlin mais « ...un outil pour fédérer les expertises. »¹⁶

¹⁵ Cf. notamment l'intervention de Bernard Carayon le 15 décembre 2004, « La sécurité économique : une stratégie globale pour l'entreprise et pour l'Etat » consultée le 4 octobre 2005 à l'adresse http://www.bcarayon-ie.com/pages_conferences/20041215.html

¹⁶ A propos du « patriotisme économique », Dominique de Villepin déclarait dans *Sentinel – Analyses & Solutions* (Sentinel N° 27 – consulté le 30 septembre 2005 à l'adresse http://www.infosentinel.com/info/news_8.htm) : « Rassembler nos forces, cela veut dire que nous valorisons le fait de défendre la France et ce qui est français. Cela s'appelle le patriotisme économique. »

Monsieur DARRASON - Président de la Compagnie européenne d'intelligence stratégique

Monsieur DARRASON donna un aperçu chronologique des initiatives prises ces dernières années en France par les secteurs privé et public dans le cadre de l'intelligence économique.

Ensuite, il souligna l'importance d'un organe de coordination bien huilé à l'échelle nationale qui, par manque de moyens, risque de perdre sa crédibilité.

Il déclara encore espérer que le projet de décret (qui énumère les secteurs à protéger et pour lequel des négociations doivent encore être menées avec les différents secteurs) ne soit pas censuré par l'Union européenne.

Monsieur MONIN, Vice-président de Knowings

KNOWINGS produit des logiciels et est spécialisée dans la *gestion des connaissances*.

Monsieur MONIN fit un exposé sur les résultats d'une enquête qu'elle a menée entre avril et juillet 2005 à propos de la perception de l'intelligence économique par les entreprises françaises. Cette enquête avait pour objectif de se faire une idée du marché et du débat actuel au sein du secteur privé en matière d'intelligence économique.

L'enquête¹⁷ a révélé que :

- les entreprises (françaises) donnent la préférence à la « *veille offensive* », en prêtant une attention toute particulière aux clients et marchés ;
- dans la pratique, l'intelligence économique au sein des entreprises est axée sur la création de réseaux (internes) ;
- les administrateurs des sociétés donnent la priorité à une gestion opérationnelle des connaissances ;
- la gestion des connaissances est de plus en plus souvent utilisée dans la gestion de projets ;
- seulement 16 % des entreprises disposent d'un « *portail collaboratif* » ;
- la priorité est donnée à la gestion de projets et aux « *relations inter-services* ».

Madame ARCHAMBAULT, RHODIA NOVECARE

Madame ARCHAMBAULT s'occupe d'intelligence économique dans l'entreprise RHODIN NOVECARE et aborda, dans son exposé, les principes appliqués dans sa société dans le cadre du processus décisionnel. Sa présentation incluait quelques informations utiles pour les dirigeants d'entreprise qui souhaitent introduire l'intelligence économique dans leur société.

¹⁷ Les résultats de l'« *Enquête KNOWINGS 2005* » sont disponibles sur le site Web <http://www.knowings.com>

Monsieur GERMONT, Institut national du sport et de l'éducation physique

Entre-temps, le concept d'« intelligence économique » a également fait son apparition dans le secteur sportif en France et a même donné lieu à la création d'une spécialité : *l'intelligence sportive*.

Son discours ne comprenait toutefois aucune révélation en matière de protection du potentiel économique. Le seul point qui mérite d'être signalé est peut-être l'aveu de monsieur Germont que le retard de la France par rapport à la Grande-Bretagne pour l'organisation des Jeux olympiques à Paris était déjà apparu avant le vote définitif.

Cette affaire démontre que même des instruments performants, tels qu'une cellule qui veille sur la position concurrentielle de l'entreprise (ou d'une autre entité) et remet des rapports à cet égard, ne sont pas une garantie de réussite. Le succès d'une stratégie peut également être influencé par d'autres facteurs (p. ex. : des facteurs contextuels).

Madame FREZAL, professeur à l'INSA, LYON

Madame FREZAL forme des étudiants qui se spécialisent dans l'intelligence économique. Dans son exposé, elle présenta les résultats d'une enquête qu'elle mena avec des étudiants auprès de petites et moyennes entreprises françaises à propos de la perception de l'intelligence économique parmi des chefs d'entreprise français.

Il ressort de son enquête qu'il est difficile de mobiliser les dirigeants de PME en faveur de l'intelligence économique, et ce, pour plusieurs raisons (manque de temps, mauvaise perception de l'utilité immédiate, mauvaise évaluation...).

L'AVENIR DE L'INTELLIGENCE ÉCONOMIQUE EN FRANCE

Monsieur DARANTIÈRE, Association pour la promotion de l'intelligence économique et concurrentielle – (SCIP France)

Monsieur DARANTIÈRE qualifie le marché de l'intelligence économique en France d'« *objet économique non identifié (OENI)* ». Les informations relatives à ce marché étant plutôt rares.

L'on dispose toutefois d'un certain nombre de chiffres. Ainsi, le marché français des services d'intelligence économique s'élèverait à 125 millions d'euros et serait aux mains d'une centaine d'entreprises. Seulement 5 % de ces entreprises afficherait un chiffre d'affaires de plus de 5 millions d'euros.

Le marché se concentrerait sur deux grandes activités : la veille (25 % des entreprises) et la stratégie (24 %). L'on estime que 800 à 1000 personnes s'occuperaient à temps plein de tâches relatives à l'intelligence économique dans les entreprises.

L'orateur esquissa ensuite les tendances et évolutions du marché de l'intelligence économique. Du point de vue structurel, il note (a) une mondialisation du marché, (b) un flux financier plus rapide et le développement du capital d'investissement, et (v) l'augmentation des reprises et fusions.

Enfin, il souligna la présence des « *Big Four* » (grandes entreprises de consultance et d'audit, telles que PricewaterhouseCoopers) sur le marché de l'intelligence économique qui en sont les nouveaux acteurs à l'échelle mondiale.

Monsieur JUILLET, 'Haut responsable à l'intelligence économique auprès du Premier ministre'

Le rapport CARAYON recommandait notamment la désignation en France d'un « Haut responsable à l'intelligence économique ». Monsieur JUILLET occupe cette fonction. Son exposé était principalement consacré à l'intelligence économique en tant que « *politique publique* ».

Il s'agit, selon lui, d'« *...un état d'esprit, un fait d'ouverture* » et d'une affaire qui concerne tout le monde, et donc pas le monopole d'une seule personne. L'intelligence économique englobe les techniques, instruments et est même « *...une science en marche* ».

Le gouvernement joue ici un rôle essentiel et les objectifs de la politique gouvernementale sont : la sensibilisation, la formation, les conseils, l'assistance et la défense des entreprises. Le gouvernement ne doit pas être considéré comme celui qui va résoudre tous les problèmes, mais plutôt comme un guide (orienteur).

Monsieur JUILLET souligna la « *pole position* » que la France occupe à présent sur le continent européen en matière d'intelligence économique. Pour que le continent européen ne soit pas écrasé entre les États-Unis et la Chine, il doit rester compétitif.

Toujours selon lui, il faut que d'autres pays européens se mobilisent également et que l'on assiste à un échange d'idées ou concepts nouveaux ou autres.

6. SÉMINAIRE EUROMED JUSTICE « DÉFINITION ET INCRIMINATIONS PÉNALES. ASPECTS TRANSVERSAUX DU CRIME ORGANISÉ »

Un membre du Service d'enquêtes a assisté à ce premier séminaire régional du programme EuroMed Justice de la Commission européenne (Madrid, 14-17 novembre 2005). Ce séminaire s'inscrit dans le cadre de la politique euro-méditerranéenne de l'Union européenne (UE).

Les participants étaient des membres des délégations des Partenaires méditerranéens suivants : (Algérie, Autorité palestinienne, Egypte, Israël, Jordanie, Liban, Maroc, Syrie, Tunisie et Turquie) et des Etats membres de l'Union européenne indiqués ci-après (Belgique, France, Espagne, Pays-Bas et République tchèque). Par ailleurs, le séminaire a bénéficié de la participation de représentants de la Cour Pénale Internationale, du Bureau des Nations unies pour les drogues et les crimes et du Conseil de l'Europe.

Les participants ont émis l'avis que ce séminaire leur avait permis :

- a) de se familiariser avec les différentes réalités concernant le thème du terrorisme et d'analyser les aspects transversaux du crime organisé dans leur contexte légal international, entre autres dans l'Union européenne, dans ses Etats membres et chez les Partenaires méditerranéens ;

- b) de mieux connaître le rôle de certaines institutions telles que la Cour Pénale Internationale, les Nations unies, l'Union européenne et le Conseil de l'Europe dans la lutte contre le terrorisme et la prévention de la criminalité transnationale organisée ;
- c) de favoriser un échange sur les pratiques et expériences, et établir des contacts entre les participants afin de promouvoir la coopération entre les différentes institutions représentées dans le domaine de la justice.

Les participants ont adressé cette déclaration auprès des Directions générales concernées de la Commission européenne, des Etats membres de l'Union européenne et des Partenaires méditerranéens.

7. SEMINAIRE SUR LE « TERRORISME »

Un membre du Comité permanent R a assisté dans le prolongement du séminaire précédant, au deuxième séminaire régional sur le « Terrorisme » du Programme EuroMed Justice de la Commission européenne (CE) qui s'inscrit dans la politique euro-méditerranéenne de l'Union européenne et qui s'est déroulé à la Haye du 12 au 15 décembre 2005. Les délégations des Partenaires méditerranéens étaient les mêmes qu'à Madrid.

Les Etats membres de l'Union européenne représentés étaient la Belgique, l'Espagne, la France, les Pays-Bas et le Portugal). Par ailleurs, le séminaire a bénéficié de la participation de représentants du Bureau des Nations unies pour les drogues et les crimes, d'Eurojust, d'Europol et du Conseil de l'Europe.

Les participants ont constaté que ce séminaire leur avait permis :

- a) d'analyser en profondeur les différentes réalités concernant le thème du terrorisme et de la lutte contre le terrorisme dans le contexte légal national et international ;
- b) de mieux connaître les procédures d'échange d'information dans la lutte contre le terrorisme et contre le financement du terrorisme en soulignant le rôle d'institutions comme Eurojust et Europol ;
- c) de favoriser un échange sur les pratiques et expériences, et établir des contacts entre les participants afin de promouvoir la coopération entre les différentes institutions représentées dans le domaine de la justice.

Les participants ont adressé cette déclaration auprès des Directions générales concernées de la Commission européenne, des Etats membres de l'Union européenne et des Partenaires méditerranéens.